STATE OF FLORIDA AUDITOR GENERAL

Information Technology Operational Audit

Report No. 2018-039
November 2017

DEPARTMENT OF CORRECTIONS

Offender Based Information System

Sherrill F. Norman, CPA
Auditor General

Secretary of the Department of Corrections

The Department of Corrections is established by Section 20.315, Florida Statutes. The head of the Department is the Secretary who is appointed by the Governor and subject to confirmation by the Senate. Julie L. Jones served as Department Secretary during the period of our audit.

The team leader was Wayne Revell, CISA, 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 are available at:

FLAuditor.gov

Printed copies of our reports may be requested by contacting us at:

State of Florida Auditor General

Claude Pepper Building, Suite G74 • 111 West Madison Street • Tallahassee, FL 32399-1450 • (850) 412-2722

DEPARTMENT OF CORRECTIONS

Offender Based Information System

SUMMARY

This operational audit of the Department of Corrections (Department) focused on evaluating selected information technology (IT) controls applicable to the Offender Based Information System (OBIS) and included a follow-up on the findings included in our report No. 2014-202. Our audit disclosed the following:

Finding 1: Access privileges granted for some Department users of OBIS did not restrict users to only those functions necessary for their assigned job duties.

Finding 2: The Department did not timely deactivate the OBIS access privileges of some former employees and employees who transferred to other bureaus within the Department and no longer needed the access assigned.

Finding 3: Department procedures for conducting periodic reviews of user access privileges need improvement to ensure the appropriateness of OBIS user access privileges.

Finding 4: Contrary to State law,[1] the Department used certain social security numbers (SSNs) to establish security in OBIS without specific authorization in law or without having established the need to use the SSNs for the performance of its duties and responsibilities as prescribed by law.

Finding 5: Certain Department security controls related to logging and monitoring and the protection of confidential and exempt data for OBIS and related IT resources need improvement.

BACKGROUND

The Offender Based Information System (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 State law.[2] The Department's Office of Information Technology (OIT) maintains OBIS for the joint use of the Department and the Commission on Offender Review.

OBIS supports three main business processes within the Department: Institutions, Health Services, and Community Corrections. The Office of Institutions is responsible for the security and supervision of all four institutional regions and operational management of all correctional facilities and for maintaining records on all inmates incarcerated. 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 inmate medical, mental health, and dental care. 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 daily to manage offenders throughout their parole and probation periods. Offenders

[1] Section 119.071(5)(a.)2.a., Florida Statutes.

[2] Section 20.315(10), Florida Statutes.

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 1: Appropriateness of Access Privileges

Effective access controls include measures that restrict user access privileges to data and information technology (IT) resources to only those functions that promote an appropriate separation of duties and are necessary for the user's assigned job duties. Also, Agency for State Technology (AST) rules[3] require that each agency manage identities and credentials for authorized devices and users. Appropriately restricted access privileges help protect data and IT resources from unauthorized modification, loss, or disclosure.

As part of our audit procedures, we evaluated all 36 active user accounts assigned to 36 users within the OIT with access privileges to OBIS production data as of May 23, 2017. Our evaluation disclosed that all 36 users were assigned inappropriate or unnecessary access privileges. Specifically, we found that:

- 25 programmers were granted a profile that provided appropriate access privileges for their job duties; however, the profile also granted the programmers update access to production data, which was inappropriate for their job duties.
- 8 users were granted a database administration profile and an application programming profile, contrary to an appropriate separation of duties.
- 3 users, who were not members of either of the two application development sections, were granted an application programming profile that exceeded what was needed for their job duties.

The existence of inappropriate and unnecessary access privileges to OBIS increases the risk of unauthorized modification, loss, or disclosure of OBIS data and related IT resources. Similar findings were noted in prior audits of the Department, most recently in our report No. 2014-202.

Recommendation: We recommend that Department management limit user access privileges to OBIS to promote an appropriate separation of duties and restrict users to only those access privileges necessary for the users' assigned job duties.

Finding 2: Timely Deactivation of Access Privileges

AST rules[4] require each agency to manage identities and credentials for authorized devices and users and ensure that IT access is removed when the IT resource is no longer required. Prompt action to deactivate access privileges when a user separates from employment or access to the information is no longer required is necessary to help prevent misuse of the access privileges. Our audit disclosed that some employees' OBIS accounts were not timely deactivated after the user separated from Department employment or transferred to a position where the access originally granted was no longer needed.

[3] AST Rule 74-2.003(1)(a), Florida Administrative Code.

[4] AST Rule 74-2.003(1)(a)8., Florida Administrative Code.

