

DEPARTMENT OF CORRECTIONS

OFFENDER BASED INFORMATION SYSTEM
(OBIS)

Information Technology Operational Audit



SECRETARY OF THE DEPARTMENT OF CORRECTIONS

Section 20.315, Florida Statutes, created the Department of Corrections. The head of the Department is the Secretary, who is appointed by the Governor and subject to confirmation by the Senate. The Secretary who served during the period of our audit was Michael D. Crews.

The audit team leader was Suzanne Varick, CPA, and the audit was supervised by Tina Greene, CPA, CISA. Please address inquiries regarding this report to Arthur Hart, CPA, Audit Manager, by e-mail at arthart@aud.state.fl.us or by telephone at (850) 412-2923.

This report and other reports prepared by the Auditor General can be obtained on our Web site at www.myflorida.com/audgen; by telephone at (850) 412-2722; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF CORRECTIONS

Offender Based Information System (OBIS)

SUMMARY

Pursuant to Section 20.315(1), 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; ensure the safety of Department personnel; and provide proper care and supervision of all offenders under its jurisdiction while assisting, as appropriate, their reentry into society. The Department uses the Offender Based Information System (OBIS) to aid in the recording of the offender's day-to-day activities as well as to record historical data.

Our operational audit focused on evaluating selected information technology (IT) controls applicable to OBIS. We also determined the status of Department corrective actions regarding selected audit findings disclosed in our report No. 2009-011. Our audit disclosed areas in which improvements in OBIS controls and operational processes were needed. The results of our audit are summarized below:

Finding No. 1: As noted in our report No. 2009-011, contrary to Section 119.071(5)(a)2.a., Florida Statutes, the Department collected and used certain social security numbers (SSNs) in OBIS without specific authorization in law or without having established the imperative need to use the SSNs for the performance of its duties and responsibilities as prescribed by law.

Finding No. 2: Controls for population counts of inmates in transit and inmate transfers needed improvement.

Finding No. 3: Department procedures related to data input of inmate transfers and reconciliations of inmate data needed improvement.

Finding No. 4: Certain Department controls related to the logging and monitoring of system activity needed improvement. A similar finding was noted in our report No. 2009-011.

Finding No. 5: Contrary to the State of Florida, *General Records Schedule* retention requirements, the Department did not retain relevant inmate count records.

Finding No. 6: Some unnecessary and inappropriate access privileges existed within OBIS. A similar finding was noted in our report No. 2009-011.

Finding No. 7: The Department did not timely deactivate the access privileges of some former and transferred employees. A similar finding was noted in our report No. 2009-011.

Finding No. 8: Certain OBIS security controls related to the protection of confidential and exempt data needed improvement, including some that were similarly communicated to Department management in connection with our report No. 2009-011.

BACKGROUND

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. The Department's Office of Information Technology (OIT) maintains OBIS for the joint use of the Department and the Parole Commission.

Offenders first received into Department custody are processed through one of six reception centers located throughout the State before being transferred to an institution. The reception centers use the Computer Assisted Reception Process (CARP) system to collect information on all offenders received into Department custody. Once

the information is entered into CARP, it is automatically uploaded into OBIS for the institution to which the offender is eventually transferred and the Department's Central Office to use.

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. The Office of Health Services uses OBIS to collect and record selected information about an inmate'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 levels 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: Use of SSNs

Section 119.071(4)(a), Florida Statutes, provides that all employee social security numbers (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.

As previously noted in our report No. 2009-011, the Department collected and used certain 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 SSNs, rather than another number. The use of SSNs is contrary to State law and increases the risk of improper disclosure of SSNs.

Recommendation: In the absence of establishing an imperative need for the use of SSNs, the Department should comply with State law by establishing another number to be used in OBIS rather than SSNs.

Finding No. 2: Inmate Population Counts

Data processing controls include controls that ensure that data is processed accurately and completely, data retains its validity during processing, and effective independent review and monitoring procedures are in place. Our audit disclosed the following control deficiencies related to the accuracy, completeness, and validity of inmate population counts:

- Inmates in transit at the time of inmate population count reporting were not always being accurately reported. We reviewed data relating to six inmates listed on the January 23, 2014, *Inmate in Transit Exception Report* and found that the inmates had not been correctly included in the inmate population count for the appropriate institution. We noted that two inmates whose data we reviewed remained in transit for 8 and 20 days and the other four inmates whose data we reviewed were erroneously reported as in transit for 117 to 524 days. Under these conditions, the risk was increased that management decision making could be hindered by inaccurate or misleading inmate population counts in OBIS.

