REPORT NO. 2015-190
JUNE 2015

DEPARTMENT OF JUVENILE JUSTICE

JUVENILE JUSTICE INFORMATION SYSTEM (JJIS)

Information Technology Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF JUVENILE JUSTICE

Section 20.316, Florida Statutes, created the Department of Juvenile Justice. The head of the Department is the Secretary of Juvenile Justice who is appointed by the Governor and serves at the pleasure of the Governor. During the period of our audit, Christina Daly served as Interim Secretary from July 1, 2014, through July 3, 2014, and as Secretary from July 4, 2014.

The audit team leader was Andrew Denny 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 JUVENILE JUSTICE

Juvenile Justice Information System (JJIS)

SUMMARY

The Department of Juvenile Justice (Department) maintains the Juvenile Justice Information System (JJIS). The JJIS is a Web-based system used by Department employees, contract providers, and criminal justice partners (e.g., Department of Law Enforcement, local law enforcement agencies, and the courts) to track juveniles through the entire juvenile justice process.

Our operational audit focused on evaluating selected information technology (IT) controls applicable to the JJIS. We also determined the status of corrective actions regarding selected audit findings included in our report No. 2014-015.

Our audit disclosed areas in which improvements in JJIS controls and operational processes were needed. The results of our audit are summarized below:

Finding No. 1: The Department had not established a JJIS application security plan that included an overview of the security requirements for the JJIS and a description of the controls in place or planned for meeting those requirements.

Finding No. 2: Department records did not always demonstrate that JJIS access privileges granted to users were appropriately authorized and that users had completed the required JJIS training prior to being granted JJIS access privileges. Similar instances were noted in our report No. 2014-015.

Finding No. 3: The Department did not have procedures for, and did not perform, comprehensive periodic reviews of the appropriateness of JJIS access privileges granted to users.

Finding No. 4: The Department had not established a mechanism to provide reasonable assurance that all program changes moved into the JJIS production environment were properly authorized, tested, and approved.

Finding No. 5: The Department lacked written procedures to ensure that *JJIS Incomplete Registration Process Reports* were timely reviewed.

Finding No. 6: Certain security controls related to JJIS user authentication, data storage and transmission, monitoring of system activity, and appropriateness of access privileges needed improvement.

BACKGROUND

Section 20.316(1)(b), Florida Statutes, provides that the Secretary of Juvenile Justice is responsible for planning, coordinating, and managing the delivery of all programs and services within the juvenile justice continuum. The term "juvenile justice continuum" means all children-in-need-of-services programs; families-in-need-of-services programs; other prevention, early intervention, and diversion programs; detention centers and related programs and facilities; community-based residential commitment and nonresidential programs; and delinquency institutions provided or funded by the Department.

Pursuant to Section 20.316(4), Florida Statutes, the Department developed the JJIS to, among other things, facilitate case management of juveniles referred to or placed in the Department's custody; provide timely access to current data and computing capacity to support outcome evaluation, legislative oversight, and other research; and provide automated support to the quality assurance and program review functions, the contract management process, and the facility operations management process.

The Bureau of Management Information Systems within the Department is responsible for the operation and maintenance of the JJIS. The Department's Bureau of Research and Planning assigned a Data Integrity Officer (DIO) to each of the State's judicial circuits to assist and train JJIS users, manage user access privileges, and ensure the accuracy and completeness of JJIS data.

FINDINGS AND RECOMMENDATIONS

Finding No. 1: Application Security Plan

Effective application security management provides a foundation for entity management to obtain reasonable assurance that an application is effectively secure. As such, security management controls include, among other things, the establishment of an application security plan. The application security plan documents an overview of the security requirements for the application and describes the controls in place or planned for meeting those requirements. An application security plan also delineates responsibilities and expected behavior of all individuals who access the system. An application security plan is documentation of the structured process of planning adequate, cost-effective security protection for an application.

