REPORT NO. 2015-087
JANUARY 2015

DEPARTMENT OF CORRECTIONS

CANTEEN OPERATIONS AND PRIOR AUDIT FOLLOW-UP

Operational Audit

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

SECRETARY OF THE DEPARTMENT OF CORRECTIONS

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

Michael D. Crews	From December 17, 2012, through November 30, 2014
Kenneth S. Tucker	Through December 14, 2012

The audit team leader was Jon M. Bardin, CPA, and the audit was supervised by Allen G. Weiner, 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 CORRECTIONS

Canteen Operations and Prior Audit Follow-Up

SUMMARY

This operational audit of the Department of Corrections (Department) focused on canteen operations and also included a follow-up on the findings noted in our report No. 2013-074. Our audit disclosed the following:

CANTEEN OPERATIONS

Finding No. 1: Annual background check rescreenings were not always timely performed for canteen contractor staff.

Finding No. 2: The Department did not always collect administrative processing fees for inmate banking services.

INFORMATION TECHNOLOGY CONTROLS

Finding No. 3: The Department did not always ensure individuals' social security numbers were appropriately protected.

Finding No. 4: As similarly noted in our report No. 2013-074, the Department did not always timely cancel information technology user access privileges upon an employee's separation from Department employment.

Finding No. 5: The Department had not established written procedures requiring employees to periodically back up Department data stored on workstations and laptops and other mobile computing devices.

COURT-ORDERED PAYMENTS

Finding No. 6: The Department did not always document that changes to payee account information were approved by management in accordance with Department policies and procedures. A similar finding was noted in our report No. 2013-074.

BACKGROUND

State law[1] specifies that the purpose of the Department of Corrections (Department) is to protect the public through the incarceration and supervision of offenders and to rehabilitate offenders through the application of work, programs, and services. According to Department records, the Department operates the third largest state prison system in the United States. The Legislature appropriated almost $2.3 billion to the Department for the 2014-15 fiscal year, including funds for more than 23,700 positions. In addition to housing over 100,000 inmates, as of July 2014, the Department supervised over 130,000 offenders on active community supervision or active-suspense community supervision.[2]

[1] Section 20.315(1), Florida Statutes.

[2] Active community supervision refers to the supervision of offenders in the community per the conditions of their supervision. Active-suspense community supervision refers to the supervision of offenders who are unavailable for direct supervision (e.g., incarcerated, in drug treatment, or hospitalized).

FINDINGS AND RECOMMENDATIONS

Canteen Operations

Department rules[3] specify that canteens are to be operated primarily to provide items of convenience to inmates. Beginning in October 2003, the Department outsourced canteen operations to Keefe Commissary Network, LLC (Keefe). The items made available to inmates through the Keefe contract include snacks and toiletries, clothing from approved catalogs, and MP3 players, accessories, and songs. According to Department records, during the period July 2012 through February 2014, sales in Department institution canteens totaled approximately $133.31 million and catalog sales totaled $868,474. During that same period, the Department received per diem revenue[4] from Keefe totaling approximately $50.66 million. In addition, the Department received MP3 program commissions from Keefe totaling $940,412 related to MP3 program sales totaling approximately $5.99 million. The Department's canteen operation services contract with Keefe expires March 31, 2015.

The canteens operate on a cashless system whereby inmates use photo identification cards in the same manner as bank debit cards to make canteen purchases. Each inmate with a sufficient account balance in the Department's Inmate Bank Trust Fund (and who is not otherwise restricted) is allowed to make canteen purchases up to a set purchase limit.[5] The purchase limit is set by the Department Secretary but, pursuant to State law,[6] weekly inmate draws for canteen purchases cannot exceed $100. According to the canteen operation services contract, items obtained by inmates from Department-approved catalogs or the MP3 program are excluded from the purchase limit.

The canteen operation services contract specifies that Keefe is to provide one full-time employee at each of the Department's major institutions (regardless of the number of canteens operating at the institution) to oversee canteen operations. Keefe may use inmate labor to assist in daily canteen operations; however, the Department is to select, provide, and pay the inmates. As of February 28, 2014, there were 373 canteens in operation at the Department's major institutions.

Finding No. 1: Background Check Rescreenings

The Department's contract with Keefe specifies that Keefe staff assigned to perform services pursuant to the contract are subject to Statewide and national criminal history background checks. The background checks are to be conducted by the Department and may occur or re-occur at any time during the contract period. The contract also specifies that, to facilitate the background checks, Keefe is to provide the Department, upon request, the personal data (e.g., name, race, gender, date of birth, social security number) of its applicable staff. To mitigate potential security risks, the contract provides that the Department may use the background check results to disqualify or remove Keefe staff from any work on the contract.

