AUDITOR GENERAL

DAVID W. MARTIN, CPA

DEPARTMENT OF CORRECTIONS

OFFENDER BASED INFORMATION SYSTEM

Information Technology Audit

SUMMARY

The Offender Based Information System (OBIS) is maintained by the Department of Corrections (Department) for the joint use of the Department and the Parole Commission. The Department uses OBIS to record data, generate reports, and support its decisions in the daily management of more than 96,000 inmates and 156,000 offenders supervised in the community as of February 2008. The Department relies upon OBIS to track every aspect of an offender's life cycle, from inmate intake to management during the court-ordered sentence, through post-release supervision. In addition to being used by the Department for internal management, data in OBIS is used by Statewide law enforcement and criminal justice entities to serve public safety. Our audit of OBIS focused on evaluating information technology (IT) controls for the period November 2007 through April 2008.

The results of our audit are summarized below:

Finding No. 1: Certain Department security controls applicable to OBIS needed improvement.

Finding No. 2: Contrary to Section 119.071(5)(a), Florida Statutes, the Department used certain employee social security numbers (SSNs) without specific authorization in law or without having established the imperative need to use the SSN for the performance of its duties and responsibilities as prescribed by law.

Finding No. 3: The Department lacked effective procedures for addressing data exchange errors generated during the upload of inmate data during inmate reception processing.

Finding No. 4: Aspects of the Department's application controls within OBIS needed improvement. We are not disclosing specific details of the issues in this report.

Finding No. 5: The Department's information security program needed improvement to document, in a more comprehensive manner, management's expectations for safeguarding IT resources.

Finding No. 6: Program change controls for OBIS needed improvement.

Finding No. 7: Quality control reviews for application changes and the subsequent moving of program changes to production were performed by staff who were not organizationally independent of the programming staff.

Finding No. 8: The Department had not designated positions of special trust and had not performed adequate background checks, including fingerprinting, of contractors and some employees occupying positions with sensitive IT responsibilities and access privileges.

Finding No. 9: The Department lacked a formal management review process to ensure that inmate gain time adjustments were uniform throughout the Department.

BACKGROUND

According to Section 20.315, Florida Statutes, the purpose of the Department of Corrections (Department) is to protect the public through the incarceration and supervision of offenders and to rehabilitate offenders through the application of work, programs, and services. The Department's mission is to protect the public safety, to ensure the safety of Department personnel, and to provide proper care and supervision of all offenders under its jurisdiction while assisting, as appropriate, their reentry into society.

According to the Department's February 2008 Monthly Status Report, the inmate population was 96,132 and another 156,223 offenders were under community supervision. Inmates are housed in 137 correctional facilities consisting of 60 major institutions, 41 work camps, 30 work release centers, 1 treatment center, and 5 road prisons throughout the State.

The Offender Based Information System (OBIS) is the daily operations support tool and the main repository of day-to-day and historical data on offenders supervised by the Department. The Department's Office of Information Technology (OIT) maintains OBIS. OBIS has been the primary system and official data repository used by the Department since 1981 to manage information on active inmates and offenders on community supervision pursuant to Section 20.315(10), Florida Statutes, requiring the Department to maintain only one offender-based information and records system for the joint use of the Department and the Parole Commission. Offender data is initially entered into the Computer Assisted Reception Process System (CARP), which is used at the five inmate reception processing centers throughout the State. CARP data is transmitted periodically to OBIS to establish a permanent record on each offender. Some of the most critical OBIS functions include collecting and analyzing data during inmate reception processing; calculating complex offender sentences; and managing information on inmate and offender location, education, behavior, medical care, disciplinary actions, vocations, training, visitors, and progress in rehabilitation.

