REPORT NO. 2014-015
OCTOBER 2013

DEPARTMENT OF JUVENILE JUSTICE

JUVENILE JUSTICE INFORMATION SYSTEM AND SELECTED ADMINISTRATIVE ACTIVITIES

Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF JUVENILE JUSTICE

The Department of Juvenile Justice is created by Section 20.316, Florida Statutes. 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, Wansley Walters served as Secretary.

The audit team leader was Jim Beaumont, CPA, and the audit was supervised by Jennifer Reeves, CPA. Please address inquiries regarding this report to David R. Vick, CPA, Audit Manager, by e-mail at davidvick@aud.state.fl.us or by telephone at (850) 412-2817.

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
and Selected Administrative Activities

SUMMARY

This operational audit of the Department of Juvenile Justice (Department) focused on Juvenile Justice Information System (JJIS) information technology (IT) controls and selected Department administrative activities. The audit also included a follow-up on the findings noted in our report No. 2012-183. Our audit disclosed the following:

JUVENILE JUSTICE INFORMATION SYSTEM

Finding No. 1: The Department did not always maintain documentation demonstrating that employees and contract providers received background screenings as a condition of employment and prior to being granted JJIS access privileges.

Finding No. 2: Department records did not always demonstrate that JJIS access privileges were limited to authorized users and that users had completed the required JJIS training.

Finding No. 3: The Department did not always timely deactivate JJIS access privileges upon the users' separation from employment. Additionally, the Department had not deactivated JJIS access privileges for a significant number of inactive user accounts.

Finding No. 4: The Department's change management process did not always provide for an appropriate separation of duties and the Department did not always adequately document JJIS program change authorizations.

Finding No. 5: Department controls to monitor user access to juveniles' social security numbers in the JJIS could be enhanced.

SELECTED ADMINISTRATIVE ACTIVITIES

Finding No. 6: The Department did not always timely cancel purchasing cards upon an employee's separation from Department employment.

Finding No. 7: The Department could not demonstrate that sensitive data was always removed from IT data storage media prior to disposal.

Finding No. 8: The Department's contract monitoring activities continue to need improvement.

BACKGROUND

The mission of the Department is to increase public safety by reducing juvenile delinquency through effective prevention, intervention, and treatment services. For the 2012-13 fiscal year, the Legislature appropriated over $523 million to the Department and authorized approximately 3,500 Department positions.

The Department is responsible for planning, coordinating, and managing the delivery of all programs and services within the juvenile justice continuum.[1] To deliver these programs and services, the Department is organized into five functional units, including Administration and four program areas:

- Detention Services,
- Prevention and Victim Services,
- Probation and Community Corrections, and
- Residential and Correctional Facilities.

Detention Services is responsible for operating 21 juvenile detention centers located throughout the State. The juvenile detention centers provide temporary supervision for juveniles awaiting a court date or placement in a residential commitment program. Prevention and Victim Services awards grants to local providers throughout the State to provide education, training, respite care, counseling, case management, and activities to reduce juvenile crime. Probation and Community Corrections is responsible for the supervision of juveniles participating in sanctions and services while remaining in their home community. Residential and Correctional Facilities is responsible for the supervision of juveniles who have been adjudicated by the court and sent to one of the 61 residential commitment facilities located throughout the State. These four program areas are administered through three regions (North, Central, and South), which are further divided according to the State's judicial circuits.

FINDINGS AND RECOMMENDATIONS

Juvenile Justice Information System

Pursuant to State law,[2] the Department developed the Juvenile Justice Information System (JJIS) to, among other things, facilitate the case management of juveniles referred to, or placed in, Department custody; provide timely access to current data and computing capacity to support outcome evaluation, legislative oversight, and other research activities; and provide automated support to the quality assurance and program review functions, the contract management process, and the facility operations management process. The JJIS contains numerous data fields, some of which contain confidential or sensitive information. Examples of specific JJIS data fields include juvenile name, social security number, race, age, school information, prior case history, immunization records, medical information, and the nature of any offenses.

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. According to Department records, there were approximately 7,900 user accounts with JJIS access privileges during the period July 2011 through February 2013.