- Inmate transfers are generally approved and scheduled before the transfer actually occurs. However, there are occasions when normal system controls need to be overridden in the event an inmate needs to be transferred without documented approval in OBIS. Automated controls in OBIS generated an electronic mail notification that was sent to a Bureau of Classification Management mailbox whenever the inmate transfer did not pass edits such as not having the associated approval in OBIS. Although the electronic mail notices were being generated and sent to the Bureau of Classification Management, the notices were not being reviewed and approved on a regular basis. Under these conditions, the risk is increased that inappropriate and unauthorized inmate transfers may be made and not be timely detected.

Recommendation: The Department should implement controls to ensure that inmate population counts appropriately include inmates in transit. Additionally, controls should be improved to ensure that inmate transfer transactions are reviewed for appropriateness and approved on a timely basis.

Finding No. 3: Data Input and Reconciliations

Effective input controls include procedures that ensure data is entered into the system in a consistent manner to promote the accuracy, completeness, and validity of data. Interface controls include procedures that are intended to provide reasonable assurance that all inputs into the target application have been accepted for processing and any interface errors are recognized and corrected in a timely manner. Such procedures typically include batch totals, control totals, and reconciliations. Written procedures help ensure that management directives are correctly and consistently applied. During our audit, we noted the following control deficiencies related to OBIS input and reconciliation controls:

- The Department's *Inmate Transfer Approval Process (Process)* describes the procedures that should be performed when approving inmate transfers. However, the *Process* did not provide relevant information that would ensure consistency across all institutions, reception centers, and the Central Office on how the inmate transfers were to be recorded in OBIS. In response to audit inquiry, Department management referenced various other technical and reference guides that were available. Nevertheless, the combination of the information contained in other technical and reference guides did not appropriately address procedures to ensure consistency in how inmate transfers should be recorded in OBIS. Without a documented procedure to ensure the consistency of the entry of inmate transfer data in OBIS, the accuracy and completeness of the data could be compromised.
- Although inmate data is automatically interfaced from CARP to OBIS on a nightly basis, the Department did not have reconciliation controls between CARP and OBIS to ensure the accuracy and completeness of data. Without an effective method to reconcile CARP inmate data uploaded into OBIS, the risk is increased that inaccurate and incomplete inmate information may be entered and processed in OBIS without being timely detected. A similar finding was noted in our report No. 2009-011.
- Department procedures describe the process that should be used to perform a physical inmate population count and describe when specific physical inmate population counts should be performed. However, Department procedures did not provide information on the process that should be followed to ensure the physical inmate population count reconciles to the related inmate population count data in OBIS. Also, our review indicated that the inmate population count reconciliation report did not always reconcile to the OBIS inmate population count reports used by the Bureau of Classification Management and the Bureau of Research and Data Analysis. Additionally, the inmate population count reports used by the Bureau of Classification Management and the Bureau of Research and Data Analysis did not always reconcile to each other due to timing differences. The lack of effective reconciliations increased the risk that the inmate population counts reported may not be valid, accurate, or complete.

Recommendation: The Department should establish procedures to ensure that data entered, interfaced, and maintained in OBIS is consistent and reconciled on a timely basis.

Finding No. 4: Logging and Monitoring of System Activity

Controls related to the logging and monitoring of system activity are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department controls related to the logging and monitoring of system activity that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising OBIS data and related IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate logging and monitoring controls related to system activity, the risk is increased that the confidentiality, integrity, and availability of OBIS data and related IT resources may be compromised. A similar finding was noted in our report No. 2009-011.

Recommendation: The Department should improve controls over the logging and monitoring of system activity to ensure the continued confidentiality, integrity, and availability of OBIS data and related IT resources.