OBIS supports three main business processes within the Department: Institutions, Health Services, and Community Corrections. The Office of Institutions manages inmates and is composed of three core processes: receiving and processing new inmates, supervising inmates, and releasing inmates. The Office of Institutions uses OBIS data to manage inmate reception, classification, sentence structure, banking, work programs, transfers, incident management, and release. The Office of Health Services manages medical care, mental health, and dental care of inmates and offenders. The Office of Health Services uses OBIS to collect and record selected information about an inmate's or offender's health record. The Office of Community Corrections supervises offenders released in the community and uses OBIS data on a daily basis to manage offenders throughout their parole and probation period. Offenders are supervised at a level commensurate to their risk classifications and supervision types and report for supervision daily, weekly, monthly or as directed by the sentencing authority.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Security Controls

Security controls are intended to protect the integrity, confidentiality, and availability of information systems data and resources. Effective security controls include access controls that are intended to ensure that users have only the access privileges needed to perform their duties, that access to sensitive resources is limited to only a few users, and that users are restricted from performing incompatible functions. Access controls include the use of individual user identification codes (IDs) and passwords to allow for attributing user activities to the responsible user. Effective access controls further include a periodic review to confirm the appropriateness of user access rights to help

reduce the risk of errors, fraud, misuse, or unauthorized alterations. Access controls are further enhanced when emergency and temporary access authorizations are automatically terminated after a predetermined period.

Our audit disclosed deficiencies in certain security controls protecting OBIS and related IT resources. Specifically:

- Five of seventy-two users with update access privileges to inmate classification within OBIS and included in our test retained access privileges for the classification supervisor profile for temporary assignments beyond the time frame necessary. The Department did not remove these access privileges, thereby allowing access privileges that were greater than necessary for the users' regular job duties and increasing the risk of unauthorized updates to OBIS data. In response to audit inquiry, Department staff indicated that the temporary access granted to these five users would be removed.

- Two of thirty users who had update access privileges to inmate classification did not appear to require access based on their current job responsibilities. In one of the instances, the Department did not remove access privileges for one user who had changed positions within the Department. Subsequent to audit inquiry, the Department determined that the second instance occurred when the user was given update access privileges to inmate classification by mistake. Under these conditions, the risk of unauthorized updates to inmate classification data was increased. In response to audit inquiry, Department staff indicated that the inappropriate access privileges would be removed.

- Although the Department had policies and procedures requiring the removal of user access to OBIS within three days after termination, 21 of 48 employees who terminated employment between January 1, 2007, and December 31, 2007, did not have their OBIS access removed in a timely manner. Under these conditions, the risk is increased of unauthorized access to OBIS data through the misuse of the former employees' access privileges. The number of days between the termination dates and the dates that the access IDs were suspended ranged from 4 to 412 days. As of March 11, 2008, one of the access IDs remained active. Three of the forty-eight former employees included in our test had their access IDs used after their termination dates. The number of days between the termination dates and the dates that the access IDs were last used ranged from 5 to 20 days. The Department was unable, upon audit inquiry, to timely determine what activities were performed with the access IDs after the employees' termination dates.

- Several computer users within OIT had access privileges to OBIS that were not necessary based on their job responsibilities, increasing the risk of inappropriate and unauthorized system actions. Specifically:

  - Three users outside of the Database Administration Section had database access privileges. In addition, the same three users had access privileges to the data utility, FILE-AID, that allowed individual data elements within a production data set to be modified.

  - Two users (a network administrator and a security administrator) had access privileges to the application programming profiles.

  - Three staff working in the Research and Data Analysis group had access privileges to the application programming profiles.

  - Three Help Desk staff and one network administrator staff had access privileges to the operator profiles.

- Certain Department security controls related to OBIS and the supporting network environment, in addition to the issues described above, needed improvement. Specific details of these deficiencies are not disclosed in this report to avoid the possibility of compromising OBIS data and IT resources. However, appropriate Department personnel have been notified of the specific deficiencies, which are summarized below:

  - Group user IDs were being used to manage some of the Department's network resources. The absence of strong user ID and password controls whereby each user is assigned a unique user ID and password increases the risk

that the Department will not be able to trace user activities to the responsible individual.

- The Department's monitoring of network firewall changes needed improvement to provide increased assurance that the firewall will operate as intended.
- Physical access to the computer data center was not always effectively restricted, increasing the risk of unauthorized access to the data center.
- The Department's processing of off-site backup tapes of OBIS data needed improvement to provide stronger protection of confidential and sensitive information.
- Some network password controls needed improvement to provide increased assurance of password confidentiality.
- Confidential and sensitive information was not adequately protected during transmission to outside entities.

