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

Final Audit Report

Subject:

FY 2008
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
FOLLOW-UP AUDIT

Report No. **4A-CI-00-08-061**

Date: 09/16/2008

--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 2008
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
FOLLOW-UP AUDIT

WASHINGTON, D.C.

Report No. **4A-CI-00-08-061**

Date: 09/16/2008

Michael R. Esser
Assistant Inspector General
for Audits

Executive Summary

U.S. OFFICE OF PERSONNEL MANAGEMENT
--
FY 2008
FEDERAL INFORMATION SECURITY MANAGEMENT ACT
FOLLOW-UP AUDIT

WASHINGTON, D.C.

Report No. 4A-CI-00-08-061

Date: 09/16/2008

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) 2008 compliance with the Federal Information Security Management Act (FISMA), as well as OPM's information technology security policy. As part of our FY 2007 FISMA audit, we audited the information technology security controls of four of OPM's major applications:

- Actuaries Group System (AGS)
- GoLearn Learning Management Systems (GoLearn)
- Learning Management System (LMS)
- Government Financial Information System (GFIS)

In addition, the FY 2007 FISMA follow-up audit indicated that the following OPM major applications had outstanding audit recommendations from the FY 2006 and FY 2005 FISMA audits:

- Fingerprint Transaction System (FTS)
- Enterprise Human Resources Integration Data Warehouse (EHRI)
- Personnel Investigations Processing System Financial Interface System (PFIS)
- Electronic Questionnaire for Investigations Processing (EQIP)

This report describes 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:

- The Office of the Inspector General (OIG) audited the information technology (IT) security controls of GoLearn in FY 2007 and issued report number 4A-HR-00-07-009 with three audit recommendations. As of August 2008, all recommendations have been implemented.

- The OIG audited the IT security controls of GFIS in FY 2007 and issued report number 4A-CF-00-07-010 with eight audit recommendations. As of August 2008, all eight recommendations have been implemented.

- The OIG audited the IT security controls of AGS in FY 2007 and issued report number 4A-RI-00-07-41 with no audit recommendations.

- The OIG audited the IT security controls of LMS in FY 2007 and issued a draft with three audit recommendations. The three audit recommendations were implemented prior to the issuance of final report number 4A-HR-00-07-42 which contained no outstanding audit recommendations.

- The 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 August 2008, two recommendations remain outstanding.

- 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 August 2008, the one outstanding recommendation has not yet been implemented.

- The OIG audited the IT security controls of EQIP 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 August 2008, two of these four recommendations remain outstanding.

- The OIG audited the IT security controls of 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 August 2008, all recommendations have been implemented.

Contents

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 the information technology (IT) security controls of the agency's major applications on a rotating basis. As part of our fiscal year (FY) 2007 FISMA audit, we reviewed the IT security controls of four of the Office of Personnel Management's (OPM) major applications:

- GoLearn Learning Management Systems (GoLearn) - *Report No. 4A-HR-00-07-009*
- Government Financial Information System (GFIS) - *Report No. 4A-CF-00-07-010*
- Actuaries Group System (AGS) - *Report No. 4A-RI-00-07-41*
- Learning Management System (LMS) - *Report No. 4A-HR-00-07-42*

In addition, the FY 2007 FISMA follow-up audit indicated that the following OPM major applications had outstanding audit recommendations from the FY 2006 and FY 2005 FISMA audits:

- Fingerprint Transaction System (FTS) - *FY2006 Report No. 4A-IS-00-06-021*;
- Enterprise Human Resources Integration Data Warehouse (EHRI) – *FY 2005 Report No. 4A-OD-00-05-013*;
- Electronic Questionnaire for Investigations Processing (EQIP) – *FY 2005 Report No. 4A-IS-00-05-026; and*
- Personnel Investigations Processing System (PIPS) Financial Interface System (PFIS) – *FY 2005 Report No. 4A-CF-00-05-025.*

This audit report details our follow-up of the outstanding recommendations from each of the audits listed above.

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 audit, we evaluated the progress that the various program offices have made in implementing our recommendations.

The "Results" section of this report documents the original audit 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.

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 GoLearn, GFIS, AGS, LMS, FTS, EHRI, EQIP, and PFIS.

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

We conducted this performance audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide 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. The audit covered program office FISMA compliance efforts through August 2008.

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.

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 Revision 1, 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 information 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 results of the sample were not projected to the entire population.