Department management stated, upon audit inquiry, that they had developed and documented a strategic security plan for the Department's information resources but had not developed an application security plan for the JJIS that included an overview of the security requirements for the JJIS and a description of the controls in place or planned for meeting those requirements. Without a JJIS application security plan, the risk is increased that the Department may not implement adequate security controls over the application and that inappropriate application access and compromised data confidentiality, integrity, and availability may occur.

Recommendation: The Department should establish a JJIS application security plan that provides an overview of the JJIS security requirements and the controls in place or planned for meeting those requirements.

Finding No. 2: Authorization of JJIS Access Privileges and JJIS Training

Effective access authorization controls include, among other things, the use of access authorization forms to document the user access privileges that management has authorized. The DIOs in the judicial circuits are responsible for granting JJIS access privileges. Department documented process, *Access to JJIS and Associated Systems*, required that the supervisor for each user requiring JJIS access privileges submit to the applicable DIO a *JJIS Access/Permission Request* form or alternative documentation to authorize the appropriate JJIS access privileges and that the user complete the required JJIS training prior to being granted JJIS access privileges. The DIO is then to assign specific user access privileges based on the *JJIS Access/Permission Request* form.

As part of our review, we examined Department records for 40 users with JJIS access privileges as of December 16, 2014, to determine if the access privileges granted to users had been appropriately authorized and the required JJIS training had been completed. As similarly noted in our report No. 2014-015, our examination disclosed that the Department's records did not always demonstrate that JJIS access privileges were appropriately authorized and that users had completed the required JJIS training prior to being granted JJIS access privileges. Specifically:

- For 19 users, the Department was unable to provide the approved *JJIS Access/Permission Request* forms or alternative documentation demonstrating that appropriate Department management had authorized the users' JJIS access privileges.

- For 16 users, the access privileges authorized on the *JJIS Access/Permission Request* forms or alternative documentation provided by the Department did not match the users' assigned JJIS access privileges.
- For 11 users, the Department was unable to provide evidence that the users had completed the required JJIS training.

Without appropriate authorization of user access privileges, the risk is increased that JJIS access privileges granted to users may not be assigned as intended by management. Additionally, the lack of completion of the required JJIS training increases the risk that users may inadvertently compromise JJIS data integrity or security.

Recommendation: The Department should ensure that access privileges granted to users are appropriately authorized and that users complete the required JJIS training prior to being granted JJIS access privileges.

Finding No. 3: Periodic Review of JJIS User Access Privileges

Agency for Enterprise Information Technology (AEIT)[1] Rule 71A-1.007(2), Florida Administrative Code, provides that agency information owners shall review access rights (privileges) periodically based on risk, access account change activity, and error rate. Periodic reviews of user access privileges help ensure that only authorized users have access and that the access provided to each user remains appropriate.

Our audit disclosed that the Department had not established procedures for, and did not perform, comprehensive periodic reviews of the appropriateness of JJIS access privileges granted to users. As a result, management could not ensure that only authorized users had JJIS access privileges and that the access privileges granted to each user remained appropriate and authorized. Without comprehensive periodic reviews of the appropriateness of JJIS access privileges granted to users, the risk is increased that inappropriate JJIS user access privileges may exist and not be timely detected and may result in compromised data integrity.

Recommendation: The Department should establish and implement procedures for performing comprehensive periodic reviews of the appropriateness of JJIS access privileges granted to users.

Finding No. 4: Program Changes to the JJIS Production Environment

Effective program change controls over modification of application programs help ensure that only authorized, tested, and approved program changes are moved into the production environment. The effectiveness of program change controls is enhanced through mechanisms that provide reasonable assurance that all program changes moved into the production environment have been processed through appropriate authorization, testing, and approval controls.

During our audit, we determined that, although the Department had established written program change control procedures to ensure program changes were authorized, tested, and approved before being moved into the JJIS production environment, the Department had not established a mechanism to provide reasonable assurance that all program changes moved into the JJIS production environment followed the established program change control

[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; pending issues and existing contracts; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code, in effect as of November 15, 2010; trust funds; and unexpended balances of appropriations, allocations, and other funds of the AEIT to the AST.

procedures. Without a mechanism to ensure that all program changes moved into the JJIS production environment followed the established program change control procedures and were authorized, tested, and approved, the risk is increased that erroneous or unauthorized program changes may be moved into the JJIS production environment and not be timely detected.