Finding No. 5: Retention of Inmate Count Records

State of Florida, *General Records Schedule GS2 for Law Enforcement, Correctional Facilities, and District Medical Examiners (General Records Schedule)* revised effective December 1, 2010, provides that inmate count records consisting of the daily listings of all inmates incarcerated in each correctional or detention facility must be retained for one fiscal year provided applicable audits have been released. The Department utilized the *DC6-215 Inmate Count Form* to record the daily inmate population count. Our audit disclosed that, as a result of the misclassification of the *Inmate Count Form*, the inmate count records were only being retained for one month instead of one fiscal year provided applicable audits have been released. Without adequate retention of inmate count records, the risk is increased that the Department may not have sufficient documentation to assist in future investigations of inmate count errors, should they occur. In addition, the Department is not in compliance with the State's record retention requirements.

Recommendation: The Department should ensure that relevant inmate count records are retained as required by the *General Records Schedule*.

Finding No. 6: Appropriateness of Access Privileges

An important aspect of IT security management is the establishment of access privileges within OBIS that restrict users to only those system functions necessary to perform their assigned job duties. Effective management of access privileges helps enforce an appropriate separation of incompatible duties and minimize the risk of unauthorized system actions. As similarly noted in our report No. 2009-011, our audit disclosed some unnecessary and inappropriate access privileges as described below that increased the risk of unauthorized disclosure, modification, or destruction of data and IT resources:

Office of Health Services

Our review of 20 of 161 user identifications (IDs) with health services profiles as of January 30, 2014, disclosed that 4 users had access privileges assigned that provided unnecessary and inappropriate access privileges. Specifically, 2 users retained access privileges for temporary assignments beyond the time frame necessary; 1 user had been granted access but there was no documentation of that access being authorized; and 1 user was granted access in excess of what was needed for her current job responsibilities.

Bureau of Classification Management

Our review of 40 of 603 user IDs with classification profiles as of February 11, 2014, disclosed that 4 users had access privileges assigned that provided unnecessary and inappropriate access privileges. Specifically, 1 user retained access privileges for the classification supervisor profile for temporary assignments beyond the time frame necessary; 1 user was given the classification supervisor profile by mistake; and 2 users were granted access in excess of what was needed for their current job responsibilities.

Office of Information Technology (OIT)

Our review of all 40 user IDs with selected OIT profiles to OBIS transactions as of February 3, 2014, disclosed that 33 users had access privileges assigned that provided inappropriate access privileges. Specifically:

- 23 programmers had been granted the correct profile; however, the profile gave them access to production data which was inappropriate for their job duties.
- 10 users outside the two Application Development Sections had access privileges to the application programming profile which was in excess of what was needed for their current job responsibilities.

Recommendation: The Department should ensure that access privileges of users are commensurate with their job duties and enforce an appropriate separation of duties.

Finding No. 7: Terminated and Transferred Employees

Agency for Enterprise Information Technology (AEIT)¹ Rule 71A-1.007(6), Florida Administrative Code, provides that access authorization shall be promptly removed when the user's employment is terminated or access to the information is no longer required. Prompt action is necessary to ensure that a former employee or others do not misuse the former employee's access privileges.

Although the Department had policies and procedures requiring the removal of user access to OBIS within three days after termination or when an employee transfers, our audit disclosed that some employees did not have their OBIS accounts deactivated in a timely manner after terminating employment or after transferring to positions where the access originally granted was no longer needed. Without timely deactivation of former or transferred employee access privileges, the risk is increased that the access privileges may be misused by former or transferred employees or others. A similar finding was noted in our report No. 2009-011. Specifically, our audit disclosed the following:

Office of Health Services

One of the 20 active IDs included in our review with a health services profile belonged to a terminated employee. The OBIS access privileges of this former employee remained active for 328 days after her date of termination. In response to audit inquiry, Department staff deactivated the OBIS account of the former employee on February 13, 2014. We obtained evidence that the access privileges of the former employee had not been used subsequent to her date of termination.

Bureau of Classification Management

Four of the 40 active user IDs included in our review with selected classification profiles belonged to terminated employees. The OBIS access privileges of these four former employees remained active for 88 to 399 days after their

¹ Chapter 2014-221, Laws of Florida, effective July 1, 2014, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code; and existing contracts of the AEIT to the AST.

dates of termination. In response to audit inquiry, Department staff deactivated the OBIS account of the four former employees on various dates between February 11 through 14, 2014. We obtained evidence that the access privileges of the former employees had not been used subsequent to their dates of termination.