The Department's Bureau of Management Information Systems (MIS Bureau) was responsible for the operation and maintenance of the JJIS and the 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.

[1] Section 20.316(1)(b), Florida Statutes, defines the juvenile justice continuum as 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.
[2] Section 20.316(4), Florida Statutes.

Finding No. 1: Background Screenings

State law[3] and Department policies and procedures[4] require that, as a condition of employment, all employees and contract providers be subject to level 2 screenings. As defined in State law,[5] a level 2 screening includes, but need not be limited to, fingerprinting for Statewide criminal history records checks through the Department of Law Enforcement, national criminal history records checks through the Federal Bureau of Investigation, and may include local criminal records checks through local law enforcement agencies. Department policies and procedures also require that Department and contract provider employees be rescreened every 5 years.

As part of our audit, we examined Department records for 60 JJIS user accounts to determine whether the applicable users had been subjected to the required level 2 screenings. The screening of JJIS user backgrounds is especially important due to the confidential and sensitive information contained in the JJIS. Our audit disclosed that for 7 JJIS user accounts the Department was unable to provide evidence that the required screenings, or rescreenings, had been requested or completed and, in response to our audit inquiry, Department management was unable to identify whether the 7 user accounts were assigned to Department employees or contract provider employees.

Absent documentation evidencing the conduct of level 2 screenings, the Department cannot demonstrate that only those individuals with appropriate backgrounds have been employed and granted access to the JJIS. Also, absent information identifying whether a JJIS user is a Department employee or a contract provider employee, the Department cannot assign responsibility for following up on any missing or untimely level 2 screenings.

Recommendation: We recommend that Department management ensure that level 2 screenings are timely conducted in accordance with the requirements of State law and Department policies and procedures and that documentation of the screening results is reviewed and maintained. To facilitate the follow up for any missing or untimely screenings, we also recommend that, when assigning a JJIS user account, the Department capture the name of the user's employer (e.g., the Department or contract provider's name).

Finding No. 2: Authorization of JJIS Access Privileges

The DIOs in each judicial circuit are responsible for granting JJIS access privileges. Department policies and procedures require that the supervisor for each user requiring JJIS access submit to the applicable DIO a *JJIS and Systems Access-Change Permission Request* form along with documentation demonstrating that the user had completed appropriate JJIS and security awareness training. The DIO is then to assign specific user access privileges based on the user's supervisor's request and the practices of the applicable judicial circuit.

As part of our audit, we examined Department records for 40 users with JJIS access during the period July 2011 through February 2013 to determine whether the users' access had been properly authorized and that the required JJIS training had been completed. Our audit tests disclosed that the Department's records did not always demonstrate that JJIS access privileges were limited to authorized users and that users had completed the required JJIS training. Specifically:

- For 32 users, or 80 percent, the Department was unable to provide the approved *JJIS and Systems Access-Change Permission Request* forms or alternative documentation demonstrating that appropriate Department management had authorized the users' access privileges.

[3] Section 984.01(2), Florida Statutes.
[4] Department Policy FDJJ-1800 and Department Procedure, *Background Screening Procedures*.
[5] Section 435.04, Florida Statutes.

- For 26 users, or 65 percent, the Department was unable to provide evidence that the user had completed JJIS training.

To properly safeguard the confidential and sensitive data contained in the JJIS, adherence to established controls requiring proper authorization for JJIS access privileges and appropriate JJIS training, is essential.

Recommendation: We recommend that Department management ensure that, prior to receiving access, JJIS users' access privileges are properly authorized and that users receive appropriate JJIS training.

Finding No. 3: Deactivation of JJIS Access Privileges

Effective access controls include provisions to timely remove employee access privileges for inactive accounts and when employment or contract terminations occur. Prompt action is necessary to ensure that access privileges are not misused by the former employee, contractor, or others. The Department's *Information Resource Security Handbook* (*Handbook*)[6] specifies that a JJIS user's access privileges are to be deactivated upon the user's separation from employment or when the user transfers to a position where JJIS access is no longer required. According to Department policies and procedures,[7] MIS Bureau staff are to deactivate Department employee JJIS access privileges upon notification of either event from Department supervisors. Similarly, the DIOs are to deactivate contract provider employees' JJIS access privileges upon notification from the applicable contract or grant manager. To further identify any user accounts that should be deactivated, a monthly personnel termination report and a monthly non-active user account report are to be reviewed by the DIOs and the applicable contract or grant managers.