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 August 2008 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 has made in addressing the recommendations made in our prior OIG FISMA audit reports. For each prior recommendation that was outstanding at the beginning of this follow-up audit, 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 further details concerning each of the unresolved audit recommendations.

I. GoLearn Learning Management Systems

GoLearn is comprised of four of OPM's major IT systems (Plateau Verizon LMS, Learn LMS, GeoLearning LMS, and the General Physics LMS). GoLearn is part of the e-training e-Government initiative which is intended to "Create a premier e-training environment that supports development of the Federal workforce through simplified and one-stop access to high quality e-training products and services, and, thus, advances the accomplishment of agency missions." OPM's Human Resources Products & Services Division (HRPS) has been designated with ownership of GoLearn. The OIG audited the IT security controls of GoLearn in FY 2007 and issued report number 4A-HR-00-07-009 with three audit recommendations. As of August 2008, all recommendations remain outstanding.

a. FY 2007 recommendation

We recommend that the GoLearn Program require Verizon to implement a formal process to evaluate the background of each employee at both data centers where the GoLearn LMS is housed.

FY2008 Status

In 2007, HRPS partially concurred with the recommendation and identified a POA&M item to "modify existing agreements with the hosting facility," with an expected completion date of January 2008, to ensure the OPM requirement was met.

As of August 2008, the recommendation remains on the POA&M with a status of complete. However, the OIG has not received any documentation indicating that HRPS has implemented this recommendation.

FY 2008 Recommendation 1

We continue to recommend that the GoLearn Program require Verizon to implement a formal process to evaluate the background of each employee at both data centers where the GoLearn LMS is housed, and provide the OIG with evidence that the audit recommendation has been implemented.

CIS/CIO Response:

"We accept the recommendation and have provided documentation to your office."

OIG Reply:

We have reviewed the documentation provided and acknowledge that Verizon has implemented a formal process to evaluate the background of employees working at the data centers where the GoLearn LMS is housed. No further action is required.

b. FY 2007 recommendation

We recommend the GoLearn Program ensure that Plateau and General Physics LMS perform an annual test of their contingency plans, and provide the OIG with evidence that the audit recommendation has been implemented.

FY2008 Status

In 2007, HRPS concurred with the recommendation and listed it as an action item on the system's POA&M.

As of August 2008, the recommendation is listed on the GoLearn POA&M with a status of complete. However, the OIG has not received any documentation indicating that HRPS has implemented this recommendation.

FY 2008 Recommendation 2

We continue to recommend that GoLearn Program ensure that Plateau and General Physics LMS's perform an annual test of their contingency plans, and provide the OIG with evidence that the audit recommendation has been implemented.

CIS/CIO Response:

"We accept the recommendation and have provided documentation to your office."

OIG Reply:

We have reviewed the documentation provided and acknowledge the efforts HRPS has taken to address this audit recommendation. No further action is required.

c. FY 2007 recommendation

We recommend that the GoLearn Program update the GeoLearning contingency plan to fully document the following information:

- References/Requirements,
- System Description and Architecture,
- Concurrent Processing Procedures, and
- Plan Deactivation Procedures.

FY2008 Status

In 2007, HRPS concurred with this recommendation and created an action item on the system's POA&M to draft a Contingency Plan consistent with applicable Federal laws and regulations.

As of August 2008, the recommendation remains on the GoLearn POA&M with a status of complete. However, the OIG has not received any documentation indicating that HRPS has implemented this recommendation.

FY 2008 Recommendation 3

We continue to recommend that the GoLearn Program update the GeoLearning contingency plan as described in the original audit recommendation, and provide the OIG with evidence that the audit recommendation has been implemented.

CIS/CIO Response:

"We accept the recommendation and have provided documentation to your office."

OIG Reply:

We have reviewed the updated contingency plan provided by HRPS and found that it addressed the audit recommendation. No further action is required.

II. Government Financial Information System

GFIS provides financial planning capabilities and a means for OPM to record financial transactions. It offers functionality to document financial planning and purchasing events, accounts receivable and payable, disbursement, and budgeting activities. The Office of the Chief Financial Officer, Center for Financial Services (CFS) has been designated with system ownership of GFIS.

The OIG audited the IT security controls of this system in FY 2007 and issued report number 4A-CF-00-07-010 with eight audit recommendations. As of August 2008, all eight recommendations have been implemented.

a. FY 2007 recommendation

We recommend that CFS document in the GFIS risk assessment the identification and analysis of the GFIS vulnerabilities, including analyzing the system's controls and determining the likelihood and adverse impact to the system for each identified vulnerability.