Office of Information Technology (OIT)

One of the 40 active user IDs included in our review with selected OIT profiles belonged to a transferred employee. Although the user was within OIT, this user had changed positions within OIT and no longer needed the application programming profile that had been granted to her. In response to audit inquiry, Department staff updated the OBIS account so that the transferred employee no longer had the application programming profile.

Recommendation: The Department should ensure that access privileges of former and transferred employees are timely deactivated.

Finding No. 8: Security Controls – Protection of Confidential and Exempt Data

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain Department security controls related to the protection of confidential and exempt data that needed improvement, including some that were similarly communicated to Department management in connection with our report No. 2009-011. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising OBIS data and related IT resources. However, we have notified appropriate Department management of the specific issues. Without adequate security controls related to the protection of confidential and exempt data, the risk is increased that the confidential and exempt information may be compromised.

Recommendation: The Department should improve security controls to ensure the continued protection of confidential and exempt data.

PRIOR AUDIT FOLLOW-UP

Except as noted in the preceding paragraphs, for those audit findings disclosed in our report No. 2009-011 that continued to be relevant and were within the scope of this audit, the Department had taken corrective actions.

OBJECTIVES, SCOPE, AND METHODOLOGY

The Auditor General conducts operational audits of governmental entities to provide the Legislature, Florida's citizens, public entity management, and other stakeholders unbiased, timely, and relevant information for use in promoting government accountability and stewardship and improving government operations.

We conducted this IT operational audit in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

The objectives of this IT operational audit were to determine the effectiveness of selected IT controls applicable to OBIS in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the confidentiality, integrity, availability, relevance, and reliability of data; and the safeguarding of IT resources. An additional objective was to determine whether management had corrected,

or was in the process of correcting, deficiencies disclosed in audit report No. 2009-011 that were within the scope of this audit.

The scope of our audit focused on evaluating selected IT controls applicable to OBIS during the period December 2013 through March 2014. The audit included selected input, processing, and output controls relevant to OBIS and selected application level general IT controls over security and risk management, systems modification, and logical access to programs and data.

This audit was designed to identify, for the IT system and controls included within the scope of the audit, deficiencies in management's internal controls and IT controls; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective IT operational policies, procedures, or practices. The focus of this IT Operational audit was to identify problems so that they may be corrected in such a way as to improve government accountability and efficiency and the stewardship of management. Professional judgment has been used in determining significance and audit risk and in selecting the particular IT controls, legal compliance matters, and records considered.

As described in more detail below, for the IT system and controls included within the scope of our audit, the audit work included, but was not limited to, communicating to management and those charged with governance the scope, objectives, timing, overall methodology, and reporting of our audit; obtaining an understanding of the IT system and controls; exercising professional judgment in considering significance and audit risk in the design and execution of the research, interviews, tests, analyses, and other procedures included in the audit methodology; obtaining reasonable assurance of the overall sufficiency and appropriateness of the evidence gathered in support of our audit's findings and conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

Our audit included the selection and examination of IT system controls and records. Unless otherwise indicated in this report, these items were not selected with the intent of statistically projecting the results, although we have presented for perspective, where practicable, information concerning relevant population value or size and quantifications relative to the items selected for examination.

An audit by its nature does not include a review of all records and actions of agency management, staff, and contractors and, as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit, we:

- Interviewed Department personnel.
- Obtained an understanding of key sources of data inputs (internal and external) and their related process flows that ensured the completeness, accuracy, validity, and confidentiality of data input into OBIS.
- Obtained an understanding of key transaction processing processes that ensured the completeness, accuracy, validity, and confidentiality of data processed in OBIS.
- Obtained an understanding of key types of data output and their related processes that ensured the completeness, accuracy, validity, and confidentiality of data outputs from OBIS.
- Documented any changes which had occurred in OBIS, including policies, procedures, hardware, software, organizational structure, and personnel relating to OBIS.
- Observed, documented, and evaluated selected transaction data input, processing, and output controls that ensured the completeness, accuracy, validity, and confidentiality of data input into OBIS.
- Observed, documented, and evaluated selected security management controls.