We examined Department records to determine whether the Department had timely deactivated JJIS access privileges for the 265 JJIS users who separated from Department employment during the period July 2011 through February 2013. Our audit tests disclosed that the Department had not deactivated the JJIS access privileges for 127 of the users and that, as of February 27, 2013, 4 to 607 days had elapsed since the users separated from Department employment. We noted for another 48 of the users that, although the Department had deactivated the users' JJIS access privileges, the deactivations were not timely as 5 to 202 days had elapsed between the users' separation dates and the dates the access privileges were deactivated.

In response to our audit inquiry, Department management stated that MIS Bureau staff were not always properly and timely notified by Department supervisors, and contract providers did not always disclose to the applicable contract or grant manager, when JJIS users separated from employment.

We also performed audit procedures to identify any existing JJIS user accounts without recent activity, thereby indicating that the users did not require JJIS access to perform their assigned job duties. As JJIS password controls require users to change their password every 90 days, we performed an analytical procedure to identify any JJIS user passwords that, as of February 27, 2013, had not been changed within the past 90 days. We identified 521 existing user accounts for which the associated JJIS password had not been modified for a year or more, including 57 user accounts for which the password had not been updated in over 1,000 days.

When user access privileges are not timely deactivated upon a user's separation from employment or when access is no longer required to perform assigned job duties, the Department is exposed to a greater risk of unauthorized disclosure, modification, or destruction of Department data and IT resources.

[6] Department Procedure 1205.30, *Information Resource Security Handbook*.

[7] Department Procedure 1205.50, *Network User Accounts Procedures,* and 1205.60, *Provider Access to the Juvenile Justice Information System (JJIS) and JJIS Data Procedures*.

Recommendation: We recommend that Department management take steps to ensure that JJIS user access privileges are timely deactivated upon a user's separation from employment. Additionally, we recommend that JJIS user accounts be timely deactivated when users no longer require JJIS access to perform their assigned job duties.

Finding No. 4: JJIS Change Management Controls

Effective controls over program changes are intended to ensure that all changes are properly authorized, tested, approved, and tracked. Change management controls that are typically employed to ensure the continued integrity of application programs and systems include providing written evidence of the program change process, performing independent testing and approval of program changes, separating between employees the responsibility for developing changes and the responsibility for moving approved changes into the production environment, and restricting programmers from accessing or updating production data.

The Department's *Handbook* specifies that the test environment is to be separated from the production environment and that, to determine whether the changes had been authorized, tested, and documented, all program changes are to be approved by the MIS Bureau Chief prior to implementation. Pursuant to Department guidance, a user request form is to be completed and provided to the MIS Bureau for all requested program changes. The MIS System Project Manager is to review the form and approve or deny the request, or in the case of new IT development (i.e., development of a new application), forward the request form to the Department's IT Steering Committee for review and approval. During the period of our audit, the Software Technology Section, within the MIS Bureau, was responsible for handling the JJIS program change requests.

According to Department records, the Department completed 422 JJIS program changes during the period July 2011 through February 2013. As part of our audit, we examined Department records for 25 of these program changes. Our audit tests disclosed that 3 program changes had been moved into production by the same employee who had developed the change. Additionally, we found that the user request forms for 4 program changes had not been signed as approved by the MIS Systems Program Manager, contrary to Department guidance and the *Handbook*.

In response to our audit inquiries, Department management indicated that a developer making changes to the JJIS was allowed to move the changes into production when a manager or database administrator observed the change being placed into production. Department management also responded that the applicable user request forms had not been signed due to an oversight.

While the independent observation of program changes being moved from the test environment to production may provide some assurance, it does not substitute for an appropriate separation of change management duties. Also, absent documentation of appropriate review and approval for each program change request, the Department lacks assurance that only authorized changes will be made to the JJIS.

