Assessment of Information System Controls for the Foreign Service National Payroll System

AUD/FM-07-38

June 2007

~~**Important Notice**~~

~~This report is intended solely for the official use of the Department of State or any agency receiving the report directly from the Office of Inspector General. No secondary distribution may be made outside the Department of State or by other agencies or organizations in whole or in part, without prior authorization by the Inspector General. Public availability of the document will be determined by the Inspector General under the U.S. Code 5 U.S.C. 552. Improper disclosure of this report may result in criminal, civil, or administrative penalties.~~

Summary

The Office of Inspector General (OIG) contracted with Leonard G. Birnbaum and Company, LLP (LGB), an independent certified public accounting firm, to audit the Department of State's (Department) financial statements for FY 2006, in compliance with the Chief Financial Officers Act, as amended.[1] Office of Management and Budget Bulletin 06-03, *Audit Requirements for Federal Financial Statements*, requires that auditors assess the adequacy of the audited entity's internal controls, including those on automated systems processing financial data. In addition, the auditor must determine whether an agency complies with applicable laws and regulations.[2]

On behalf of LGB, Harper, Rains, Knight & Company, P.A. (HRK), performed an assessment of information system general controls for the Foreign Service National Payroll System (FSN Pay). This work also helped LGB determine whether the Department had complied with OMB Circular A-130,[3] which requires that all federal agencies establish automated information system security programs and describes the minimum requirements for those programs.

During its work, HRK concluded that FSN Pay had general information security controls in place, including physical security, to ensure that critical financial and operational data were maintained in a manner that ensured confidentiality, integrity, and availability. The Department had developed and documented formal operating procedures and guidelines for FSN Pay, including those related to access control, segregation of duties, incident response, and configuration/change management. The general controls for FSN Pay were sound and featured the concept of least privileged user access rights, which were monitored daily. FSN Pay personnel understood the key components of access control, segregation of duties, incident response, and configuration/change management. HRK found that the contingency plan in place at the Global Financial Services Center in Bangkok, Thailand (GFS/B), had not been tested.

Background

FSN Pay generates payments to all foreign national employees of the Department and to more than 40 other government agencies serviced by the Department. FSN Pay is currently processed at two locations, the GFS Center in Charleston, South Carolina (GFS/C), and in Bangkok. GFS/C and GFS/B are responsible for certain posts. They run independently, and each has a payroll processing group.

---

[1] Pub. L. No. 101-576.

[2] In addition to the financial statement audits, OIG performs separate work to determine whether the Department complies with the Federal Information Security Management Act (Pub. L. No. 107-347), which requires agencies to develop agencywide security plans.

[3] *Management of Federal Information Resources*, Appendix III, Security of Federal Automated Resources.

FSN Pay is a server-based system consisting of graphical user interface components, reporting components, and batch record processing components. Its capabilities include:

- processing bi-weekly payroll,
- calculating payroll,
- processing reports,
- reporting financial data,
- preparing and distributing payments and results,
- calculating exceptions, and
- capturing project costs.

FSN Pay data were stored in a file format known as Indexed Sequential Access Method (ISAM). The ISAM data were protected through a combination of controls, including application code controls, an internal application control file, and standard Windows permission. Permission to access the data and application programs is granted using a combination of login scripts and the application control file.

Objectives, Scope, and Methodology

The Department has numerous systems that provide financial or performance data that are used to prepare the annual financial statements. OIG and LGB identified more than 20 financial systems that are considered significant to the preparation of financial statements. LGB, in consultation with OIG, decided to perform cyclical reviews of these systems to comply with federal auditing requirements. The Government Accountability Office (GAO) agreed to this approach.

LGB chose to assess FSN Pay during the audit of the Department's FY 2006 financial statements. LGB used HRK to conduct the assessment of information system general controls of FSN Pay. HRK used the Federal Information System Controls Audit Manual, issued by GAO, as the basis for its assessment.

HRK interviewed key personnel who manage, modify, and use the FSN Pay application; assessed the logical and physical controls maintained for the FSN Pay application; and tested certain controls in GFS/C and GFS/B. It also reviewed policies and procedures related to FSN Pay, relevant technical documents, and reports produced by the system. HRK divided the assessment procedures into eight functional areas that are essential to the effective operation of the general information system environment.

- Security Program Planning and Management – Controls that provide the framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibility, and monitoring the adequacy of computer-related security controls.
- Access Control – Controls that limit and/or monitor access to computer resources (data, programs, equipment, and facilities) to protect against unauthorized modification, loss, and disclosure.

- Change Control – Controls that help prevent the implementation of unauthorized programs or modifications to existing programs.
- Authorization Control – Controls that ensure transactions are authorized and that unauthorized transactions are detected and removed.
- Completeness Control – Controls that ensure transactions are complete and outgoing data are reconciled.
- Accuracy Control – Controls that validate and edit transactions to prevent erroneous data entry.
- Segregation of Duties – Controls that constitute policies, procedures, and an organizational structure to prevent one individual from controlling key aspects of computer-related operations, thus deterring unauthorized actions or access to assets or records.
- Service Continuity – Controls that involve procedures for continuing critical operations without interruption when unexpected events occur.

OIG provided a copy of the draft report to the Bureau of Resource Management (RM) on March 21, 2007. RM's comments are included in their entirety as Appendix A.

Results

HRK conducted an assessment of information system controls related to FSN Pay and concluded that FSN Pay had general information security controls in place to ensure that critical financial and operational data were maintained in a manner that ensured confidentiality, integrity, and availability. However, HRK found that the contingency plan in place at GFS/B had not been tested.