FY 2008 Status

The most recent version of the GFIS risk assessment includes the identification and analysis of the system's vulnerabilities. In addition, the risk assessment analyzes the system's controls and determines the likelihood of an adverse impact to the system for each of the identified vulnerabilities. No further action is required.

b. **<u>FY 2007 recommendation</u>**

We recommend that CFS distribute and require that each user review and sign the GFIS rules of behavior statement. These signed rules of behavior statements should be maintained by the system designated security officer (DSO).

<u>FY 2008 Status</u>

Signed rules of behavior statements for GFIS users are documented and maintained. The OIG judgmentally selected a sample of 15 of 391 GFIS users and verified that a Rules of Behavior statement was signed. OIG reviewed both hard and electronic copies and compared them to a list of authorized GFIS users. CFS also provided evidence that quarterly reviews are conducted to ensure all active users have signed the rules of behavior statement. We found that CFS maintains copies of the signed agreements for all users at a central location. No further action is required.

c. **<u>FY 2007 recommendation</u>**

We recommend that CFS implement the OPM [redacted] Configuration Policy on the GFIS data warehouse [redacted]. Furthermore, we recommend that CFS document this implementation.

<u>FY 2008 Status</u>

The most recent version of the GFIS information system security plan (ISSP) has been updated by CFS to include a section accepting the risks associated with and the reason for not implementing the OIG recommendation to support the [redacted] configuration. No further action is required.

d. **<u>FY 2007 recommendation</u>**

We recommend that GFIS security administrators periodically review user access lists for inactivity and promptly revoke access for accounts that exceed 35 days of inactivity in accordance with the OPM IT Security Policy.

<u>FY 2008 Status</u>

CFS has established procedures to review user access lists and has implemented quarterly reviews of GFIS users for inactivity. No further action is required.

e. **<u>FY 2007 recommendation</u>**

We recommend that CFS review the GFIS access list and deactivate the access for duplicate and generic user accounts.

<u>FY 2008 Status</u>

GFIS user access lists are reviewed for duplicate and generic user accounts on a quarterly basis. OIG was provided with a sample duplicate report that showed user IDs, user names, and a status of “inactive” for all users that had duplicate accounts. No further action is required.

f. <u>FY 2007 recommendation</u>

We recommend that CFS document and maintain on file authorizations that specify the authorized privileges for each GFIS user. In addition, we recommend that CFS periodically verify that only authorized users have access and that their privileges are appropriate for GFIS by reviewing user authorization forms and comparing them to access lists. We recommend that this recommendation be added as a milestone to the GFIS POA&M.

<u>FY 2008 Status</u>

User access lists for GFIS users are documented and maintained. The OIG judgmentally selected a sample of 15 of 391 GFIS users and verified that authorization to access GFIS is documented, maintained, and periodically reviewed and compared to access lists. We also verified that the authorization was approved prior to granting the user access to the system. No further action is required other than the continuation of the quarterly comparison of access lists to authorizations.

g. <u>FY 2007 recommendation</u>

We recommend that an independent review be conducted of the system's IT security controls that were tested by the GFIS DSO.

<u>FY 2008 Status</u>

An independent security test and evaluation (ST&E) was conducted by CIS/CIO as part of the GFIS re-certification and accreditation (C&A). OIG was provided with the final ST&E, signed by the IT Security Officer. The recommendation was added to the GFIS POA&M and labeled as completed as of the 3rd quarter of 2008. No further action is required.

h. <u>FY 2007 recommendation</u>

We recommend that an independent source review the security test and update the test report with detailed results and corrective actions. Furthermore, we recommend that CFS add corrective actions as milestones to the GFIS POA&M.

<u>FY 2008 Status</u>

An independent review of the security test and reports with the detailed results and corrective actions was conducted by the OCIO in FY 2007. No further action is required.

III. <u>Actuaries Group System</u>

AGS pulls data extracts from the Federal Employees Retirement System, the Civil Service Retirement System, the Federal Employees Health Benefits Program, the Federal Employees’ Group Life Insurance Program, and the Central Personnel Data File. The data extracts are run through batch sub-systems to project the financial health of these various benefit programs. The Division for Strategic Human Resources Policy has been designated with ownership of AGS.

