



AUDITOR GENERAL

WILLIAM O. MONROE, CPA



DEPARTMENT OF CORRECTIONS

INMATE BANK SYSTEM

Information Technology Audit

Summary

The Inmate Bank System, administered by the Department of Corrections, accounts for moneys received and disbursed for an inmate's personal use or benefit. Until October 2000, the Inmate Bank System was a Statewide application that ran independently at each of the Department's facilities. During October 2000, in an effort to accommodate budget restraints, according to the Department, this function was centralized, and, during our audit period, resided within the Department's Central Office, Bureau of Finance and Accounting.

Our audit of the Inmate Bank System for the period March 2003 through June 2003, and selected Department actions taken through July 2003, focused on evaluating selected information technology functions, and determining the effectiveness of selected general and application controls, including application system modifications, access to programs and data, user controls and controls over selected areas of input, processing, output, and manual follow-up. We also determined management's awareness of the Health Insurance Portability and Accountability Act of 1996 (HIPAA) legislation and what actions, if any, had been taken concerning this legislation. In addition, we determined whether the Department had corrected, or was in the process of correcting the access and reconciliation related deficiencies disclosed in audit report No. 03-022.

The results of our audit are summarized as follows:

Finding No. 1: Improvements were needed in the Department's program change control procedures with regard to documenting program changes in the client server environment.

Finding No. 2: The Department needs to improve its IT risk management practices and certain security controls protecting the Inmate Bank System.

Background

Florida law¹ provides that the Department may accept and administer as a trust any money received for the personal use or benefit of any inmate, deposit money so received in banks qualified as State depositories, withdraw any such money and use it to meet the current needs of the inmate as they may exist from time to time, and invest such moneys not required to be used for current needs of the inmate. The application used by the Department to record deposits and withdrawals of such moneys is named the Inmate Bank System, which is a hybrid mainframe and client server system. As of July 18, 2003, the system maintained a separate account for each of the 77,912 inmates. As of June 30, 2003, the composite total of inmate liability was \$6,252,669.

The Inmate Trust Fund serves as the depository for such moneys which are deposited into local bank accounts. Moneys received and deposited into an inmate's account are used primarily to purchase additional personal items for consumption or use

¹ Section 944.516(1), Florida Statutes

either from the prison-maintained canteens or approved catalogs. In addition, an inmate's account can be debited or credited for a number of other reasons including medical co-payments, postage, legal copies, disciplinary report expenses, or court costs; or for deposits received from individuals, PRIDE (Prison Rehabilitative Industries and Diversified Enterprises), or work release programs.

Until October 2000, the Inmate Bank System was a Statewide application and ran independently at each of the Department's facilities and separate bank accounts were established at each of the Department's seven service centers. To accommodate budget restraints, according to the Department, this function was centralized and, during our audit period, resided in the Department's Central Office, Bureau of Finance and Accounting.

Finding No. 1 Program Changes

Proper program change control procedures should require that documentation is maintained to evidence program change requests and associated approvals, to ensure that only authorized programs are moved into the production environment.

During our audit, we noted that, although the Department's procedures prescribed the use of a change request form to document the requested change and associated approvals in the mainframe environment, there were no similar procedures prescribed for program changes to the client server environment. Thus, for ten items tested within the client server environment, no documentation was available evidencing management approval before program movement into production. In addition, for the ten items tested, the audit trail was not adequate to associate the program change to the authorized program change request. In order to attribute the program change to its associated change request, one had to compare the new version of the program to the old one to determine what had been changed, and search the change requests in that timeframe to try to

identify which change request title seemed to match what was actually changed.

Failure to maintain adequate documentation of program changes may result in difficulty in ensuring that only authorized program changes are moved into production. Subsequent to our testing, the Department indicated that it had begun the process of accommodating the need for documentation in the client server environment, including the development of the eSystems Application/Module Promotion Request form and expansion of the Systems Development Standard for Program Reviews to include client server program modifications.

Recommendation:

The Department should continue its efforts to establish proper procedures for maintaining program change documentation and audit trails in its client server environment to help ensure that only authorized program changes are moved into production.

Finding No. 2 System Security

Security controls are intended to protect the integrity, confidentiality, and availability of information systems data and resources.