We compared the list of 5,124 employees who separated from Department employment during the period July 1, 2016, through June 2, 2017, to the 130 active user accounts with Health Services profiles as of May 9, 2017, and the 637 active user accounts with classification officer, senior classification officer, and classification supervisor Classification profiles as of May 24, 2017. Our audit procedures disclosed that OBIS user accounts remained active for 2 former employees after their separation from Department employment. Specifically, we found that:

- The OBIS access privileges for 1 former employee within the Office of Health Services remained active for 355 days after the employee separated from Department employment.
- The OBIS access privileges for 1 former employee within the Bureau of Classification Management remained active for 14 days after the employee separated from Department employment.

Through additional audit procedures we also noted that the OBIS access privileges for 2 former employees with Classification profiles who separated from Department employment after May 24, 2017, remained active for 5 and 11 days after the employees' separation dates. Through our review of Department records, we determined that the accounts for these 2 former employees and the 2 aforementioned former employees were not used subsequent to the dates of the users' employment separation.

Additionally, as part of our audit, we evaluated the appropriateness of OBIS user access privileges within the Bureau of Classification Management. Our evaluation of 40 of 637 active user accounts with Classification profiles as of May 24, 2017, disclosed that 2 users had transferred to bureaus within the Department other than the Bureau of Classification Management and no longer needed the Classification profiles assigned. According to information provided by Department staff, the Classification profiles for these 2 transferred users remained active for 87 and 101 days after the users' transfer dates.

Timely deactivation of OBIS user access privileges upon employees' separation or transfer dates reduces the risk that the OBIS access privileges may be misused by the former employees or others. A similar finding was noted in prior audits of the Department, most recently in our report No. 2014-202.

Recommendation: We recommend that Department management ensure that access privileges of former or transferred employees are timely deactivated to minimize the risk of compromising OBIS data and IT resources.

Finding 3: Periodic Review of Access Privileges

AST rules[5] require that agency control measures address responsibilities of information stewards that facilitate periodic reviews of access rights with information owners. Agency responsibilities related to Information Security Managers include establishing an information security program that includes information security policies, procedures, standards, and guidelines.[6] Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

[5] AST Rule 74-2.003(1)(a)6., Florida Administrative Code.

[6] AST Rule 74-2.002(1)(f)8.c., Florida Administrative Code.

As part of our audit, we evaluated Department procedures and made inquiries with Department management related to the performance of periodic reviews of OBIS user access privileges. Our review disclosed, as noted in Findings 1 and 2 above, that the Department's procedures and process for the periodic review of OBIS user access privileges were not adequate. Specifically, Department procedures[7] only addressed the review of local area network and data center user accounts and did not include a review of the appropriateness of OBIS user access privileges.

Without an adequate periodic review of OBIS user access privileges, management's assurance that user access privileges are appropriate is limited.

Recommendation: We recommend that Department management improve procedures and controls for the periodic review of OBIS user access privileges to ensure that such privileges are appropriate.

Finding 4: Use of Social Security Numbers

State law[8] provides that all employee social security numbers (SSNs) held by an agency are confidential and exempt from public inspection. Pursuant to State law,[9] an agency may 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 used SSNs in OBIS to establish user security. As 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 identifier, this use of SSNs is contrary to State law and increases the risk of improper disclosure of SSNs. A similar finding was noted in prior audits of the Department, most recently in our report No. 2014-202.

Recommendation: In the absence of an established imperative need for the use of SSNs, the Department should comply with State law by utilizing another identifier to be used to establish OBIS user security rather than the user's SSN.

Finding 5: Security Controls – Logging and Monitoring and Protection of Confidential and Exempt Data

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit procedures disclosed that certain security controls related to logging and monitoring and the protection of confidential and exempt data need 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. Similar issues were also communicated to Department management in connection with prior audits of the Department, most recently in our report No. 2014-202.

[7] Department Procedure Number 206.007, *User Security for Information Systems*.

[8] Section 119.071(4)(a)1., Florida Statutes.

[9] Section 119.071(5)(a)2.a., Florida Statutes.

The lack of appropriate OBIS security controls related to logging and monitoring and the protection of confidential and exempt data increases the risk that the confidentiality, integrity, and availability of OBIS data and related IT resources may be compromised.

Recommendation: To ensure the confidentiality, integrity, and availability of OBIS data and related IT resources, we recommend that Department management improve certain OBIS security controls related to logging and monitoring and the protection of confidential and exempt data.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings included in our report No. 2014-202.

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 from May 2017 through July 2017 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 the audit findings and our conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for the audit findings and our conclusions based on our audit objectives.