The OIG audited the IT security controls of this system in FY 2007 and issued report number 4A-RI-00-07-41 with no audit recommendations.

IV. Learning Management System

LMS is owned and operated by OPM's Center for Leadership and Capacity Services (CLCS). The mission of CLCS is to provide leadership training and development for Federal executives and managers. LMS is a combination of several commercial-off-the-shelf packages that provides a real-time, centralized system for managing training course and participant training information. It utilizes a web based front-end interface running on an OPM web server, and a back-end [redacted].

The OIG audited the IT security controls of this system in FY 2007 and issued a draft with three audit recommendations. The three audit recommendations were implemented prior to the issuance of final report number 4A-HR-00-07-42, which contained no outstanding audit recommendations.

V. Fingerprint Transaction System

FTS allows for the electronic scanning of fingerprint images so that Federal agencies can conduct electronic searches of these images. 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 August 2008, three recommendations remain outstanding.

a. FY 2006 recommendation

We recommend that the Federal Investigative Services Division (FISD) update the FTS ISSP to identify the current DSO and system owner and include their contact information.

FY 2008 Status

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

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

In August 2008, the OIG reviewed a copy of the most recent ISSP where the DSO and system owner have been properly documented. No further action is required.

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 2008 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 . . . 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 had not received documentation indicating that FISD had implemented this recommendation. The recommendation remained on the FTS POA&M with a status of "Pending." However, the target completion date of June 30, 2007 had passed.

In August 2008, the OIG was provided with documentation that indicated that FISD was following NMG's Standard Operating Procedures related to the tracking of system changes. No further action is required.

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 2008 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 had not received documentation indicating that FISD had implemented this recommendation. The recommendation remained on the FTS POA&M with a status of "Pending." However, the target completion date of March 31, 2007 had passed.

In August 2008, the OIG was provided with a training log showing personnel with significant security responsibilities had received specialized training. The log included the name of the user, type of training they took and the date it was completed. No further action is required.

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 them to access lists.

FY 2008 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 had not received documentation indicating that FISD had implemented this recommendation. The recommendation remained on the FTS POA&M with a status of "Pending." However, the target completion date of June 30, 2007 had passed.

As of August 2008, the recommendation has been partially implemented. The OIG was provided with an Interconnectivity Security Agreement that includes a list of FTS users, but does not specify the authorized privileges for each. In addition, the OIG was provided the required steps for obtaining authorization to submit electronic fingerprints to OPM. However, the OIG has not been provided with evidence that FISD is periodically reviewing the authorization forms and access lists to verify that only authorized users have access to FTS. The recommendation is included in the FTS POA&M with a status of "delayed" and an expected completion date of December 30, 2008.

FY 2008 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 them to access lists.

CIS/CIO Response:

The CIS/CIO and FISD both concur with the recommendation. In addition, FISD stated that "External users previously identified as FTS users have been clarified with the IG in a meeting held August 4, 2008, as users of the fingerprint machines that transmit data to the FTS application. The fingerprint machines are the only connection to the FTS application from the external agency and the connection is documented in an Interconnection Security Agreement (ISA) established with each external agency. A copy of the ISA was previously provided for review by the IG office. The FTS application users are internal to OPM and FISD has obtained documented file authorizations for each of them and providing evidence attached to this response as Attachment 1. In addition, FISD is establishing a process to periodically review the access for those users to validate their usage on the FTS application."

OIG Reply:

We acknowledge the steps FISD is taking to address this recommendation, and recommend that FISD continue its efforts to establish a process to maintain and periodically review access authorizations for FTS users internal to OPM.

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 2008 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 had not received documentation indicating that FISD had implemented this recommendation. The recommendation remained on the FTS POA&M with a status of "Pending." However, the target completion date of June 30, 2007 had passed.

In August 2008, the OIG was provided with a Production Change Request Form indicating that the four settings listed in the recommendation had been appropriately adjusted. No further action is required.

f. FY 2006 recommendation

We recommend that FISD ensure that for the planned FY 2006 re-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 2008 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.

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

As of August 2008, the recommendation remains on the FTS POA&M with a status of "delayed" and a target completion date of July 31, 2008.

<u>FY 2008 Recommendation 5</u>

We continue to recommend that FISD ensure that the appropriate actions outlined in the original recommendation are implemented during the re-certification and accreditation of FTS.