Recommendation: The Department should improve security controls in OBIS to ensure that temporary and terminated user access is timely revoked and that access to computer resources is appropriate based on job responsibilities. The Department should also strengthen user ID and password controls and ensure that appropriate network barrier and transmission controls are in place. Additionally, the Department should effectively restrict physical access to the data center and improve controls to protect confidential and sensitive information contained on backup tapes of OBIS data.

Finding No. 2: Use of SSNs

Section 119.071(4)(a), Florida Statutes, provides that all employee SSNs held by an agency are confidential and exempt from public inspection. Pursuant to Section 119.071(5)(a)2.a., Florida Statutes, an agency shall not collect an individual's SSN unless the agency has stated in writing the purpose for its collection and unless the agency is specifically authorized by law to do so or it is imperative for the performance of that agency's duties and responsibilities as prescribed by law.

The Department collected and used certain employee SSNs in OBIS. No specific authorization existed in law for the Department to collect the SSNs of OBIS users and the Department had not established the imperative need to use the SSN, rather than another number. Although requested, written documentation stating the purpose for collecting and using employee SSNs was not provided. The use of the SSN is contrary to State law and increases the risk of improper disclosure of SSNs.

Recommendation: The Department should comply with State law by clearly establishing why the use of employee SSNs is imperative for the Department to perform its duties and responsibilities or alternatively establish another number to be used rather than the SSN.

Finding No. 3: Data Exchange Exception Reporting

Effective exception reporting procedures allow erroneous transactions to be identified without disruption of other transactions. The periodic review of exception reports and prompt follow-up on exceptions increase management's assurance that erroneous actions taken through a computer system, should they occur, will be timely detected and corrected.

Our audit disclosed that, although data exchange errors were generated online when inmate data entered in CARP did not upload correctly to OBIS, data exchange errors and inmate data were automatically deleted after seven days if not addressed by Department staff. Effective procedures for the review of data exchange errors did not exist to ensure that errors were corrected within seven days. Without effective procedures for the review of data exchanges, there is an increased risk that inmate data entered during the inmate reception process in CARP will not be transmitted to OBIS.

Recommendation: The Department should address the timely monitoring of data exchange errors.

Finding No. 4:
Application Controls

Our audit disclosed certain aspects of the Department's application controls within OBIS that needed improvement. Specific details of these deficiencies are not disclosed in this report because of the sensitive nature of the information. However, we have notified appropriate Department management of the specific issues. In these circumstances, there is an increased risk of inappropriate system actions not being detected in a timely manner.

Recommendation: The Department should improve OBIS application controls to allow for the timely detection of inappropriate or unnecessary system actions.

Finding No. 5:
Security Program

An entitywide program for security planning and management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. The program establishes a framework and continuing cycle of activity for assessing risks, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Security programs typically include appropriate security policies and controls to mitigate identified risks, classify information resources, designate positions of special trust, and promote security awareness. The Department had addressed many of the IT security elements necessary for a successful entitywide security program in the form of Department policies. However, important aspects of a well-designed security program were not addressed, increasing the risk that management's expectations for information security may not be clearly understood and that security controls may be inadequate or inconsistently applied. Specifically:

- The Department had not implemented a security awareness training program. The Department had a draft security awareness procedure and had developed security awareness training modules; however, neither the procedure nor the training modules had been implemented as of April 2008. In addition, documentation of employee acceptance of Department security policies as required by Department Procedure 206.007, User Security and Information Systems, was not available.
- The Department did not have an ongoing documented program for risk management. Specifically, no policies and procedures existed for periodic risk analysis for critical information resources or for a comprehensive risk analysis after major changes in software, procedures, environment, organization, or hardware.
- The Department did not have a policy or procedure for classification of OBIS data as confidential, sensitive, or public. Also, our audit disclosed instances of confidential data that were not adequately restricted. Specific details of these instances are not disclosed in this report to avoid the possibility of compromising the confidentiality of data protected by State law. Furthermore, the Department did not have a policy addressing the disposal of confidential information resources, including confidential data residing on personal computers.