Recommendation: The Department should establish a mechanism to provide reasonable assurance that all program changes moved into the JJIS production environment are properly authorized, tested, and approved.

Finding No. 5: Review of JJIS Incomplete Registration Process Reports

Effective error handling procedures during data origination and entry reasonably ensure that errors and irregularities are detected, reported, and corrected. Such procedures reasonably ensure that all inputs into the application have been accepted for processing and accounted for and that any missing or unaccounted-for source documents or input files have been identified and investigated. Effective procedures also ensure that exceptions are resolved within a specific time period.

The JJIS provides reports of the incomplete processing of juvenile intake registration transactions by judicial circuit. Our review of *JJIS Incomplete Registration Process Reports* for 20 judicial circuits indicated that 13 of 20 judicial circuits had incomplete juvenile intake registration transactions that were between 1 and 91 days old as of January 23, 2015. In response to our inquiry, Department staff stated that these reports are for probation supervisors and DIO staff. Probation supervisors use the reports weekly or daily to ensure that incomplete juvenile intake registration transactions (transactions) are completed. DIO staff use the reports at a minimum monthly for their assigned areas to ensure incomplete transactions are completed. However, the Department did not have written procedures that required a specified frequency for probation supervisors and DIO staff to review *JJIS Incomplete Registration Process Reports*. Additionally, as evidenced by the age of some of the incomplete transactions, *JJIS Incomplete Registration Process Reports* were not being reviewed and the transactions completed in a timely manner. Without timely review of *JJIS Incomplete Registration Process Reports*, the risk is increased that JJIS data may not be complete.

Recommendation: The Department should develop written procedures specifying the frequency of review and ensure that *JJIS Incomplete Registration Process Reports* are reviewed and transactions are completed in a timely manner.

Finding No. 6: Security Controls – JJIS User Authentication, Data Storage and Transmission, Monitoring of System Activity, and Appropriateness of Access Privileges

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. Our audit disclosed certain security controls related to JJIS user authentication, data storage and transmission, monitoring of system activity, and appropriateness of access privileges that needed improvement. We are not disclosing specific details of the issues in this report to avoid the possibility of compromising JJIS data and related IT resources. However, we have notified appropriate Department management of the specific issues. A similar finding regarding monitoring of system activity was noted in our report No. 2014-015. Without adequate security controls related to JJIS user authentication, data storage and transmission, monitoring of system activity, and appropriateness of access privileges, the risk is increased that the confidentiality, integrity, and availability of JJIS data and related IT resources may be compromised.

Recommendation: The Department should implement appropriate security controls related to JJIS user authentication, data storage and transmission, monitoring of system activity, and appropriateness of access privileges to ensure the continued confidentiality, integrity, and availability of JJIS data and related IT resources.

PRIOR AUDIT FOLLOW-UP

Three of the eight prior audit findings included in our report No. 2014-015 were not in the scope of this audit. The Department had taken corrective actions for three of the five findings included in our report No. 2014-015 that were applicable to the scope of this audit. Corrective actions were not taken for one of the five prior audit findings as described in the findings above. In addition, one prior audit finding was partially corrected.

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 November 2014 through January 2015 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 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. 2014-015 that were applicable to the scope of this audit.

The scope of our audit focused on evaluating selected business process application controls over data input, processing, and output applicable to the JJIS during the period July 2014 through January 2015 and selected actions through March 10, 2015. The audit also included selected application-level general controls over security management, logical access to programs and data, and configuration management.