<u>CIS/CIO Response:</u>

The CIS/CIO and FISD both concur with the recommendation. In addition, FISD stated that they have "completed the re-certification and accreditation of FTS on July 14, 2008. A copy of the signed Authority to Operate is provided as evidence of completion and attached to this report as Attachment 2."

<u>OIG Reply:</u>

We have reviewed the documentation provided to confirm that FISD has completed the re-certification and accreditation of FTS in accordance with the original audit recommendation. No further action is required.

g. <u>FY 2005 recommendation</u>

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.

<u>FY 2008 Status</u>

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

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

As of August 2008, the recommendation remains on the FTS POA&M with a status of "delayed" and a target completion date of April 30, 2008.

FY 2008 Recommendation 6

We continue to recommend that FISD prepare the FTS contingency plan to document the items listed in the original recommendation.

CIS/CIO Response:

The CIS/CIO and FISD both concur with the recommendation. In addition, FISD stated that they have "developed a comprehensive FTS contingency plan and will complete a final version by August 29, 2008."

OIG Reply:

We will evaluate the updated contingency plan of FTS as part of the 2009 FISMA follow-up audit. The recommendation will remain outstanding until the OIG is able to confirm that the FTS contingency plan has been properly updated.

VI. 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 August 2008, 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 2008 Status

In FY 2005, EHRI stated that they have "begun planning 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 had not yet been implemented. The EHRI POA&M stated that the target completion date was September 2007.

As of August 2008, the OIG has not received any documentation indicating e-Gov has implemented this recommendation.

FY 2008 Recommendation 7

Until proof of closure can be provided, we continue to recommend that the Human Resources Line of Business (HRLOB) Program Management Office implement independent organization segments for the development and migration of system programming changes to EHRI.

CIS/CIO Response:

The CIS/CIO concurs with this recommendation. In addition, the program office stated that "Management concurs with the recommendation . . . . EHRI is currently completing the migration of the EHRI Data Warehouse development and production environments to a new hosting provider. As part of this move, EHRI is in the process of establishing a test environment separate from the development and production environments. Once these three environments have been established, the development/integration team will no longer have privileged access to the production environment. Furthermore, EHRI will ensure that the principles of separation of duties and least privilege are employed when user rights and privileges are established for the three environments. Until it has completed the activities described, EHRI concurs that all related action items should be listed as "open" on the EHRI Data Warehouse Plan of Action and Milestones."

OIG Reply:

We acknowledge the steps that HRLOB is taking to address this recommendation. We will evaluate HRLOB's progress in implementing independent organization segments for the development and migration of system programming changes to EHRI as part of the 2009 FISMA follow-up audit.

VII. Electronic Questionnaire for Investigations Processing

EQIP 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).

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 August 2008, these two recommendations remain outstanding.

a. <u>FY 2005 recommendation</u>

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

<u>FY 2008 Status</u>

In FY 2005, the Federal Investigative Services Division (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 EQIP rules of behavior statement had not been formally accepted by EQIP users, and FISD was still in the process of implementing automated acceptance of the EQIP rules of behavior. Consequently, the recommendation remained outstanding. FISD did not respond to the FY 2006 follow-up audit.

As of September 2007, FISD had not yet implemented this recommendation. Although the recommendation had been added to the EQIP POA&M as an action item, the target completion date of June 30, 2006 had passed and the status was listed as "Pending."

As of August 2008, the recommendation could not be traced to the most recent POA&M. In addition, FISD's DSO indicated that the recommendation has not been implemented.

<u>FY 2008 Recommendation 8</u>

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. In addition, we recommend that the program office keep action items listed as open in their POA&M until the weakness is fully corrected and proof of closure can be provided.

<u>CIS/CIO Response:</u>

The CIS/CIO and FISD both concur with this recommendation. In addition, FISD stated that "Each existing e-QIP administrator, operators and developers will sign Rules of Behaviors to be retained by the FISD DSO. Copies will be provided to the IG as evidence of closure by August 29, 2008."

OIG Reply:

We acknowledge the steps that FISD is taking to address this audit recommendation, and will confirm that all existing EQIP users have signed a Rules of Behavior document as part of the 2009 FISMA follow-up audit.

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 2008 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 EQIP rules of behavior statement had not been formally accepted by EQIP users, and FISD was still in the process of implementing automated acceptance of the EQIP rules of behavior. Consequently, the recommendation remained outstanding. FISD did not respond to the FY 2006 follow-up audit.

