Assessment of the Implementation of the Federal Personnel/Payroll System (FPPS)

OIG Report Number 01-09-AIC

PURPOSE OF ASSESSMENT

The Office of Inspector General (OIG) conducted an assessment of the Agency's Federal Personnel/Payroll System (FPPS) implementation. This assessment was conducted as part of OIG's ongoing effort to evaluate the Agency's information systems as required by the *Government Information Security Reform Act*[1] *(GISRA), Public Law 106-398, Title X, subtitle G.*

SCOPE AND METHODOLOGY

The scope of the assessment included reviewing: (1) the various processes used by EEOC in the planning and implementation of FPPS; (2) the Office of Human Resources' FPPS data verification effort; and (3) the FPPS information system security features.

In order to make our final determinations we: (1) interviewed senior managers who are responsible for the system; (2) spoke with the members of the implementation team[2]; (3) obtained and reviewed implementation planning documentation; and (4) reviewed guidance, policies, and procedures regarding FPPS, as well as FPPS internal information security.

This evaluation was conducted in accordance with generally accepted government auditing standards, as published in the *Comptroller General's Government Auditing Standards, 1999 Revision through Amendment Three*. Our fieldwork was conducted during the November 2001 through August 2002 timeframe.

BACKGROUND

The Agency's previous personnel system, Personnel Information Resources Systems (PIRS), was scheduled to be retired by the General Services Administration (GSA) and was no longer to be supported after September 30, 2001.

---

[1] GISRA provides a comprehensive framework for establishing and ensuring the effectiveness of controls over information resources that support Federal operations and assets.

[2] The FPPS Implementation Team consisted of staff from the Office of Human Resources (OHR), Office of Information Technology (OIT), the Department of Interior's - National Business Center, and the Government Services Administration Payroll Center located in Kansas City, Missouri.

During the second quarter of FY2001, EEOC entered into a cross-servicing agreement with the Department of Interior's (DOI), National Business Center (NBC) to provide the Agency with human resource management information system support.[3] This agreement was borne out of the need to replace PIRS. According to DOI-NBC, the Federal Personnel and Payroll System (FPPS) is a modern, full featured, totally integrated system that meets or exceeds all mandatory and regulatory requirements established by the *President's Council on Management Improvement for Federal Automated Systems*; the *Paperwork Reduction Act*; and the *Joint Financial Management Improvement Program*. FPPS is hosted on the DOI-NBC mainframe computer located in Denver, Colorado. FPPS was developed using modern database and computer-aided software engineering technology, and was fully developed by December 1998.

The Agency completed its conversion to FPPS by September 23, 2001.

MANAGEMENT COMMENTS

No management comments were provided by either the Office of Human Resources (OHR) or the Office of Information Technology (OIT), the two Agency offices principally responsible for the FPPS conversion.

ASSESSMENT FINDINGS

No Significant Problems Occurred During the FPPS Implementation

During the course of this assessment OIG found no significant problems regarding the implementation of FPPS.

Our assessment included discussions with members of the FPPS Implementation Team to obtain an overall understanding of the implementation process, as well as to identify any lessons learned. Overall, the comments from those interviewed were highly positive regarding system implementation. According to DOI-NBC's FPPS Project Manager for EEOC, both OIT and OHR played an important role in the overall success of FPPS's implementation. The Project Manager noted that the implementation was one of the fastest and cleanest ever conducted by DOI-NBC.

[3]NBC provides automated human resource and payroll operations cross-servicing to DOI organizations, as well as a number of non-DOI agencies.

Furthermore, in an effort to ensure the integrity of the data being transferred, DOI-NBC conducted extensive parallel testing between PIRS and FPPS. The parallel testing overall found few discrepancies[4]. Those discrepancies identified were either corrected or addressed by DOI-NBC prior to data conversion.

Significant Progress Made in Data Verification

OIG found that OHR has made significant progress regarding the verification and correction of data being placed into FPPS.

As part of the Agency's implementation plan, the implementation team conducted a data verification review of PIRS data to ensure that only accurate information was entered into FPPS. OHR established a data verification task force whose responsibility was to identify and correct erroneous data.[5] At the onset of this task, OHR reported the following data discrepancies:

- 109 instances where address information needed to be verified;
- 41 other discrepancies (i.e. incorrect sex codes, tenure, and race codes);
- 169 instances where there were appraisal discrepancies;
- 453 instances where employees reported incorrect educational levels; and
- 379 instances where other types of changes were needed.

Total: **1151**

OHR completed this data verification and correction effort during the calendar year 2002.

FPPS Information System Internal Security Controls are Adequate

OIG found the internal information system security controls established by the Agency for FPPS to be adequate.

Although EEOC is not responsible for managing the FPPS computer mainframe security, the Agency does manage its own information access control and password assignment. Management of this process is controlled through OHR. Currently the Agency has over 800

[4]For example, one of the differences found between the two systems was how each system calculated state and local tax withholdings.

[5]OHR issued a memorandum to each employee, providing a copy of their personal data and requesting that they verify the information's accuracy and completeness.

employees who have access to FPPS for various purposes.