Recommendation: We recommend that Department management ensure that the responsibilities for developing and moving JJIS program changes into production are appropriately separated. Additionally, we recommend that all JJIS program change approvals be properly documented.

In the Department's response to this finding, Department management indicated that, due to limited resources, change management responsibilities cannot always be appropriately separated. Although we acknowledge the Department's resource concerns, as we noted in the finding, the Department completed 422 JJIS program changes during the period July 2011 through February 2013. The large number of program changes and the nature of the information contained in the JJIS makes effective change management

controls vitally important. The separation of responsibilities for developing changes and moving approved changes into the production environment is an essential change management control that should be established for all IT departments that employ more than one programmer or developer.

Finding No. 5: Confidential Data

Security controls are intended to protect the confidentiality, integrity, and availability of data and IT resources. The Department's *Handbook* specifies that confidential information is to be accessible to authorized personnel in the performance of their duties on a strict "need-to-know" basis. Additionally, the Department's *Handbook* requires that an auditable record of the transfer of all confidential and sensitive information be maintained. Logs of accesses to confidential or critical information and software, modifications of confidential or critical records, and all changes to automated security or access rules are also to be maintained. Pursuant to the Department's *Handbook*, authorized personnel are to be granted access so that the logs can be reviewed.

In July 2011, the Department modified the JJIS application controls to partially mask juveniles' social security numbers (SSNs), and only display the last four digits. Subsequent modifications were completed in January 2013 to provide for viewing the entire 9-digit SSNs, as well as tracking the JJIS users who viewed the SSNs. However, in response to our audit inquiry, Department management indicated that procedures for periodically monitoring logs of user SSN views had not been established.

As part of our audit, we were provided inquiry-only access privileges to the JJIS training environment to view JJIS intake screens. During audit testing, we encountered an error message that disclosed certain juveniles' entire SSNs. According to Department management, the mechanism used to track user views of SSNs did not identify or log any user views resulting from the error. Subsequent to our audit inquiry, Department management indicated that steps had been taken to correct this issue.

Periodic monitoring of JJIS user access to juveniles' SSNs would provide greater assurance that such access was appropriate and necessary and would also provide the Department with a mechanism to timely identify the need for corrective actions when inappropriate access occurs. Without adequate security controls, such as the complete tracking and monitoring of user access to protected data, the confidentiality, integrity, and availability of data and IT resources may be compromised, increasing the risk that Department data and IT resources may be subject to improper disclosure, modification, or destruction.

Recommendation: We recommend that Department management establish procedures to periodically monitor the appropriateness of JJIS user access to juveniles' SSNs.

Selected Administrative Activities

The Department's Office of Administrative Services is responsible for providing a wide array of services to Department staff and agencies doing business with the Department. These services or functions include: financial services; general services, including facility repairs and oversight of facility construction, purchasing and leasing, property management, telecommunications, and other support services; computer information systems; and personnel. In addition, staff in each of the Department's four program areas are responsible for activities related to contract management and monitoring. As part of our audit, we evaluated selected Department administrative activities, including those related to purchasing cards, IT data storage media disposal, and contract monitoring.

Finding No. 6: Purchasing Card Cancellations

The Department's Purchasing Card Manual specifies that supervisors are to alert the Department's Purchasing Card Program Administrator (PCPA), through the Separation Notification System, of the effective date of employment separation for all employees who had been assigned a purchasing card. The supervisors are also to collect the purchasing cards from the employees and immediately destroy the cards. The PCPA is responsible for terminating the cardholder account on the employee's separation date.

As part of our audit, we examined Department records to evaluate the timeliness of purchasing card cancellations for cardholders who had separated from employment during the period July 2011 through December 2012. According to Department records, 522 of the 1,245 employees who separated from employment during this period had been assigned a purchasing card. Our audit tests disclosed that, for 183 of the 522 cardholders, or 35 percent, the number of days that had elapsed from the dates of employment separation to the dates of purchasing card cancellation ranged from 2 to 389, and averaged 36.