As of September 2007, FISD had not implemented this recommendation. Although the recommendation had been added to the EQIP POA&M as an action item, the target completion date of June 30, 2006 had passed and the status was listed as "Pending."

As of August 2008, the recommendation remains on the EQIP POA&M with a new expected completion date of December 31, 2008.

FY 2008 Recommendation 9

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

CIS/CIO Response:

The CIS/CIO and FISD both concur with this recommendation. In addition, FISD stated that "Each agency is responsible for documenting and maintaining the authorization of their respective e-QIP users. However, effective immediately all new agency e-QIP administrators will be required to review and accept the Rules of Behavior prior to being granted access to the application. A copy of the Rules of Behavior is included in this report as Attachment 3."

OIG Reply:

We acknowledge the steps that FISD has taken to require all new agency EQIP administrators to review and accept the rules of behavior document. No further action is required.

c. FY 2005 recommendation

We recommend that FISD 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 EQIP to identify and authenticate users provides the access controls necessary to maintain an appropriate level of security. If FISD and the CIS/CIO agree to an alternate access control methodology, this agreement should be documented.

FY 2008 Status

In FY 2005, FISD stated that it would "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 audit.

In FY 2007, the EQIP POA&M indicated that the recommendation had not yet been implemented. FISD stated that they were 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 EQIP agency users. The target completion date for implementing this recommendation was December 31, 2007, and the status was listed as "Pending."

As of August 2008, the recommendation could not be traced to the most recent POA&M. In addition, FISD's DSO indicated that the recommendation has not been implemented.

FY 2008 Recommendation 10

We continue to recommend that the FISD implement technical controls to identify and authorize system users, or document an alternate agreement with the CIS/CIO. In addition, we recommend that the program office keep action items listed as open in their POA&M until the weakness is fully corrected and proof of closure can be provided.

CIS/CIO Response:

The CIS/CIO concurs with this recommendation. FISD stated that they "concur with the recommendations. OPM's IT Security Policy requires username and password for identification and authorization. FISD has implemented the identification and authorization (username and password) of agency system users to e-QIP through the OPMIS Secure Portal and further strengthened through the e-Authentication process, as mandated by OMB. Once in the OPMIS Secure Portal, agency system users are required to provide answers to a series of Golden Questions and Answers (GQ/GA) to gain access into the e-QIP application. This process has been agreed to between the CIS/CIO and FISD as the appropriate level of security as required by the OPM IT Security Policy. A copy of the communication reflecting this agreement is included in this report as Attachment 4."

OIG Reply:

We acknowledge the steps that the CIS/CIO and FISD have taken to address this audit recommendation; no further action is required.

d. FY 2005 recommendation

We recommend that FISD verify that only authorized users have access to EQIP and maintain authorization forms for users, including administrators, operators, and developers.

FY 2008 Status

In FY 2005, FISD stated that it would "verify that only authorized users have access to EQIP and will maintain a file of these users." FISD documented the recommendation as "complete" on the system's POA&M.

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

As of September 2007, FISD had not yet implemented this recommendation. Although the recommendation had been added to the EQIP POA&M as an action item, the target completion date of June 30, 2006 had passed and the status was listed as "Pending."

As of August 2008, the recommendation remains on the EQIP POA&M with a status of "on-going" and an expected completion date of December 31, 2008.

FY 2008 Recommendation 11

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

CIS/CIO Response:

The CIS/CIO and FISD both concurred with the recommendation. In addition, FISD stated that "Each agency is responsible for documenting and maintaining the authorization of their respective e-QIP users. For agency e-QIP administrators, OPM operators and developers, FISD worked with CIS/CIO to develop an automated solution to remedy this requirement due to the volume of users. Due to competing priorities and Network Management Group of CIS/CIO's ability to move forward at this time, FISD has begun efforts to contract the development of an automated solution to provide the documented approval of access and ability to conduct periodic reviews to validate the authorized access and roles in the e-QIP system."

OIG Reply:

We will evaluate FISD's progress in implementing this audit recommendation as part of the 2009 FISMA follow-up audit.

VIII. PIPS Financial Interface System

PFIS provides a functional interface between PIPS and the 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.

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. As of August 2008, all recommendations have 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, the OIG 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. The additional recommendation has since been implemented and requires no further action.

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 "Pending."

In August 2008, OIG met with the PFIS DSO and was provided evidence that audit trails have been incorporated into the system and procedures for reviewing user activity were reviewed by auditors. 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