OHR has established a FPPS security team that is responsible for developing and maintaining user profiles for all users and resetting employee passwords. The security team has implemented the following policies:

- required office directors to send an email to the FPPS mailbox within 48-72 hours when a timekeeper, certifier, or releaser is no longer permitted to access the T&A System;

- employed a password reset policy which provides a more secure mechanism for requesting and receiving newly reset passwords via e-mail and;

- required office directors to complete an Assignment Designation Form, identifying the names of all employees who are responsible for processing time cards and/or Standard Form 52s, as well as completing an EEOC/DOI Mainframe Access Request Form for each authorized user.

Furthermore, we found that the FPPS security team has established specific user access levels and system access requirements for individuals who use FPPS. Upon our review of policies and procedures established by the National Institute of Science and Technology (NIST), it is OIG's opinion that the internal control security measures established by the Agency for system access provides the Agency with adequate FPPS information security.

However, during the course of our assessment, information was disclosed to us concerning the possible unauthorized access to sensitive FPPS information by employees of OIT. The question was raised, by OHR, as to whether it was appropriate for OIT employees to have access to sensitive data that resides in FPPS.

According to several members of the implementation team, OHR downloads several files bi-weekly that contain a detailed snapshot of all information that resides in FPPS. Information that is downloaded by OHR is generated by DOI-NBC and made available to agencies who are supported by DOI-NBC. Preservation of these downloads is critical because the information is overwritten each pay period and is non-recoverable. Once OHR downloads these files, the data files are placed in a file folder that resides on an Agency network server that services OHR and is only accessible to individuals in OHR and several individuals in OIT who are part of the FPPS Implementation Team. OIT is in the process of developing an Oracle database to maintain and allow access to this historical information. According to OIT, in order to develop and populate this historical database, access to the

downloads and subsequent access to sensitive data is necessary.

The Privacy Act [5 U.S.C. § 552a(b)] states that:

> *No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains,* ***unless disclosure of the record would be to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.***

OIG concludes that this "need to know" exception authorizes the intra-agency disclosure of a record for necessary, official purposes. Currently, access to this information is limited to those who have a need to know. Based on the "need to know" exception, OIT's access to FPPS data files, as part of their ongoing effort to develop other Agency information systems, is warranted and valid.

Not withstanding OIG's findings, the General Accounting Office (GAO) report, dated July 2001, *Information Security - Weak Controls Place Interior's Financial and Other Data at Risk*, stated that DOI-NBC did not adequately limit access granted to authorized users, control all aspects of the system software controls, or secure access to its network. The weaknesses identified in GAO's report affected the center's ability to: (1) prevent and detect unauthorized changes to financial information, including payroll and other payment data; (2) control electronic access to sensitive personnel information; and (3) restrict physical access to sensitive DOI-NBC financial and personnel information. GAO's report also stated that these weaknesses and risks also affect other agencies that use computer processing services at DOI-NBC. On March 15, 2002, DOI-NBC issued a memorandum to National Business Center mainframe clients regarding mainframe security changes. DOI-NBC initiated changes regarding:

- setting a sufficient password history retention length to disallow reuse of previous passwords;
- revocation of user IDs after 3 invalid password attempts;
- revocation of user IDs that have not been used in 90 days;
- changing the maximum interval between required changes to be no more than 60 days for all clients on all mainframe systems; and
- new password rules were developed for all mainframe systems.

OIG reviewed DOI-NBC's March 15, 2002, memorandum and compared it to password security guidance provided by NIST and the General Accounting Office (GAO). OIG found the new password controls established by DOI-NBC met guidelines established by NIST and should provide the Agency some added assurance of external information security.

Finally, OIG determined that the Agency had not conducted its own risk assessment as to the effectiveness of FPPS's security controls. *GISRA* requires that the Agency's Chief Information Officer, or comparable officer, ensure that the agency effectively implement and maintain information security polices, procedures, and control techniques. The CIO is responsible for:

> *"providing advice and other assistance to the head of the executive agency and other senior management personnel of the executive agency to ensure that information technology is acquired and information resources are managed in a manner that implements the policies and procedures of this division, as well as the priorities established by the head of the executive agency."*

Furthermore*, OMB Circular A-130, Management of Federal Information Resources* states that Agency's will:

> *"ensure that information is protected commensurate with the risk and magnitude of the harm that would result from the loss, misuse, or unauthorized access to or modification of such information*."

During fiscal year 2002, OIT had an outside contractor conduct and complete a risk assessment of FPPS in order to assess its security controls. Results from the risk assessment found no significant technology based information security concerns, however, the risk assessment identified the following internal control issues: (1) sensitive FPPS system access not being granted based on the user's job function; and (2) EEOC not documenting internal controls and operational requirements in an EEOC system security plan. OIT, as well as OHR, are currently in the process of addressing these issues.

CONCLUSION

It is OIG's opinion that FPPS has had a successful first year. The success of this

implementation is largely attributed to solid teamwork between all parties involved. OIG found no significant problems regarding FPPS's overall planning, its implementation, as well as its execution. Furthermore, during the year the Agency also made significant progress in completing its FPPS data verification effort.

Finally, in our opinion, the Agency has established acceptable internal controls to ensure that Agency data is properly secured and access limited only to authorized personnel.