- Observed, documented, and evaluated the effectiveness of selected OBIS access controls.
- Observed, documented, and evaluated the effectiveness of selected OBIS configuration management controls.
- Evaluated the appropriateness of selected access privileges to OBIS healthcare system profiles.
- Evaluated the appropriateness of selected access privileges to OBIS inmate classification system profiles.
- Evaluated the appropriateness of selected access privileges to OBIS data, including terminated and transferred employees.
- Evaluated the effectiveness of the OBIS program change management process. Specifically, we reviewed 20 of 165 completed program changes from December 16, 2013, through February 4, 2014, to determine whether program changes were authorized, tested, approved, and appropriately moved to production.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, as necessary, to accomplish the objectives of the audit.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe those matters requiring corrective action.

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 operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a letter dated June 12, 2014, the Secretary provided responses to our preliminary and tentative findings. This letter is included at the end of this report as **EXHIBIT A**.

**EXHIBIT A
MANAGEMENT'S RESPONSE**



*Changing Lives to
Ensure a Safer Florida*

**FLORIDA
DEPARTMENT of
CORRECTIONS**

Governor
RICK SCOTT
Secretary
MICHAEL D. CREWS

501 South Calhoun Street, Tallahassee, FL 32399-2500

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

June 12, 2014

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

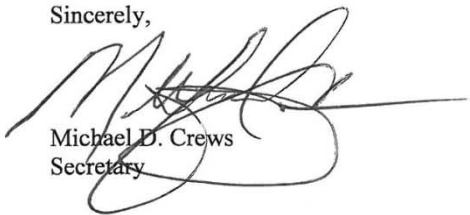
Dear Mr. Martin:

In accordance with section 11.45(4)(d), Florida Statutes, I am enclosing the Department's response to the preliminary and tentative findings and recommendations contained in the information technology operational audit of the Department of Corrections Offender Based Information System (OBIS).

This response reflects the specific action taken or contemplated to address the findings cited in your report.

Thank you for the opportunity to review and provide comments. If you have any questions or need additional information, please contact Paul Strickland, Chief Internal Auditor, at (850) 717-3408.

Sincerely,



Michael D. Crews
Secretary

Enclosure

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

**RESPONSE TO PRELIMINARY AND TENTATIVE FINDINGS INFORMATION
TECHNOLOGY OPERATIONAL AUDIT OF THE DEPARTMENT OF
CORRECTIONS OFFENDER BASED INFORMATION SYSTEM (OBIS).**

Finding No. 1: As noted in our report No. 2009-011, contrary to Section 119.071(5)(a)2.a., Florida Statutes, the Department collected and used certain social security numbers (SSNs) in OBIS without specific authorization in law or without having established the imperative need to use the SSNs for the performance of its duties and responsibilities as prescribed by law.

Recommendation: In the absence of establishing an imperative need for the use of SSNs, the Department should comply with State law by establishing another number to be used in OBIS rather than SSNs.

Agency Response: The Department has no suitable substitute for the SSN required to uniquely identify individuals including thousands of state employees and contractors requiring access to departmental systems. The Department continues to investigate a substitute for this data item. This change will be a substantial effort to the Department costing substantial time and dollars. All personnel handling SSN are trained in Security Awareness and have successfully completed a Level II Electronic Fingerprint check as required by state and federal law.

Finding No. 2: Controls for population counts of inmates in transit and inmate transfers needed improvement.

Recommendation: The Department should implement controls to ensure that inmate population counts appropriately include inmates in transit. Additionally, controls should be improved to ensure that inmate transfer transactions are reviewed for appropriateness and approved on a timely basis.

Agency Response: Classification Management immediately implemented a control to ensure that in transits are reviewed on a daily basis. Any in transit identified on the Population Report is cleared the next business day. The additional control that requests that transfers transactions are reviewed for appropriateness and approved on a timely basis refers to transfers that occur after hours. Classification Management is willing to review these transfers but the authorization is provided through the after hours process. Effective immediately Classification Management will review these daily to see if there is anything unusual. We will not be able to approve them because the transfer will have already taken place. However, if any transfer appears to be inappropriate, we will take corrective action.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 3: Department procedures related to data input of inmate transfers and reconciliations of inmate data needed improvement.

Recommendation: The Department should establish procedures to ensure that data entered, interfaced, and maintained in OBIS is consistent and reconciled on a timely basis.

Agency Response: The Department will add a section to the Automated Bed Space Management and Behavioral Assessment Manual to address movement and how to enter movement into OBIS. This direction will cover information that is not addressed in other technical and reference manuals and will provide direction to those technical and reference manuals when relevant.