Recommendation: The Department should continue its development of an entitywide security program. Appropriate security policies and procedures should be implemented to mitigate the identified risks and support the confidentiality, availability, and integrity of information resources. Management should also promote security awareness through adequate training programs.

Finding No. 6:
Program Change Controls

Effective controls over program changes are intended to ensure that all requests for changes are standardized and subject to formal change management procedures, including a tracking and reporting system for keeping change requestors and stakeholders up to date about

the status of changes to the application. Program change controls include procedures to ensure that all changes are properly authorized, tested, and approved for implementation and that access to and distribution of programs are carefully controlled. Additionally, the approval and periodic updating of written policies and procedures for system development and program changes are important to ensure that the related activities are performed as management intended.

Our audit disclosed aspects of the Department's program change controls applicable to OBIS that needed improvement to demonstrate consistent compliance with Department policy and appropriate program change control practices. In our test of 38 OBIS program changes on 31 work orders, we noted:

- One change for which an authorized user of OBIS did not initiate the change request. The change was requested by OIT staff instead of an authorized user from the program area, contrary to Department policy.
- Eight changes where evidence of programmer testing prior to moving the change into the production environment was unavailable, contrary to Department policy.
- Ten changes that lacked evidence of user testing and approval, contrary to Department policy.
- Eight changes that lacked required OIT management and quality control approvals, contrary to Department policy.
- Two changes for which the quality control staff who moved the program into the production environment also made the program change. This combination of duties and access privileges was contrary to an appropriate separation of duties.
- One change for which the log within the library management system did not record information as to who moved the change into the production environment, thus the move could not be attributed to the responsible person.
- The work order status was not closed upon completion of the change request for 13 of the 31 work orders tested, contrary to Department policy and limiting the accuracy of the work order status. Additionally, in these circumstances, there is an increased risk that work orders left open may be reused for other changes not documented in the work order description.

Our audit procedures related to program change controls disclosed additional areas that needed improvement. Specifically:

- No supervisory review existed to ensure that required approvals were in place prior to moving changes into the production environment or to ensure that each program that had been moved into the production environment had proper supporting documentation. Under these conditions, the risk is increased that unauthorized program changes will be implemented in the production environment.
- A test environment for user acceptance testing that mirrors the production environment did not exist. Absent a test environment that emulates the future environment in which the system will operate, the risk is increased that programs that would not function properly in the production environment will not be detected and corrected during program testing.
- Although Department Standard Operating Procedure (SOP-AD-001) required biannual reviews of standards, the following standards and manuals were outdated: the Standard for Programming Reviews, the Standard for Software Testing, and the Application Development Reference Manual (ADRM). Additionally, the ADRM, the Information System Development Methodology manual, the Request Tracking Process Procedure, and the Standard for Programming Reviews did not reflect current practices for the implementation of program changes and, in some instances, referenced obsolete positions within OIT. Additionally, although these documents addressed most aspects of the control process, the documents did not fully address the use of the library management system by programmers, managers, and quality control staff. The absence of current written program change control procedures increases the risk that program changes will not be made in a manner consistent with management intent.

Recommendation: The Department should implement improved change controls to ensure that program modifications are properly authorized, tested, and approved. The Department should also ensure that its written system development and program change control procedures are complete and reflect current Department practices.

Finding No. 7:
Quality Control Organizational Placement

Effective program change control procedures include controls to ensure that the movement of programs among program libraries is controlled by an organizational segment that is independent of both the user and the programming staff. Separating this function from user and programming staff maximizes the objectivity and independence and enables sufficient authority to monitor compliance with change management policies and procedures.

At the Department, programs were moved into the production environment by the quality control staff located within the OIT, Bureau of Systems Development. Quality control staff reported directly to an OIT, Bureau of System Development, Data Processing Manager responsible for OBIS application development. The Data Processing Manager was responsible for monitoring both application programmers and quality control reviews that included moving changed programs into the production environment. Without independent oversight of quality control reviews and the movement of changes to the production environment, the potential exists for quality control staff to be influenced by management responsible for application development, increasing the risk of unauthorized changes being moved into the production environment.

Recommendation: The Department should review the placement of the quality control function within the OIT, Bureau of Systems Development and reposition this function to strengthen its independence and authority.