Department management indicated in response to our audit inquiry that, during the period we evaluated, the PCPA did not always receive the necessary separation notifications from the Separation Notification System due to a problem that had since been corrected. Department management also stated that some delays may be attributed to supervisors not updating the Separation Notification System, as required.

Although our audit tests did not disclose any purchasing card usage for the 183 cards subsequent to the cardholders' separation from Department employment, absent timely cancellation of purchasing cards the risk of unauthorized purchases is increased.

Recommendation: We recommend that Department management take appropriate actions to ensure the timely cancellation of purchasing cards when cardholders separate from Department employment.

Finding No. 7: Disposal of IT Data Storage Media

IT resource controls prescribe that procedures be implemented to prevent access to confidential and sensitive information and software on computers, disks, and other equipment or media when these items are disposed of or transferred to another user. Such procedures ensure that data deleted from equipment to be disposed cannot be retrieved by any internal or third party. IT resource controls also include the logging of disposed sensitive items to maintain an audit trail.

Department procedures require that written assurance be maintained to document that confidential and sensitive information has been removed from applicable IT storage devices prior to disposal. IT data storage media sanitization is to be performed by:

- Using software to overwrite data on computer media;
- Degaussing;[8] or
- Physically destroying the media.

To document that confidential and sensitive data has been removed from IT data storage media prior to disposal, the Department requires that a *Surplus Certification of State Property* form and *Data Storage Media Sanitization or Destruction* form be completed. For computers, the *Surplus Certification of State Property* form is to be completed by the

[8] Degaussing is the process of erasing the magnetic field (i.e., information) stored on a disk drive.

Department's General Services liaison, Property liaison, or applicable contract manager and approved by the MIS Bureau Regional Leader or designee. For other equipment with data storage capabilities, the *Data Storage Media Sanitization or Destruction* form is to be completed and signed by the authorizing supervisor and also signed by MIS Bureau personnel once the equipment has been sanitized or destroyed.

According to Department records, during the period July 2011 through February 2013, the Department disposed of approximately 2,400 items with potential data storage capabilities. These items had been assigned to various organizational areas within the Department and included computers, printers, copiers, Ethernet switches, and servers.

As part of our audit, we examined Department records for 25 of the 2,400 items disposed. We noted that for 6 items, including one computer, three printers, and two Ethernet switches, neither a *Data Storage Media Sanitization or Destruction* form nor a *Surplus Certification of State Property* form had been completed. Additionally, we found that no alternative documentation was available to evidence that any stored information had been removed in accordance with Department procedures prior to the items' disposal. In response to our audit inquiry, Department management indicated that data sanitization had not been completed due to oversight or because staff were unaware of the data storage capabilities of the items.

To sufficiently safeguard confidential and sensitive information, it is critical that organizations properly identify items with data storage capabilities and, prior to disposing of such items, remove and document the removal of any stored data.

Recommendation: We recommend that Department management ensure that confidential and sensitive information is removed from all items with data storage capabilities prior to disposal.

Finding No. 8: Contract Monitoring

Pursuant to State law,[9] State agencies are responsible for enforcing the terms and conditions of all contracts and ensuring that contract deliverables are appropriately satisfied. As part of these responsibilities, the Department is to perform contract monitoring to evaluate whether desired service outcomes are being achieved and to identify performance problems as early as possible so that corrective action may be timely initiated.

The Department utilizes contract providers to deliver a range of services, including health care, detention, delinquency prevention, and probation and community intervention. As of February 2013, the Department had 362 active contracts, totaling approximately $1.6 billion, for services within its four program areas (Detention Services, Prevention and Victim Services, Probation and Community Corrections, and Residential and Correctional Facilities). These 362 contracts had been awarded to 161 providers located throughout the State.

Department procedures[10] require both administrative and programmatic monitoring of contracts be completed at least annually. Administrative monitoring focuses on accountability for fiscal resources, while programmatic monitoring evaluates the efficiency and effectiveness of contract providers in meeting program goals and objectives.