Security Program Planning and Management

HRK concluded that the Department had an appropriate security program in place related to FSN Pay. FSN Pay had appropriate controls in place that provided for a continuing cycle of activity for managing security risks, developing security policies, and monitoring computer-related security. HRK found that security was an ongoing daily process that was communicated to all FSN Pay personnel. The Department corrected and reported on identified vulnerabilities using a Plan of Action and Milestones report. FSN Pay used security software to identify security incidents. It also had sufficient audit trail capabilities, and these capabilities were used appropriately. HRK found that the policies and procedures addressed security.

Access Control

HRK concluded that the Department had adequate access controls in place related to FSN Pay. FSN Pay had controls that limit and monitor access to protect against unauthorized modification, loss, and disclosure. HRK found that a standard access authorization form was used to approve the level of access. The Department periodically reviewed user access rights and had implemented adequate physical security controls. It also had a policy in place to secure computer terminals when they are not in use. HRK found that FSN Pay staff had implemented

the system using the concept of least privileges, meaning that staff had access only to the areas that they needed to perform their jobs.

Change Control

HRK concluded that FSN Pay had appropriate change controls in place to prevent the implementation of unauthorized programs or modifications to existing programs. The Department had developed policies and procedures related to this issue and had provided training to FSN Pay personnel. HRK found that standard software change request forms were in place, and they were tracked. The Department tested and authorized changes before the changes were allowed to be put in production. HRK found that all of the changes were tracked and that the different versions were controlled. In addition, the FSN Pay codes were protected through access controls.

Authorization Control

HRK concluded that FSN Pay had authorization controls in place to ensure that transactions were authorized and that unauthorized transactions were detected and removed. The Department compared all incoming data with master table data to identify erroneous data. HRK found that FSN Pay staff had corrected items included in the automatic error reports before final processing.

Completeness Control

HRK concluded that FSN Pay had controls in place to ensure that processed transactions were complete and that outgoing data were reconciled. The Department had implemented manual controls to reconcile data received from and sent to posts.

Accuracy Control

HRK concluded that FSN Pay had controls in place to validate and edit transactions to ensure accuracy and prevent erroneous data entry. The system applied edit and validation checks throughout the process. In addition, the Department had implemented additional manual controls to determine the reasonableness of data before processing. HRK found that erroneous data were captured in error reports and addressed before processing. HRK also found that the system produced standard reports that were reviewed for accuracy and reasonableness before processing.

Separation of Duties

HRK concluded that the Department had implemented appropriate separation of duties related to FSN Pay. HRK found policies and procedures in place that would deter unauthorized actions or access to assets or records by any one individual. In addition, the organization was structured in a way that ensured that distinct system functions were performed by different individuals. No one individual had complete control over incompatible transaction processing functions. HRK found that the job descriptions accurately reflected assigned duties and that personnel were aware of the importance of separating duties.

Service Continuity

HRK found that the Department had developed a Continuity of Operations Plan (COOP) that included FSN Pay. The Department reviewed and regularly updated its contingency plans, and personnel were aware of their roles and responsibilities. However, HRK found that GFS/B had not tested its COOP.

> **Recommendation 1:** Harper, Rains, Knight & Company recommends that the Bureau of Resource Management develop a plan to test the emergency response procedures, including critical systems, operations, and functions, at the emergency relocation site for the Global Financial Services Center in Bangkok. Harper, Rains, Knight & Company also recommends that the Bangkok Center obtain guidance from the Charleston Center on executing and coordinating these tests.

RM concurred with this recommendation and indicated that it tested the COOP for the FSN Pay system after the end of fieldwork. RM indicated that the test was successful. On the basis of RM's response, this recommendation is resolved, pending receipt of documentation related to the completion of this test.

United States Department of State
Assistant Secretary for Resource Management
and Chief Financial Officer
Washington, D.C. 20520

UNCLASSIFIED

MEMORANDUM

APR 3 0 2007

TO: OIG – Howard J. Krongard

FROM: RM – Bradford R. Higgins

SUBJECT: RM Response to the OIG Recommendation Regarding the Draft Audit - Assessment of Information Systems Controls for FSN Payroll

I endorse and am forwarding the comments contained in the attached response to the subject OIG correspondence.

Attachment: Memorandum dated April 9, 2007 OIG Draft Audit - Assessment of Information Systems Controls for FSN Payroll

Cleared:
P. Schlatter – RM/EX 04-11-07

UNCLASSIFIED

United States Department of State
Deputy Assistant Secretary
Global Financial Services
P.O. Box 150008
Charleston, SC 29415-5008
FAX: 843 579 5876

APR 0 9 2007

MEMORANDUM

TO: RM - Bradford R. Higgins

FROM: RM/GFS - James L. Millea

SUBJECT: Draft Audit – Assessment of Information System Controls for the FSN Payroll System (AUD/FM-07-XX)

We have reviewed the Office of Inspector General's draft audit report subject as above. The GFS response for recommendation 1 is provided below.

Recommendation 1: Harper, Rains, Knight & Company recommends that the Bureau of Resource Management develop a plan to test the emergency response procedures, including critical systems, operations, and functions, at the emergency relocation site for the Global Financial Services Center in Bangkok. Harper, Rains, Knight & Company also recommends that the Global Financial Services Center in Bangkok obtain guidance from the Global Financial Services Center in Charleston in executing and coordinating these tests.

Response: Concur. On November 3, 2006, RM/GFS Bangkok, in conjunction with RM/GFS Charleston conducted a test of FSN Pay systems located at the emergency Continuity of Operations Plan (COOP) relocation site at Charleston. A successful test was obtained of the complete functionality of the system.

GFS appreciates the opportunity to comment on the draft report. The operational point of contact is Janet Brooks. She may be reached by email brooksj2@state.gov or by phone at (843) 202-3858.