Finding No. 8:
Positions of Special Trust

Section 110.1127(1), Florida Statutes, provides that each employing agency shall designate those employee positions that, because of the special trust or responsibility or sensitive location of those positions, require that persons occupying those positions be subject to a security background check, including fingerprinting, as a condition of employment. Section 435.04(1), Florida Statutes, provides that all employees in positions designated by law as positions of trust or responsibility shall be required to undergo security background investigations referred to as level 2 background screenings as a condition of employment and continued employment. The level 2 background screenings are to include fingerprinting for all purposes, Statewide criminal and juvenile records checks through the Department of Law Enforcement, and Federal criminal records checks through the Federal Bureau of Investigation. Section 435.05(1)(a), Florida Statutes, provides that every person employed in a position for which an employment screening is required must, within five working days after starting to work, submit to the employer a complete set of information necessary to conduct a screening under this section.

The Department had not established a written policy for designating positions of special trust. Although the Department had a policy dated in 1959 requiring all employees to be fingerprinted upon appointment, the policy did not contain specific procedures for processing background checks, including the time frame for processing. Although it was the Department's practice to fingerprint all new employees within two weeks of employment, our audit disclosed 2 of 21 employees included in our test who did not have level 2 background screenings with fingerprints on file as of February 5, 2008. These two employees had been with the Department for over five years. Subsequent to audit inquiry, Department staff indicated that level 2 background screenings have now been conducted on the two employees.

Additionally, the Department did not require level 2 background screenings for contractors. According to Department staff, some contractors were subject to employment background screenings; however, the Department did not have a centralized repository for tracking contractor background checks and was unable to provide documentation of such background screenings performed. According to Department staff, screenings for contractors were conducted using the Florida Crime Information Center and the National Crime Information Center systems. However, fingerprinting of contractors was not conducted as required for level 2 background screenings. By not designating positions of special trust and not ensuring that contractors were appropriately screened, the risk is increased that a person with an inappropriate background could be employed in a position of special trust or as a contractor.

Recommendation: The Department should define positions of special trust and update its policies and procedures to specify the processing requirements and time requirements for conducting level 2 background screenings. Additionally, the Department should conduct periodic reviews of personnel records to ensure that all security background checks are completed. Furthermore, the Department should take measures to ensure that contractors in positions of special trust are screened to the level 2 requirement, including fingerprinting. The Department should develop a centralized repository for tracking contractor background checks to ensure that contractors are screened prior to gaining access to sensitive information and information systems.

Finding No. 9:
Gain Time

Sections 944.275 and 944.278, Florida Statutes, and Department of Corrections Rule 33-601.101, Florida Administrative Code, set forth incentive gain time eligibility requirements for inmates. Specifically, gain time is utilized by the Department as a management tool to encourage satisfactory inmate behavior, provide incentive for inmates to participate in productive activities, and to reward inmates who perform outstanding deeds or services. Gain times are a means whereby eligible inmates may reduce the amount of time served on their sentences subject to certain parameters established by State law.

A matrix within OBIS was used to automatically calculate base gain time awards for each inmate monthly. Additionally, an inmate's base gain time award could be adjusted up or down each month depending on the inmate's behavior at the institution, based on security, work, and program evaluations. Once gain time awards were entered into OBIS, there was no formal review by management to ensure that discretionary gain time awards had been made in accordance with established State law. Absent a formal management review process to ensure that a uniform approach was used for awarding discretionary gain time and modifying suggested matrix base gain time awards, the Department's ability to demonstrate the fairness and reasonableness of adjustments to inmate sentences may be hindered.

Recommendation: The Department should establish a formal review process to ensure that discretionary gain time award guidelines are being followed.

OBJECTIVES, SCOPE, AND METHODOLOGY

The objectives of this IT audit were to determine the effectiveness of selected general and application controls relating to OBIS.

The scope of our audit focused on evaluating selected IT controls applicable to OBIS during the period November 2007 through April 2008.

This IT audit was conducted in accordance with applicable Generally Accepted Government Auditing Standards. In conducting our audit, we interviewed appropriate Department personnel, reviewed policies and procedures and other applicable documentation, observed processes and procedures, used computer-assisted audit techniques, and performed various other audit procedures to test selected controls related to OBIS.