We examined Department documentation for 36 contracts, totaling approximately $333.5 million, that were active during the period July 2011 through February 2013. Our examination disclosed that the Department did not always conduct administrative and programmatic monitoring. Specifically, during the period July 2011 through February 2013, administrative monitoring had not been completed for 10 contracts, totaling approximately $11.6 million, and

[9] Section 287.057(14), Florida Statutes.
[10] Department of Juvenile Justice Contract Management and Program Monitoring Guidelines, sections 2-9 and 3-2.

programmatic monitoring had not been completed for 6 contracts, totaling approximately $184.2 million. For two additional contracts, totaling approximately $1.4 million, neither administrative nor programmatic monitoring had been completed.

In response to our audit inquiry, Department management reported that a new agencywide system, Program Management and Monitoring, was scheduled for release in November 2013. The new system is to be used by the program areas to track both administrative and programmatic monitoring for all contracts.

Absent completion of the required monitoring activities, the Department has reduced assurance that contract providers operated in compliance with contract terms and conditions and that the desired service outcomes were achieved. Similar issues were noted in prior audit reports, most recently in our report No. 2012-183, finding No. 7.

Recommendation: We again recommend that Department management ensure that the required administrative and programmatic monitoring of contracts is completed in accordance with established procedures.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings noted in our report No. 2012-183.

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 operational audit from January 2013 through May 2013 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.

This operational audit focused on JJIS IT controls and selected Department administrative activities. The overall objectives of the audit were:

- To evaluate management's performance in establishing and maintaining internal controls, including controls designed to prevent and detect fraud, waste, and abuse, and in administering assigned responsibilities in accordance with applicable laws, administrative rules, contracts, grant agreements, and guidelines.
- To examine internal controls designed and placed in operation to promote and encourage the achievement of management's control objectives in the categories of compliance, economic and efficient operations, the reliability of records and reports, and the safeguarding of assets, and identify weaknesses in those internal controls.
- To determine whether management had corrected, or was in the process of correcting, all deficiencies disclosed in our report No. 2012-183.
- 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 those programs, activities, or functions 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 transactions, legal compliance matters, records, and controls considered.

As described in more detail below, for those programs, activities, and functions 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 program, activity, or function; 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 transactions and records. Unless otherwise indicated in this report, these transactions and records 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 vendors, and as a consequence, cannot be relied upon to identify all instances of noncompliance, fraud, abuse, or inefficiency.

In conducting our audit we:

- Reviewed applicable laws, rules, regulations, and Department policies and procedures, and interviewed Department personnel to gain an understanding of Department IT general controls and JJIS application controls.
- Obtained an understanding of JJIS IT controls, assessed the risks of those controls, evaluated whether selected general and application IT controls were in place, and tested the effectiveness of the controls.
- Examined documentation related to 25 JJIS program changes made during the period July 2011 through February 2013 to determine whether the program changes had been appropriately authorized, tested, and approved.
- Examined records for 40 users who had access to the JJIS during the period July 2011 through February 2013 to determine whether the Department:
    - Maintained documentation demonstrating that the level of JJIS access granted was appropriate for the user's job responsibilities.
    - Maintained documentation demonstrating that JJIS access was properly approved.
    - Maintained documentation demonstrating that the JJIS users had completed the required training prior to being granted access.
- Examined records for 60 users who had access to the JJIS during the period July 2011 through February 2013 to determine whether the Department maintained documentation demonstrating that level 2 screenings had been conducted for JJIS users.
- Performed analytical procedures to determine whether the Department timely removed access privileges when a user separated from employment or JJIS access was no longer required.