This IT operational audit focused on evaluating selected IT controls applicable to OBIS during the period July 2016 through July 2017 and selected actions subsequent thereto. The audit included selected business process application controls over transaction data input and processing; selected application-level general controls over logical access, data security, logging and monitoring, and record retention related to OBIS; and audit findings disclosed in audit report No. 2014-202. The overall objectives of the audit were:

- To determine the effectiveness of selected IT controls 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; the safeguarding of IT resources.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2014-202.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

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; instances of noncompliance with applicable governing laws, rules, or contracts; and instances of inefficient or ineffective operational policies, procedures, or practices. The focus of this 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 this audit, our 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 the 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 the audit findings and our conclusions; and reporting on the results of the audit as required by governing laws and auditing standards.

This 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 this audit, we:

- Interviewed Department personnel and reviewed OBIS-related documentation to obtain an understanding of:
  - The purpose and goals of OBIS with respect to financial, operations, and compliance requirements.
  - The data and business process flows for OBIS, including key sources of data input and key types of application data output related to OBIS.
  - The OBIS computing platform including applicable hardware, operating system, database management system, and security software related to the application.
- Evaluated OBIS business process application controls related to input and processing. Specifically, we:
  - Evaluated the Office of Institutions Bureau of Classification Management *Automated Bed Space Management and Behavioral Assessment Scale Technical Manual* to determine whether adequate procedures were in place regarding the entry of inmate transfer data in OBIS.
  - Evaluated the Office of Institutions *Procedure Number 602.006, Count Procedure*, to determine whether adequate procedures were in place for controlling the reconciliation of inmate counts.
  - Inspected documentation of the reconciliation of inmate population count reports used by the Bureau of Security Operations and the Bureau of Research and Data Analysis.
  - Reviewed electronic mail notifications sent to the Office of Institutions Bureau of Security Operations mailbox (public folder), and examples of corrective actions taken by staff after their review of overrides related to inmate transfers.
  - Reviewed documentation of the daily review of in-transits and evidence to determine whether in-transits identified on the *Transfer Exceptions* Report were cleared the next business day.

- Evaluated application access controls. Specifically, we:
  - Evaluated the Office of Information Technology *Procedure Number 206.007, User Security for Information Systems*, to determine whether adequate procedures were in place for controlling access to the Department's IT systems and the related periodic review of access appropriateness.
  - Evaluated the appropriateness of the access privileges for 15 of the 130 active user accounts with Health Services profiles as of May 9, 2017.
  - Evaluated the appropriateness of the access privileges for 36 active user accounts within the Office of Information Technology with selected OIT profiles to OBIS production data as of May 23, 2017.
  - Evaluated the appropriateness of the access privileges for 40 of the 637 active user accounts within the Bureau of Classification Management with classification officer, senior classification officer, and classification supervisor Classification profiles as of May 24, 2017.
  - Compared the list of 5,124 employees who separated from Department employment during the period July 1, 2016, through June 2, 2017, to the 130 active user accounts with Health Services profiles as of May 9, 2017, and the 637 active user accounts with classification officer, senior classification officer, and classification supervisor Classification profiles as of May 24, 2017, to determine whether active OBIS accounts with these profiles remained for the former employees.
- Evaluated the effectiveness of the Department's monitoring controls related to OBIS.
- Evaluated access controls that protect confidential and exempt data. Specifically, we:
  - Evaluated the Department's *Protected/Sensitive Information Agreement* to determine whether controls were in place regarding employee handling of sensitive data.
  - Evaluated the Office of Information Technology *Procedure Number 206.010, Information Technology Security Relating to HIPAA*, to determine whether adequate procedures were in place to address the handling of OBIS data when related to the Health Insurance Portability and Accountability Act of 1996 (HIPAA).
- Evaluated controls related to data retention requirements. Specifically, we:
  - Evaluated the Office of Institutions *Procedure Number 602.006, Count Procedure*, to determine whether adequate procedures were in place for the retention of inmate count records in compliance with *General Records Schedule GS2 for Law Enforcement, Correctional Facilities, and District Medical Examiners* effective August 2017.
  - Inquired of Department management, including selected correctional facilities management, and evaluated inmate count documentation for the retention of inmate count records for August 24, 2016, to determine whether inmate count records were retained in accordance with the *General Records Schedule GS2 for Law Enforcement, Correctional Facilities, and District Medical Examiners*, for 8 of 68 correctional facilities.
- Communicated on an interim basis with applicable officials to ensure the timely resolution of issues involving controls and noncompliance.
- Performed various other auditing procedures, including analytical 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 the matters requiring corrective actions. Management's response is included in this report under the heading ***MANAGEMENT'S RESPONSE***.

AUTHORITY

Section 11.45, Florida Statutes, provides that the Auditor General may conduct audits of the IT programs, activities, functions, or systems of any governmental entity created or established by law. 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.

