Follow-up of the Office of the Auditor General's Report 2009-011
OFFENDER BASED INFORMATION SYSTEM
Information Technology Audit
Audit Report #A09015F

March 27, 2009

State of Florida
Department of Corrections
TO: Walter A. McNeil  
Secretary

FROM: Walt Murphree  
Interim Inspector General

DATE: March 27, 2009


The Bureau of Internal Audit performed a follow-up audit to the Office of the Auditor General’s Department of Corrections, Offender Based Information System Information Technology Audit, Report # 2009-011, issued in September 2008. The objective of this follow-up was to determine the corrective actions taken on reported audit findings and whether actions taken achieved the desired results as intended by management. The scope of our follow-up consisted of obtaining from the Office of Information Technology, Institutions, and Human Resource Management a written response of actions taken to correct reported findings. The follow-up response was then evaluated to determine if management’s actions were adequate and timely. We have evaluated the response to each finding and have assessed that appropriate action has been taken or is being taken to address the issues identified in the report. No further follow-up is necessary for this audit.

[Signature]
Interim Inspector General

WM/PS/ps
Attachment
Richard D. Davison, Deputy Secretary
Bonnie Rogers, Chief of Staff
Gene Hatcher, Chief Information Officer
George Sapp, Deputy Secretary for Institutions and Re-entry
Glory Parton, Director of Human Resource Management
Terry L. Shoffstall, Director of Joint Legislative Auditing Committee
BACKGROUND

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. The Office of the Auditor General's audit of OBIS focused on evaluating information technology (IT) controls for the period November 2007 through April 2008.


OBJECTIVES

Our follow-up objectives were to determine:

- what corrective actions were taken on reported audit findings, and
- whether actions taken achieved the desired results as intended by management.

SCOPE AND METHODOLOGY

A request was made to the Office of Information Technology, Institutions, and Human Resource Management for a written response on the status of corrective actions taken.

RESULTS OF FOLLOW-UP

Finding 1: Certain Department security controls applicable to OBIS needed improvement.

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.
Management’s Original Response: 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.

Management’s Follow-Up Response: The Department notified the Security Coordinators in early January 2009 reminding them of their responsibility to monitor the SAR process. The information security group continues to review this process on a monthly basis to ensure all users are current.

The Department’s firewall changes are managed by the OIT change management process that ensures management review and approval of all changes to the Department’s computing infrastructure. Additionally, network managers monitor firewall logs for changes weekly as well as a separate word document is kept of all changes on a shared network drive.

Quarterly audits of the data center access are now conducted and any changes to access are now done electronically. OIT is investigating the use of encryption to protect the backup tapes. At this point in the investigation, this will be a costly and major project. The use of network password controls has been updated. Each technician is assigned a unique password, enabling the traceability of changes to an individual. Internal exchange e-mail encryption was completed 11/2008. External e-mail encryption is waiting on Department approval of funding.

Finding 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.

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.
Management’s Original Response: 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.

Management’s Follow-Up Response: At this time, the Department is reviewing its database architecture for creating an alternative to the SSN; furthermore, to mitigate the use of the SSN in the security access request form, the Department is implementing the ability for the user to enter the employee ID when available. 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. OIT is currently working with the Office of Legal Services to establish the appropriate language for this disclaimer statement.

Finding 3: The Department lacked effective procedures for addressing data exchange errors generated during the upload of inmate data during inmate reception processing.

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

Management’s Original Response: 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.

Management’s Follow-Up Response: The issue with timely monitoring of data exchanges errors will be eliminated at the completion of the Department’s project to bring the reception process from CARP to OBIS. This project is currently underway.

Finding 4: Aspects of the Department’s application controls within OBIS needed improvement. We are not disclosing specific details of the issues in this report.

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

Management’s Original Response: The Department will implement additional control processes to further detect and prevent inappropriate or unnecessary system actions.

Management’s Follow-Up Response: The Department has adapted enhanced security rules, and is in the process of implementing other controls, some of which are contingent upon LBR approval.

Finding 5: The Department’s information security program needed improvement to document, in a more comprehensive manner, management’s expectations for safeguarding IT resources.

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.

Management's Original Response: 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.

Management's Follow-Up Response: The Department's Bureau of Staff Development has approved the security awareness training developed by OIT. Training is now available via Staff Development for all departmental employees and contractors.

An Information Security Strategic Plan and Risk Management Program are in development. Once completed, these documents will be published as part of the agency wide Security Program. A more detailed Security Awareness Plan will be part of the Strategic Plan and Security Program. The Department is researching the feasibility of an automated application to document an employee's acceptance of the Security Policy.

The Department completed the Risk Assessment and submitted it to the Agency for Enterprise Information Technology (AEIT). Assets have been identified and threats have been defined. Next steps are to document known vulnerabilities and match up controls.

Efforts are underway to stand up OpenMDR application (originally from DOH) as a way to classify data in an efficient manner. The Department is developing a Security Bulletin to clarify HIPAA and confidential data. The Department utilizes the industry standard Department of Defense method of destroying and disposing of confidential data residing on personal computers. This practice has been formally defined by departmental policy 206.010.

Finding 6: Program change controls for OBIS needed improvement.

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.

Management's Original Response: 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.

Management’s Follow-Up Response: The Department has set up a process to review standards and current processes; moreover, the process includes placing these standards and processes on schedule for review annually.

The Department now requires testing documentation for OIT Change Management and Quality Control before anything is moved to the production environment. Procedures for the promotion process are updated to reflect current practices.

The Department moved the Quality Control function from the Bureau of System Development to the Bureau of Service Delivery. This ensures the same person that made the program changes is not the same person that performs the quality control or moves the change to production.

The Department continues to review its test development and user acceptance test environments for improvement in the frequency of refresh per audit recommendation. Due to the budgetary constraints concerning staff overtime, the Department is unable to make any decisions immediately.

Finding 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.

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.

Management’s Original Response: 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.

Management’s Follow-Up Response: As stated in the original response, the quality control function was relocated organizationally to report to the Bureau of Service Delivery in the same section as the OIT change management process as opposed to the Bureau of Systems Development per the audit recommendation.

Finding 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.

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.

**Management’s Original Response:** 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.

**Management’s Follow-Up Response:** A procedure on “Positions of Special Trust” as it relates to employees in established positions has been drafted by the Bureau of Personnel and is being reviewed.

The Office of Information Technology and the Office of Personnel have completed the fingerprinting of all existing contract personnel who previously passed the FCIC/NCIC background checks per audit recommendation. A new DC/OIT Policy is being developed to reflect current practices. The Department has developed a centralized repository to track contract personnel’s compliance. This document is stored in a locked and secured file drawer per the audit recommendation.

**Finding 9:** The Department lacked a formal management review process to ensure that inmate gain time adjustments were uniform throughout the Department.

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

**Management’s Original Response:** 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.

**Management’s Follow-Up Response:** Department staff makes approximately 200,000 individual case management decisions each month regarding the award of inmate gain time. An automated system is utilized to calculate and apply the gain time to ensure each award is consistent with rules and policy.

Automated reports are available to the administration of local facilities to monitor their gain time awards and to compare the results with other facilities in their region or the state. Further, inmates also have the ability to grieve the monthly gain time awards to management staff and we find the number of inmates grieving the discretionary award to be minimal. This is an indication that the current method of applying the discretionary gain time is being applied fairly and consistently throughout the state.

The department will consider establishing a management review standard for incentive gain time as part of our Operation Review process. This will help ensure that inmate gain time adjustments are uniform and the reviews documented.