- Inquired of Department personnel and reviewed records to determine whether the Department periodically reviewed user access privileges for appropriateness.
- Reviewed Department records for 25 property items, totaling $72,061, with data storage capabilities that had been disposed of during the period July 2011 through February 2013 to determine whether the disposal had been approved and that any confidential and sensitive information had been appropriately removed from the items prior to their disposal.
- Reviewed Department mobile computing and storage device IT security policies and procedures to determine whether the devices were required to be tracked and, as applicable, encrypted, to safeguard sensitive information.
- Reviewed Department records for 36 contracts, totaling approximately $333.5 million, that were active during the period July 2011 through February 2013, to determine whether administrative and programmatic monitoring was performed in accordance with Department procedures.
- Interviewed Department personnel and reviewed the Department's process to determine whether the Department sufficiently documented that Quality Assurance reviewers met minimum work experience requirements.
- Reviewed Department procedures to determine whether conflict of interest statements were required to be signed by all QA reviewers.
- Reviewed Department policies and procedures, interviewed Department personnel, and reviewed selected records to determine whether the Department's incident review process ensured that reported incidents were accurately and completely recorded, reported, and communicated to Department personnel.
- Reviewed Department policies and procedures, interviewed Department personnel, and reviewed selected records to determine whether Administrative Review Unit procedures ensured that all administrative reviews were completed within 30 days.
- Reviewed Department records to determine whether reconciliations of motor vehicle data in the Florida Equipment Electronic Tracking System to Florida Accounting Information Resource Subsystem (FLAIR) data were completed timely in accordance with the requirements of Department policies and procedures.
- Reviewed Department records to determine if Department staff received, reviewed, and followed up on financial reporting packages due to the Department pursuant to the Florida Single Audit Act requirements.
- Reviewed the Department's State Purchasing Card Program procedures and performed analytical procedures to determine whether the Department timely canceled purchasing cards for 522 cardholders who had separated from Department employment during the period July 2011 through December 2012.
- Performed analytical procedures to identify purchasing cards assigned to Department employees, but not used during the period July 2011 through December 2012.
- Reviewed Department procedures and interviewed Department personnel to gain an understanding of the Department's processes for safeguarding social security numbers maintained in Department records.
- Reviewed Department records to evaluate the appropriateness of FLAIR access privileges granted to Department employees and to determine whether FLAIR access had been timely deactivated for employees who separated from Department employment during the period July 2011 through December 2012.
- 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.

AUTHORITY

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each State agency on a periodic basis. Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENT'S RESPONSE

In a response letter dated September 19, 2013, the Secretary of the Department provided responses to our audit findings and recommendations. The Secretary's response is included as **EXHIBIT A**.

EXHIBIT A
MANAGEMENT'S RESPONSE

FLORIDA DEPARTMENT OF JUVENILE JUSTICE

Rick Scott, Governor **Wansley Walters, Secretary**

September 19, 2013

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 and Selected Administrative Activities. 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 help close some gaps we had in some of our processes.

Sincerely,

Wansley Walters,
Secretary

cc: J. Alex Kelly, Chief of Staff – Signed on behalf of Secretary Walters
Fred Schuknecht, Director of Administration
Scott Morgan, Chief of MIS
Amy Johnson, Director of Program Accountability
Mark Greenwald, Chief of Research and Planning

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 and Selected Administrative Activities

Finding No. 1: Background Screenings

1. *The Department did not always maintain documentation demonstrating that employees and contract providers received background screenings as a condition of employment and prior to being granted JJIS access privileges.*

Response:
Per FDJJ 1800-Background Screening Policy; Employment background screening shall be completed prior to hiring an employee or utilizing the services of a volunteer, mentor, or intern. All contracted provider and Department employees are screened in accordance with Level 2 standards, as set forth in Chapter 435, Florida Statutes, as a condition of employment.

It is the responsibility of the employee supervisor to maintain background screening information on an employee. Once the supervisor receives the background screening results, they contact their local Data Integrity Officer (DIO) to request JJIS training for their employee.

Action Item:
The DIOs will create an "Access Request Form" which will be used for new accounts or permissions increases. A field requiring a date for background screening and who verified the background screen will be required.

Finding No. 2: Authorization of JJIS Access Privileges

2. *Department records did not always demonstrate that JJIS access privileges were limited to authorized users and that users had completed the required JJIS training.*

Response:
It is the Department procedure that the DIOs train all users on JJIS prior to granting system access, and have an approved JJIS and System Access – Change Permissions Request form.

Action Item:
The 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.