Sherrill F. Norman, CPA
Auditor General

MANAGEMENT'S RESPONSE

FLORIDA
DEPARTMENT of
CORRECTIONS

Governor
RICK SCOTT

Secretary
JULIE L. JONES

501 South Calhoun Street, Tallahassee, FL 32399-2500

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

November 17, 2017

Ms. Sherrill F. Norman
Office of the Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1450

Dear Ms. Norman:

In accordance with Section 11.45(4)(d), Florida Statutes, I am enclosing the Department's response to the preliminary and tentative finding and recommendation contained in the information technology operational audit of the Department of Corrections, Offender Based Information System. This response reflects the specific action taken or contemplated to address the finding 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,

Julie L. Jones
Secretary

Enclosure

★INSPIRING SUCCESS BY TRANSFORMING ONE LIFE AT A TIME ★

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

Finding 1: Access privileges granted for some Department users of OBIS did not restrict users to only those functions necessary for their assigned job duties.

Recommendation: We recommend that Department management limit user access privileges to OBIS to promote an appropriate separation of duties and restrict users to only those access privileges necessary for the users' assigned job duties.

Agency Response: *The Department concurs with the audit finding.*

Since the initial audit finding OIT has made progress to ensure more secure access privileges of users. Compliance with FDC Procedure 206.007, and additional training of security coordinators directed toward a better understanding of their responsibilities, including identification of types and levels of access they control and approve, has improved mitigation of this finding. Additional language will be added to 206.007 to dictate the process of performing recurring assessment of the appropriateness of access assignments.

Finding 2: The Department did not timely deactivate the OBIS access privileges of some former employees and employees who transferred to other bureaus within the Department and no longer needed the access assigned.

Recommendation: We recommend that Department management ensure that access privileges of former or transferred employees are timely deactivated to minimize the risk of compromising OBIS data and IT resources.

Agency Response: *The Department concurs with the audit finding.*

The provisioning team within OIT currently monitors separated users reported via the nightly PeopleFirst-to-FDC download that updates the human resource database (HRD). This download indicates separation of employees (terminations) which prompt the provisioning team to send notices to security coordinators as reminders to submit 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 and the aforementioned notice sent to local security coordinators by the provisioning team are sufficient to address separating employees. The accounts identified in this finding were missed through human-error. Part to the solution to the issue will be remedial training for both the provisioning team and involved supervisors. In addition, FDC has initiated a project to replace the current Security Access Request (SAR) program with a more automated process for the creation and removal of users in Service Now. The implementation of this new process/application will further mitigate these oversights.

Finding 3: Department procedures for conducting periodic reviews of user access privileges need improvement to ensure the appropriateness of OBIS user access privileges.

Recommendation: We recommend that Department management improve procedures and controls for the periodic review of OBIS user access privileges to ensure that such privileges are appropriate.

Agency Response: *The Department concurs with the audit finding.*

Additional language will be added to FDC Procedure 206.007 to dictate the process of performing recurring assessment of the appropriateness of access assignments. Improvements to the frequency of these reviews and management oversight of these reviews will be considered as a part of the effort to revise 206.007. Automation of some access/provisioning tasks using Service Now will further help mitigate this finding.

Finding 4: Contrary to State law, the Department used certain social security numbers (SSNs) to establish security in OBIS without specific authorization in law or without having established the need to use the SSNs for the performance of its duties and responsibilities as prescribed by law.

Recommendation: In the absence of an established imperative need for the use of SSNs, the Department should comply with State law by utilizing another identifier to be used to establish OBIS user security rather than the user's SSN.

Agency Response: *The Department concurs with the audit finding.*

Ongoing review of OIT procedures includes consideration of the use and protection of SSNs in relation to OBIS. Additionally, FDC has implemented a "Protected/Sensitive Information Agreement" to further outline user responsibilities regarding handling of sensitive data, such as SSNs.

Development efforts for modules within OBIS include review for justification of SSN use and removal of SSN fields wherever appropriate. Due to the substantial resource requirements necessary to immediately execute these changes, FDC continues to make improvements over time to eventually phase out use of SSNs as identifiers in OBIS. The timeline for full completion of this tasking is unknown.

Finding 5: Certain Department security controls related to logging and monitoring and the protection of confidential and exempt data for OBIS and related IT resources need improvement.

Recommendation: To ensure the confidentiality, integrity, and availability of OBIS data and related IT resources, we recommend that Department management improve certain OBIS security controls related to logging and monitoring and the protection of confidential and exempt data.

Agency Response: *The Department concurs with the audit finding.*

The Department will implement additional control processes to further detect and prevent inappropriate or unnecessary system actions and to further the protection of confidential and exempt data.