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 IT audit.

David W. Martin, CPA
Auditor General

MANAGEMENT RESPONSE

In a letter dated September 11, 2008, the Secretary provided a response to our preliminary and tentative findings. This letter is included at the end of this report as APPENDIX A.

This audit was conducted by Brenda Shiner 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 other audit reports prepared by the Auditor General can be obtained on our Web site (http://www.myflorida.com/audgen/); by telephone (850) 487-9024; or by mail (G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450).

THIS PAGE INTENTIONALLY LEFT BLANK

APPENDIX A

MANAGEMENT RESPONSE

FLORIDA
DEPARTMENT of
CORRECTIONS

Governor
CHARLIE CRIST

Secretary
WALTER A. McNEIL

An Equal Opportunity Employer

2601 Blair Stone Road • Tallahassee, FL 32399-2500

http://www.dc.state.fl.us

September 11, 2008

The Honorable David W. Martin, CPA
Auditor General
Office of the Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

RE: Preliminary and Tentative Audit Findings, Information Technology Audit of the Department of Corrections, Offender Based Information System (OBIS), for the period November 2007 through April 2008.

Dear Mr. Martin:

We have reviewed the preliminary and tentative findings and recommendations included with your letter dated July 10, 2008. As required by Section 11.45(4)(d), Florida Statutes, our response is attached.

This response reflects the specific action taken or contemplated to address the deficiencies cited.

Thank you for your continued cooperation and presentation of recommendations for the improvement of our operations.

Sincerely,

Walter A. McNeil
Secretary

WAM/PD/ps
Attachment
Cc: Richard Prudom, Chief of Staff
Richard D. Davison, Deputy Secretary
Gene Hatcher, Chief Information Officer
Ralph Kiessig, Director of Human Resource Management
George Sapp, Assistant Secretary of Institutions
Franchatta Barber, Deputy Assistant Secretary of Institutions
Mary Huff, Assistant Chief of Personnel
Paul C. Decker, Inspector General

FLORIDA DEPARTMENT OF CORRECTIONS
RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS
INFORMATION TECHNOLOGY AUDIT OF THE DEPARTMENT OF CORRECTIONS, OFFENDER BASED INFORMATION SYSTEM (OBIS), FOR THE PERIOD NOVEMBER 2007 THROUGH APRIL 2008.

Finding 1:

The Department's security controls protect the integrity, confidentiality and availability of OBIS data as well as all other systems in its charge. OBIS data is depended upon by law enforcement agencies throughout the state to ensure public safety. The confidentiality of OBIS data is rigorously maintained. The Office of Information Technology's (OIT) Information Security Administration section depends on the submission of an electronic Security Access Request Form (SAR) when any change in employee status occurs that may affect system security. Every case identified by the audit where access did not match employee status was due to a SAR not being submitted. The Department will improve the SAR component of the security access process by way of internal periodic audits and end user awareness training.

The Department maintains a secure network with multiple layers of protection and detection facilities. The network and all of its components operate as designed and intended. The network resources managed by a unique group ID were redefined to unique individual IDs as suggested by the audit. The Department's firewall changes are managed by the change management process that ensures management review and approval of all changes to the Department's computing infrastructure. Additional controls recommended by the audit were implemented.

The Department's data center is secured by multiple layers of security and as such is rigorously managed. Additional controls recommended by this audit were implemented.

Off-site backup tape storage is in accordance with state policy and consistent with the approach of other state public safety agencies. This process will be reviewed for improvement according to audit findings.

Information transmitted to external entities is currently under review for encryption requirements and will be resolved to conform to all regulatory requirements.

Finding 2:

The Department currently has no suitable substitute for the SSN required to positively identify an individual, including the thousands of state employees and thousands of contract employees, requiring access to departmental systems. However, the Department will review options for replacing this identifier with a substitute of equivalent reliability commensurate with the value of departmental data. This change will be a substantial effort for the Department. In the interim, the standard departmental disclaimer statements regarding purpose of collection and exclusive use will be included on the security access request form.