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 ineffective or inefficient 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, 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 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 data input, processing, and output controls that ensure the completeness, accuracy, validity, and confidentiality of data input into the JJIS.
- Observed and evaluated selected transaction data input, processing, and output controls that ensure the completeness, accuracy, validity and confidentiality of JJIS data.
- Evaluated application security management controls related to the JJIS, including the application security plans, employee screenings, and the security awareness program.
- Evaluated the adequacy of security administration activity logging related to the JJIS. Specifically, we made inquiries of management regarding the security administration activity logging capabilities to the JJIS and reviewed an access change log as of March 9, 2015.
- Evaluated the adequacy of the monitoring of system activity by JJIS users. Specifically, we made inquiries of management regarding the monitoring of JJIS system activity by JJIS users and reviewed a system activity monitoring log as of January 13, 2015.
- Evaluated the effectiveness of selected user authentication controls for the JJIS. Specifically, we reviewed Department policies and other documentation regarding authentication settings and we reviewed authentication settings to determine if the settings were sufficient to restrict access.
- Evaluated the effectiveness of selected access controls to ensure that access privileges to the JJIS were appropriately authorized and that the required JJIS training had been completed. Specifically, we reviewed the access authorization forms and JJIS training documentation as of December 16, 2014, for 40 JJIS users to determine if the access privileges granted were authorized and the required JJIS training had been completed.
- Evaluated the effectiveness of selected logical access controls for the JJIS to ensure that user access privileges were appropriately restricted. Specifically, we reviewed user access privileges as of December 16, 2014, for 40 JJIS users to determine if the access privileges granted were appropriate.
- Evaluated the appropriateness of user database access privileges to the JJIS database management system. Specifically, we reviewed the access privileges of all 3 user accounts with update access privileges to the JJIS database management system as of December 16, 2014. Additionally, we reviewed the access privileges of all 28 user accounts with system administrator access privileges to the JJIS database management system as of February 5, 2014.
- Evaluated the effectiveness of application configuration management controls related to the JJIS. Specifically, we reviewed 8 of 82 JJIS program change requests that were closed between July 1, 2014, and January 28, 2015, to determine whether the program changes were appropriately authorized, documented, tested by an independent party, and approved and implemented into the production environment.
- Evaluated the effectiveness of the *Detention Risk Assessment Instrument* (*DRAI*) as part of the juvenile intake process at Juvenile Assessment Centers. Specifically, we reviewed the records of 40 juveniles across 16

judicial circuits as of January 7, 2015, to determine if *DRAI* assessments were performed in accordance with *JJIS Business Rule, Procedure Number 99-001* and Department of Juvenile Justice Rules 63D-9.001 and 63D-9.002, Florida Administrative Code.

- 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 May 15, 2015, 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

FLORIDA DEPARTMENT OF JUVENILE JUSTICE

Rick Scott, Governor **Christina Daly, Secretary**

May 15, 2015

David W. Martin
Auditor General
G74 Claude Pepper Building
111 West Madison Street
Tallahassee, FL 32399-1450

Dear Mr. Martin:

Please find attached the department's responses to the findings from your recent audit of the Juvenile Justice Information System (JJIS). We agree with the findings and have taken the appropriate steps to ensure corrective actions will be or have already been put in place.

I appreciate the professionalism shown by your staff while conducting the audit and feel this audit will assist in improving JJIS and some of our processes.

Sincerely,

Christina Daly,
Secretary

cc: Fred Schuknecht, Chief of Staff
Scott Morgan, Chief of Management Information Systems
Mark Greenwald, Chief of Research and Data Integrity

Enclosure

2737 Centerview Drive • Tallahassee, Florida 32399-3100 • (850) 488-1850
http://www.djj.state.fl.us

The mission of the Department of Juvenile Justice is to increase public safety by reducing juvenile delinquency through effective prevention, intervention, and treatment services that strengthen families and turn around the lives of troubled youth.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Juvenile Justice
Juvenile Justice Information System (JJIS) Information Technology Operational Audit

Finding No. 1: JJIS Application Security Plan

1. *The Department had not established a JJIS application security plan that included an overview of the security requirements for the JJIS and a description of the controls in place or planned for meeting those requirements.*

Response:
We concur. The Department has drafted a security plan specific to JJIS based on NIST Special Publication 800-53 and FIPS PUB 199 Guidelines.