During our audit, we identified deficiencies in the Department's IT risk management practices and in certain security control features implemented by the Department. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising Department information. However, the appropriate Department personnel have been notified of the deficiencies.

Recommendation:

The Department, together with the State Technology Office, should enhance its IT risk management practices. Additionally, the Department should implement the specified security control features to enhance the safeguarding of Department IT resources.

Other Matters

Reconciliations

Our audit report No. 03-022, dated September 2002, disclosed that the Department had not performed bank statement-to-Inmate Trust Fund accounting record reconciliations for October 2000 through November 2001. At that time we reported that bank reconciliations had not been timely performed because of limited human resources and time consuming manual processes temporarily conducted during the centralization of the Inmate Bank System.

In the Department's Office of Inspector General's Six-Month Follow-up document, dated April 4, 2003, the Inspector General noted that though the Department had completed the monthly bank statement reconciliations for the Inmate Trust Fund through December 2002, there were still large unexplained differences.

During our audit, we noted that according to the Department, progress in explaining monthly bank and accounting record differences had been made by performing the reconciliations, however, unexplained differences remained. The Department had not yet determined whether the unexplained differences were the result of the conversion, an ongoing variance, or both. The reconciliation differences may be considered in a future audit.

Department Actions Concerning the Health Insurance Portability and Accountability Act of 1996 (HIPAA)

HIPAA² addresses the data interchange, privacy, and information security standards for personal health information. Pursuant to HIPAA, the United States Department of Health and Human Services has published regulations on electronic data interchange standards, privacy, and security. The final Transaction Rule, which contains electronic interchange standards, was incorporated as a Federal regulation and had a compliance date of October 16, 2002, but the deadline

may be extended to October 16, 2003, by filing an extension request. The final Privacy Rule was incorporated as a Federal regulation and compliance was required by April 14, 2003. The final Security Rule was incorporated as a Federal regulation and compliance is required by April 21, 2005. HIPAA also provides for civil and criminal penalties for noncompliance.

In response to our inquiry regarding the HIPAA legislation, the Department provided us with a letter from the Department's Office of the General Counsel dated July 10, 2003. This letter indicated that the Department was subject to and must comply with the HIPAA Rules. Additionally, information attached to a memo dated August 1, 2003, indicated that the Department had elected to manually fax requests for health care authorizations, a covered transaction under HIPAA, rather than sending them electronically via e-mail because converting Department IT systems to a HIPAA Transaction and Code Sets format would require substantial sums of money. The Department stated that it would continue to follow privacy and information security standards set forth by the HIPAA Privacy and Security rules. The Department's compliance with selected HIPAA Rules may be considered in a future audit.

Scope, Objectives and Methodology

The scope of this audit included an evaluation of selected information technology functions applicable to the system during the period March 2003 through June 2003, and selected Department actions taken through July 2003.

Our objectives were to determine the effectiveness of selected general controls over application system modifications and access to programs and data, and also application control activities over selected areas of input, processing, output, manual follow-up, and user control activities within the system. In addition, we were to determine management's awareness of the HIPAA legislation and what actions, if any, had been taken concerning this legislation, and determine

² Public Law 104-191

whether the Department had corrected, or was in the process of correcting, the access related deficiencies disclosed in audit report No. 03-022.

In conducting the audit, we interviewed appropriate Department personnel, observed Department processes and implemented procedures, and used various audit procedures to test selected controls related to the Inmate Bank System.

Authority

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.



William O. Monroe, CPA
Auditor General

Auditee Response

In response letters dated November 10, 2003, and November 6, 2003, the Department’s Secretary and the Chief Information Officer for the State Technology Office, respectively, generally concurred with our audit findings and recommendations. The Secretary’s and Chief Information Officer’s responses can be viewed in their entirety on the Auditor General Web site.

To promote accountability and improvement in government operations, the Auditor General makes audits of the information technology programs, activities, and functions of governmental entities. This information technology audit was made in accordance with applicable standards contained in Government Auditing Standards issued by the Comptroller General of the United States. This audit was conducted by William Tuck, CISA, and supervised by Tina Greene, CPA*, CISA. Please address inquiries regarding this report to Jon Ingram, CPA*, CISA, Audit Manager, via e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

This report and audit reports prepared by the Auditor General can be obtained on our Web site (<http://www.state.fl.us/audgen>); by telephone (850 487 9024); or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

*Regulated by State of Florida.