Finding 3:

The Department agrees with Finding 3 relating to the data exchange errors between CARP and OBIS. We are currently in the process of moving our reception processing from the Computer Assisted Reception Process (CARP) to our Offender Based Information System (OBIS). Once completed, this item will become moot as there will be no data exchange between CARP and OBIS.

The Office of Information Technology will institute a monitoring process to ensure that any data exchange errors are corrected within seven days to complement the controls already in place that ensure reception data integrity.

Finding 4:

The Department will implement additional control processes to further detect and prevent inappropriate or unnecessary system actions.

Finding 5:

The Department's Bureau of Staff Development is reviewing the security awareness training developed and submitted by OIT. Once approved, this training will be a required module for all departmental employees and contractors.

The Department is working with the state information security office to formalize certain documentation with respect to the Department's overall information security program including a risk assessment.

The Department is currently developing a data classification process for adoption as soon as possible. The Department utilizes the industry standard Department of Defense method of destroying and disposing of confidential data residing on personal computers. This practice will be formally defined by departmental policy.

Finding 6:

The Department manages requests for modifications and enhancements to OBIS utilizing structured processes and industry standard management tools and practices. Pre-approval processes exist to ensure that only quality control staff moves programs into the production environment. System changes are tested by the Systems Development staff and the requestor prior to promotion to production. Utility programs do not require the same rigor as functional programs in terms of end user testing. All OBIS changes are managed by an industry standard library management system. OIT management reviews and approves changes to the system prior to promotion to production. The quality control process dictates that no program can be promoted to production without an associated valid work order. Work orders defining program changes are discreet units of work, however, if multiple work orders involve modifications to a single program those work orders are tested, approved and promoted to production singularly.

The Department will update its process documentation to reflect current practice and identified improvements per audit recommendation. The new process documentation will be submitted to the Department's Bureau of Policy for oversight and update management to ensure perpetual review.

The Department will review its test development and user acceptance test environments for improvement in frequency of refresh per audit recommendation. Additionally, the Department will consider additional application controls.

Finding 7:

The quality control function was relocated organizationally to report to the Bureau of Service Delivery in the same section as the change management process as opposed to the Bureau of Systems Development per the audit recommendation.

Finding 8:

The Department concurs it should define positions of special trust to include all employees of the Department of Corrections (the agency has not limited background checks to specific positions). The Department currently performs background checks (FCIC/NCIC) on all employees prior to hiring and subsequently follows up with fingerprinting of all new hires. We will formalize our business practice by updating our procedures and adding timeframes. As noted in your findings, there were 2 issues identified in which documentation was lacking. In one instance, the employee was a re-hire who had been gone for a short period; however, the initial background screening was done and subsequent background screening was completed. In the other instance, there was a copy of a fingerprint card that had been sent to FDLE; however the file was lacking documentation of the results.

NOTE:
Effective January 1, 2007, FDLE required that all certified officers (Correctional Officers and Correctional Probation Officers) be fingerprinted electronically. In addition, the Department of Corrections is using electronic fingerprinting for all employees hired after that date.

The Office of Information Technology has always required criminal background checks through FCIC and NCIC for contract personnel; however, fingerprinting of all new contract personnel is now required as well. The Office of Information Technology is currently working with the Office of Personnel to fingerprint all existing contract personnel who previously passed the FCIC/NCIC background checks per audit recommendation.

Finding 9:

The Department acknowledges finding is accurate. Approximately 200,000 individual gain time decisions are made each month. This number accounts for the fact many inmates are sentenced under several different gain time laws, requiring multiple gain time decisions to be made for these inmates. The Department uses an automated rating matrix in an attempt to ensure that the gain time awards made each month are consistent with rules and policy. This automated matrix ensures that all inmates with the same ratings will receive the same base gain time award. Staff then uses the base gain time award from the automated matrix to make individual gain time decisions based on their knowledge of the inmate. Staff's knowledge of the case may result in the base award being aggravated or mitigated up to four days so long as the final award does not exceed the maximum allowable by law or is below zero. The criteria for aggravation and mitigation are established in rule for uniform application.

As staffing and funding becomes available the department will consider a means to address this finding.

THIS PAGE INTENTIONALLY LEFT BLANK