Action Item:
Completed. Developed a specific application security plan for JJIS.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Juvenile Justice
Juvenile Justice Information System (JJIS) Information Technology Operational Audit

Finding No. 2: Authorization of JJIS Access Privileges and JJIS Training

2. *Department records did not always demonstrate that JJIS access privileges granted to users were appropriately authorized and that users had completed the required JJIS training prior to being granted JJIS access privileges. Similar instances were noted in our report No. 2014-015.*

Response:

The following process is in place: The Data Integrity Officers (DIOs) will require all users to sign training sheets. The DIOs will retain electronically all sign in sheets from training and a copy of the approved access request form. The JJIS access privileges process / controls were implemented October 28, 2013. Half of the users selected in the sample were accounts created prior to the implementation date of October 28, 2013.

Action Item:

Process implemented on October 28, 2013. The DIO Supervisor has addressed the correct process with DIO staff.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Juvenile Justice
Juvenile Justice Information System (JJIS) Information Technology Operational Audit

Finding No. 3: Periodic Review of JJIS User Access Privileges

3. *The Department did not have procedures for, and did not perform, comprehensive periodic reviews of the appropriateness of JJIS access privileges granted to users.*

Response:
We concur. The Data Integrity Officer Supervisor (DIO) is in the process of establishing quarterly permission reviews by program offices. The DIOs will work with MIS to restructure the permissions report to get accurate permission data from the Juvenile Justice Information System. The Data Integrity Officers will document quarterly reviews that are completed.

Action Item:
The DIO supervisor is in the process of developing policies / procedures for quarterly reviews. The estimated time frame for implementation is 10/1/15.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Juvenile Justice
Juvenile Justice Information System (JJIS) Information Technology Operational Audit

Finding No. 4: Program Changes to the JJIS Production Environment

4. *The Department had not established a mechanism to provide reasonable assurance that all program changes moved into the JJIS production environment were properly authorized, tested, and approved.*

Response:
We concur. The Department currently has a manual process which tracks all program changes and code movement from each environment. The development environment consists of Development, Quality Testing, and Production.

However, the Department recognizes that this manual process can be improved with the use of automated tools.

Action Item:
An automated change management tracking system has been developed to track incoming requests, assignments and changes throughout the development life cycle. The estimated time frame for implementation is June 2015.

Furthermore, the Department will research the feasibility and cost-effectiveness of implementing an automated tool for managing changes to the JJIS production environment which will augment the automated change management tracking system. No date is being set for implementing these changes at this time. Research is necessary to document the requirements, identify an automated tool, and identify funds necessary for the purchase and maintenance associated with the automated tool.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Juvenile Justice
Juvenile Justice Information System (JJIS) Information Technology Operational Audit

Finding No. 5: Review of JJIS Incomplete Registration Process Reports

5. *The Department lacked written procedures to ensure that JJIS Incomplete Registration Process Reports were timely reviewed.*

Response:
We concur. The Data Integrity Officer Supervisor is in the process of developing written procedures for the DIOs to perform a monthly review of the JJIS Incomplete Registration Process Reports and to correct any outstanding registrations for their assigned areas.

Action Item:
The Data Integrity Officer Supervisor is working on a written policy/procedure for the DIOs to conduct monthly reviews. The estimated time frame for implementation is 7/1/15.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Department of Juvenile Justice
Juvenile Justice Information System (JJIS) Information Technology Operational Audit

Finding No. 6: Security Controls – JJIS User Authentication, Data Storage and Transmission, Monitoring of System Activity, and Appropriateness of Access Privileges

6. *Certain security controls related to JJIS user authentication, data storage and transmission, monitoring of system activity, and appropriateness of access privileges needed improvement.*

Response:
We concur.

Action Item:
The Department will continue to address security controls where appropriate.