Finding No. 3: Deactivation of JJIS Access Privileges

3. *The Department did not always timely deactivate JJIS access privileges upon the users' separation from employers. Additionally, the Department had not deactivated JJIS access privileges for a significant number of inactive user accounts.*

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Response:
The Separation Notification System is used to notify key staff members that an employee is separating from the Department. This triggers the DIOs to terminate the employee's system access.

Action Item:
The system will be modified to automatically deactivate (lock) the user's JJIS account after 30 days of inactivity. After 120 days of inactivity, the system modification will automatically terminate (end-date) the user's JJIS account.

Finding No. 4: JJIS Change Management Controls

4. *The Department's change management process did not always provide for an appropriate separation of duties and the Department did not always adequately document JJIS program change authorizations.*

Response:
Due to the limited amount of resources, Department priorities and staff workload, application development staff is required to carry out multiple duties which cannot always be appropriately separated. The Application Technology Unit has written policy in place for change management to confirm the movement of code from the quality testing environment (QT) to the production environment. This includes oversight and signoff by a Data Processing Manager, Database Administrator, Systems Project Consultant or Application Manager is present before moving code from the QT environment to Production.

Action Item:
The Application manager will ensure that the JJIS change approvals are properly documented. MIS future plans (pending funding availability) are to automate the change management process which includes document routing and an approval component.

Finding No. 5: Confidential Data

5. *Department controls to monitor user access to juveniles' social security numbers in the JJIS could be enhanced.*

Response:
Program changes have been made and have been moved to production to record user information, along with the date and time when a juvenile SSN is fully displayed. Reports have been generated to assist in periodic monitoring of access to juvenile SSNs.

Action Item:
None. These changes were completed before the audit concluded.

Finding No. 6: Purchasing Card Cancellations

6. *The Department did not always timely cancel purchasing cards upon an employee's separation from the Department employment.*

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Response:
Per FDJJ– 1407.05P Purchasing Card Procedures; prior to an employee's separation from employment, the supervisor shall enter the appropriate information into the DJJ Separation Notification System that will in turn notify the Purchasing Card Program Administrator (DJJPCPA) advising them of the effective date of the action. Upon such separation, the cardholder shall return the card to their supervisor. The supervisor will immediately cut the card in half and discard it.

Action Item:
To ensure timely cancellation of separated department employee's P-cards, Finance and Accounting has coordinated with the Bureau of Personnel to receive the termination report for the department on a consistent monthly basis. This extra safeguard is in place to capture separated employees who have separated without using the notification system. While this may still cause a delay in the cancellation of the P-card depending on when the employee separated, Finance and Accounting is also requiring the field liaisons to cut up the PCard and submit to Finance and Accounting for destruction. This practice may assist in minimizing the number of days between separation and cancellation.

Finding No. 7: Disposal of IT Data Storage Media

7. *The Department could not demonstrate that sensitive data was always removed from IT data storage media prior to disposal.*

Response:
The Department recognizes the critical security risks (i.e. identity theft and unauthorized disclosure of confidential information) that are posed by the use of office machines with data storage capabilities.

Action Item:
The Bureau of Management Information Systems (MIS) and the Bureau of General Services will provide guidance for the procurement, operation, and surplus of all devices with data storage capability. In response to the audit finding, going forward, all office machines with data storage media shall be inspected by the Bureau of Management Information Systems (MIS) during the disposition and disposal process to ensure that all data is removed from the device and securely sanitized *before* the device/media is removed from a DJJ facility. Effective immediately, MIS staff shall complete the *Data Storage Media Sanitization/Destruction Form* (Form 1260-1) to document and verify the sanitization of all data storage media. If the device is being surplused a Surplus Certification of State Property (Form 25) must also be completed and attached to form 1260-1. The Department will also begin conducting statewide training via webinars and conference calls to educate staff on the proper procedures and processes for disposing IT equipment.

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 8: Contract Monitoring

1. *The Department's contract monitoring activities continue to need improvement.*

Response:
The Department concurs with this finding and recommendation.

Action Item:
The Department is developing and implementing an automated contract monitoring data system to ensure all Department contracts are monitored timely and outstanding compliance issues are resolved in a timely manner. It is anticipated that this system will be fully implemented in November 2013.