FLORIDA
DEPARTMENT of
CORRECTIONS

Equal Opportunity Employer

2601 Blair Stone Road • Tallahassee, FL 32399-2500
Phone: (850) 488-7480

Governor
JEB BUSH

Secretary
JAMES V. CROSBY, JR.

<http://www.dc.state.fl.us>
Fax: (850) 922-2848

November 10, 2003


Mr. William O. Monroe
Auditor General
State of Florida
G 74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

Pursuant to Section 11.45(4)(d), Florida Statutes, we have received the Preliminary and Tentative Findings of the Information Technology Audit of the Department of Corrections Inmate Bank System dated October 10, 2003. Enclosed please find our response to the findings.

If you have any questions, please call Scott McPherson at 410-4740.

Sincerely,


James V. Crosby, Jr.
Secretary

Enclosure

cc: JoAnne Leznoff
Scott McPherson
Rhonda Vause

**Department of Corrections
Inmate Bank System
Auditor General Information Technology Audit
Response to Findings**

Finding No. 1: Program Changes

Improvements were needed in the Department's program change control procedures with regard to documenting program changes in the client server environment.

Finding No. 1: Response

The Department's mainframe and client server environments differed in their use of a paper form to gather the signatures of development supervisors and the user. It was believed that the existing paperless approach provided an adequate audit trail to document and track the changes made to client server systems while the mainframe process also included a paper form. The paperless documentation for client server applications included the user request and final user approval of the Work Request recorded in the Service Level Agreement Tracking System (SLATS), and the specific changes to programming, the developer's identification and the date and time that the change was made recorded in Microsoft's Visual Source Safe (VSS). To remove the difference in the environments, on April 10, 2003, the eSystems Application/Module Promotion Request form and a review process were implemented. This provided an audit trail to include a review step and a paper form to document user and supervisor sign-off. In addition, at the same time the form was added, work control data including the SLATS Work Order number was added to the record of programming changes stored in VSS providing a link between changes and the user request in VSS, as well as, that contained in SLATS.

Finding 2: System Security

The Department needs to improve its IT risk management practices and certain security controls protecting the Inmate Bank System.

Finding 2: Response

The Department conducted its risk management practices in a way recognized by the State Technology Office as a best practice for the State of Florida and was instrumental in coordinating similar opportunities for the other agencies within the purview of the State Technology Office. Specifically, the Department has conducted annual updates and tests of its Disaster Recovery Plan and passed a risk assessment by TruSecure, a world-renowned cybersecurity company. The Department also retains TruSecure for Intrusion Detection monitoring and ongoing vulnerability assessments. As the Department is continually vigilant to improve its security controls, it is ever ready to use the standards and procedures provided by the State Technology Office, once they are released, to continue to implement improved risk management practices. In addition, the Department will eagerly work with the State Technology Office to research, establish and implement new standards, procedures and tools to improve security controls for all agencies within the State Technology Office.



JEB BUSH
Governor

TONI JENNINGS
Lieutenant Governor

KIMBERLY BAHRAMI
Chief Information Officer



November 6, 2003

Mr. William O. Monroe, CPA
Auditor General
State of Florida
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Mr. Monroe:

Pursuant to Section 11.45(4)(d), Florida Statutes, below is the response to your report of the of the *Department of Corrections, Inmate Bank System, for the period March 2003 through June 2003, and selected Department actions through July 2003*. Our response corresponds with your findings and recommendations.

Finding No. 2:

The Department needs to improve its IT risk management practices and certain security controls protecting the Inmate Bank System.

Response:

The STO concurs with the finding. The STO has implemented cost-effective security controls to minimize the risk to the Department of Corrections through vulnerability assessments to the information technology infrastructure. Additionally, the STO in coordination with the Department has continued to monitor the information technology infrastructure to identify threats and mitigate risk to the system.

If further information is needed concerning any of our responses, please contact Gerry York at 850-410-1698.

Sincerely,

Kimberly Bahrami
Florida Chief Information Officer

Cc: Steve Rumph, Department of Management Services, Inspector General

4030 Esplanade Way
Suite 115
Tallahassee, Florida 32399-0950

Phone 850.410.4777
Fax 850.922.5162
<http://www.MyFlorida.com>