The Department is currently working to move CARP into OBIS. Once there are no longer two systems, the discrepancies will no longer be present. The Department expects this to be completed in approximately one year.

Control room staff will utilize the OBIS/CDC screen (DC52) to reconcile each formal count and document the reconciliation on the "Control Room Log," DC6-207. The counts referred to are documents that print at separate times. The count constantly changes with movement and counts produced at different times will be different based upon this movement. The count is reconciled each day in population management and an official midnight count is produced.

Finding No. 4: Certain Department controls related to the logging and monitoring of system activity needed improvement. A similar finding was noted in our report No. 2009-011.

Recommendation: The Department should improve controls over the logging and monitoring of system activity to ensure the continued confidentiality, integrity, and availability of OBIS data and related IT resources.

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

**EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE**

Finding No. 5: Contrary to the State of Florida, General Records Schedule retention requirements, the Department did not retain relevant inmate count records.

Recommendation: The Department should ensure that relevant inmate count records are retained as required by the General Records Schedule.

Agency Response: *The Department has submitted the following "Pen and Ink Changes" for Procedure 602.006. A "Formal Count Sheet," DC6-212A, indicating each count station will be utilized by control room staff for the compilation of the institution count. At the completion of the Formal Count, all of the DC6-215s and the DC6-212A will be kept on record for one (1) fiscal year provided the applicable audits have been released.*

Finding No. 6: Some unnecessary and inappropriate access privileges existed within OBIS. A similar finding was noted in our report No. 2009-011.

Recommendation: The Department should ensure that access privileges of users are commensurate with their job duties and enforce an appropriate separation of duties.

Agency Response:

Office of Health Services

This finding cited individuals from non-health services bureaus that have access to health related information in OBIS. Health Services is reviewing all access privileges in terms of appropriateness. Where needed, new Security Access Requests (SAR's) will be generated with appropriate justification or in some cases, access may be terminated.

Bureau of Classification Management

The four users identified in the audit with inappropriate access were reviewed to ensure there had been no improper use of the access privileges. The profiles of these staff were corrected so they had only the access to the system necessary for their duties.

Office of Information Technology

Stricter adherence to procedure 206.007 by all staff, and additional training of security coordinators directed toward helping them understand their responsibilities and identify what types and levels of access they control and approve, should correct this finding. Further, a defined, established Department-supported security coordinator function in all program areas, operating in an established separation of duties system will improve the maintenance of information security in the Department.

**EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE**

Finding No. 7: The Department did not timely deactivate the access privileges of some former and transferred employees. A similar finding was noted in our report No. 2009-011.

Recommendation: The Department should ensure that access privileges of former and transferred employees are timely deactivated.

Agency Response:

Office of Health Services

This finding cited one individual who had terminated employment with the Department and did not have their health services access removed. Health Services is reviewing all employees with access to health services information in OBIS to ensure continued employment within the Department. Health Services is also developing a process for ongoing review to prevent future incidents.

Bureau of Classification Management

The four access ID's identified in the audit that belonged to terminated employees were reviewed to ensure there had been no improper access to the system after termination. The user accounts for these four employees were deactivated.

Office of Information Technology

The information security team within OIT currently monitors separated users reported via the nightly PeopleFirst-to-DOC download that updates the human resource database (HRD). This download evidences separations of employees (terminations). The information security team sends notices to security coordinators thought to be involved with the submission of disablement security requests for these separated users. It is believed that both the 208.029 Separation Process for Terminated Employees procedure performed by the supervisor at the time of separation (that includes the instruction to submit the disablement request) and the after the fact notice sent to local security coordinators by the information security team are sufficient to address separating employees. Additionally, stricter adherence to procedure 206.007(2)(c) by all staff with regard to transfers and position changes, and additional training of security coordinators directed toward helping them understand their responsibilities should correct this finding. Should additional steps be required the information security team will work with appropriate Department Institutions and Community Corrections staff to improve the existing processes and materials.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 8: Certain OBIS security controls related to the protection of confidential and exempt data needed improvement, including some that were similarly communicated to Department management in connection with our report No. 2009-011.

Recommendation: The Department should improve security controls to ensure the continued protection of confidential and exempt data.

Agency Response: The Department will implement additional control processes to further the protection of confidential and exempt data.