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

TO: Julie L. Jones, Secretary

FROM: Lester Fernandez, Inspector General

DATE: June 29, 2018

SUBJECT: FOLLOW-UP AUDIT REPORT NO. A18009F – DEPARTMENT OF CORRECTIONS OFFENDER BASED INFORMATION SYSTEM, REPORT NO. 2018-039

The Bureau of Internal Audit performed a follow-up audit to the Auditor General's Offender Based Information System Audit, Report No. 2018-039, issued in November 2017. The objectives of this follow-up were to determine if corrective action was taken on the reported audit findings and/or whether the action taken corrected the findings identified in the original report.

The scope of the follow-up consisted of obtaining from the Office of Information Technology a written response along with documentation of corrective action taken to implement the audit recommendations. The Bureau of Internal Audit has evaluated the follow-up response and documentation provided and determined that the Office of Information Technology needs to perform additional work to correct the findings identified in the original report. Therefore, the findings warrant further follow-up by the Bureau of Internal Audit.

for Ken Sumpter, DIG
Inspector General

LF/PS/dm
Attachment

cc: Steven Fielder, Chief of Staff
Wendy Ling, Chief Information Officer
Chris Ajhar, Deputy Chief Information Officer
Sibyle Walker, Government Operations Consultant II
Joint Legislative Auditing Committee
Kenneth Sumpter, Deputy Inspector General

OFFICE OF THE INSPECTOR GENERAL BUREAU OF INTERNAL AUDIT

FLORIDA DEPARTMENT OF CORRECTIONS

Follow-up of Auditor General's Report 2018-039 Department of Corrections Offender Based Information System

Lester Fernandez, Inspector General

Report #A18009F *Paul R. Strickland, Chief Internal Auditor* *June 29, 2018*

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. The Department's Office of Information Technology 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 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. In November 2017, the Office of the Auditor General published Report No. 2018-039, Department of Corrections, Offender Based Information System.

OBJECTIVES

The follow-up objectives were to determine:

- if corrective action was taken on reported audit findings; and
- whether the action taken corrected the findings in the original audit report.

SCOPE AND METHODOLOGY

The scope of the follow-up consisted of obtaining from the Office of Information Technology (OIT) a written response along with documentation of corrective action taken to implement the audit recommendations.

RESULTS OF AUDIT

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.

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 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 the Auditor General's audit procedures, they 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. The Auditor General's evaluation disclosed that all 36 users were assigned inappropriate or unnecessary access privileges. Specifically, the Auditor General 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 the Auditor General's report No. 2014-202.

Recommendation: The Auditor General recommended 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.

Management's Original 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.*

Management's Follow-Up Response: *Department Procedure 206.007 will be revised to dictate the process of performing recurring assessment of the appropriateness of access assignments.*

Bureau of Internal Audit Comments**:** *The Bureau of Internal Audit has evaluated OIT's follow-up response and documentation. The OIT needs to perform additional work to correct the finding. The revision of the Department Procedure 206.007 will be completed upon the replacing the Security Access Request system.*

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.

AST rules 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. The Auditor General's 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.

The Auditor General 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. The Auditor General's audit procedures disclosed that OBIS user accounts remained active for 2 former employees after their separation from Department employment. Specifically, the Auditor General 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 the Auditor General 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 the Auditor General's review of Department records, the Auditor General 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 the Auditor General's audit, they evaluated the appropriateness of OBIS user access privileges within the Bureau of Classification Management. The Auditor General's 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 the Auditor General's report No. 2014-202.

Recommendation: The Auditor General recommended 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.

Management's Original 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 of 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.*

Management's Follow-Up Response: *The Department is in the process of replacing the Security Access Request system.*

***Bureau of Internal Audit Comments**: The Bureau of Internal Audit has evaluated OIT's follow-up response and documentation. The OIT needs to perform additional work to correct the finding. The anticipated project end date for replacing the Security Access Request system is August 31, 2018.*

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

AST rules 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. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

As part of the Auditor General's audit, they evaluated Department procedures and made inquiries with Department management related to the performance of periodic reviews of OBIS user access privileges. The Auditor General's 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 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: The Auditor General recommended that Department management improve procedures and controls for the periodic review of OBIS user access privileges to ensure that such privileges are appropriate.

***Management's Original 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.*

***Management's Follow-Up Response:** Department Procedure 206.007 will be revised to dictate the process of performing recurring assessment of the appropriateness of access assignments.*

***Bureau of Internal Audit Comments**: The Bureau of Internal Audit has evaluated OIT's follow-up response and documentation. The OIT needs to perform additional work to correct the finding. The revision of the Department Procedure 206.007 will be completed upon the replacing the Security Access Request system.*

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.

State law provides that all employee social security numbers (SSNs) held by an agency are confidential and exempt from public inspection. Pursuant to State law, 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 the Auditor General's 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.

***Management's Original 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.

Management's Follow-Up Response: *Currently, the department's Security Access Request (SAR) is being re-written to no longer require the user's SSN to setup and establish an OBIS user account for FDC users. There is a business requirement for department users that require access to the JFI system (which is owned by FDLE) to have their SSN entered into the department's Top-Secret security system. When a department user tries to connect to the FDLE JFI system, the user's SSN is passed from Top-Secret to the FDLE JFI system. This is a requirement from FDLE to access their JFI* *system. Since the new SAR application will no longer require SSN to create an OBIS user account for FDC users, OIT will develop a process that identifies the departments JFI users and will automate populating the SSN from the People First Data Warehouse into the appropriate Top-Secret user records. The new SAR app will require the full SSN for new contracted employees since the contracted employee's info is not located in the People First system.*

Bureau of Internal Audit Comments*: *The Bureau of Internal Audit has evaluated OIT's follow-up response and documentation. The OIT needs to perform additional work to correct the finding. The anticipated project end date for replacing the Security Access Request system is August 31, 2018.

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.

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. The Auditor General's audit procedures disclosed that certain security controls related to logging and monitoring and the protection of confidential and exempt data need improvement. They are not disclosing specific details of the issues in this report to avoid the possibility of compromising OBIS data and related IT resources. However, they 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 the Auditor General's report No. 2014-202. 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, the Auditor General recommended that Department management improve certain OBIS security controls related to logging and monitoring and the protection of confidential and exempt data.

***Management's Original 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.

Management's Follow-Up Response: *The Department is having discussions with the Agency for State Technology in regards to security controls for the logging and monitoring and the protection of confidential and exempt data for OBIS and related IT resources.*

Bureau of Internal Audit Comments: *The Bureau of Internal Audit has evaluated the follow-up response and documentation provided and determined that the OIT needs to perform additional work to correct the finding identified in the original report.*

This follow-up audit was conducted in accordance with the International Standards for Professional Practice of Internal Auditing as published by the Institute of Internal Auditors. This follow-up audit was conducted by Dan McWilliams, Professional Accountant Supervisor, and supervised by Paul R. Strickland. Please address inquiries regarding this report to Paul R. Strickland, Chief Internal Auditor, at (850) 717-3408.