Prior to the placement of Keefe staff at a Department institution, the Department conducted Statewide and national criminal history background checks on the applicable Keefe staff. The Department also elected to rescreen Keefe staff annually on or near the anniversary date of the staff person's initial background check. The Department maintained an electronic list to track the dates the background check rescreenings were due for Keefe staff.

[3] Department Rule 33-203.101(1), Florida Administrative Code.
[4] The Department's contract with Keefe requires Keefe to compensate the Department $0.96 per day per inmate (per diem) based on the Department's average daily population.
[5] Department Rule 33-203.101, Florida Administrative Code.
[6] Section 945.215(1)(f), Florida Statutes.

Our examination of background check records for the 132 Keefe employees hired and assigned to perform services pursuant to the contract during the period July 1, 2012, through May 1, 2014, disclosed that the names and annual rescreening dates for 4 Keefe employees were not included on the Department's electronic background screening list. Consequently, 2 of the 4 Keefe employees were not subject to timely annual rescreenings. The rescreenings for these 2 Keefe employees occurred 131 days and 3 years 6 months, respectively, after the rescreenings were due. Additionally, we noted that another Keefe employee who terminated employment was rehired 65 days after the expiration of his last background check and was not rescreened until 107 days after rehire, and subsequent to our audit inquiries.

Timely and appropriate background checks and rescreenings are necessary to ensure that the Keefe staff assigned to perform services related to the contract have appropriate backgrounds. Absent the maintenance of a complete and accurate list of the Keefe staff approved to perform contract services, the Department has reduced assurance that timely background check rescreenings will be conducted.

Recommendation: We recommend that Department management ensure that annual background check rescreenings are timely conducted for applicable Keefe staff.

Finding No. 2: Uncollected Administrative Processing Fees

State law[7] and Department rules[8] provide that the Department may charge inmates an administrative processing fee of up to $6 each month for banking services to offset the cost of Department operations. The fee is to be based upon an inmate's account activity each month, whereby the Department is to charge inmates 1 percent of their total weekly canteen purchases[9] and $0.50 per deposit.[10] State law specifies that if an inmate account has a zero balance at the end of a billing cycle, a hold is to be established to collect the processing fee when funds become available.

As part of our audit, we examined documentation related to banking transactions made by 113 inmates. For each inmate, we selected the month during the period July 2012 through February 2014 in which the inmate's canteen activity was the highest to determine whether the Department had collected processing fees in accordance with State law and Department rules. Our audit procedures disclosed that for 47 of the 113 inmates, the Department was unable to collect the 1 percent processing fees, totaling $16, because the inmates' accounts had insufficient funds. In response to our audit inquiry, Department management indicated that inmate bank accounts are established such that if an inmate receives a deposit within a week after the Department is unable to collect processing fees due to insufficient funds, the outstanding processing fees are withdrawn from the deposited amount. However, Department management acknowledged that if an inmate does not receive a deposit within a week, the hold required by State law is not placed on the inmate's account and the outstanding processing fees are not collected.

In response to our audit inquiry, Department management estimated that approximately $116,000 in administrative processing fees each year went uncollected. Absent appropriate controls, including procedures to establish inmate account holds, Department management has limited assurance that administrative processing fees will be collected as provided by State law.

[7] Section 944.516(1)(h), Florida Statutes.
[8] Department Rule 33-203.201(1)(h), Florida Administrative Code.
[9] The 1 percent charge is not assessed for catalog or MP3 program purchases.
[10] Inmates who were honorably discharged from the U.S. military are not subject to the fees.

Recommendation: We recommend that Department management establish appropriate controls, including procedures to establish inmate account holds, to ensure that administrative processing fees for inmate banking services are collected as provided by State law.

Information Technology Controls

As State agencies rely on information technology (IT) to record, process, maintain, and report essential financial and program information, State agency management is responsible for establishing effective IT controls that provide reasonable assurance regarding the confidentiality, integrity, and availability of data and IT resources. The absence of effective IT controls can result in significant risks to State agency operations and assets. Such risks include, for example, the risks of unauthorized disclosure of sensitive information, inappropriate data modification, and destruction of data or IT resources.

Finding No. 3: Confidential and Exempt Information Sent by E-Mail

State law[11] provides that social security numbers (SSNs) held by a State agency are confidential and exempt from public record disclosure requirements. Agency for Enterprise Information Technology (AEIT) rules[12] state that State agencies are to exercise due diligence to protect confidential and exempt information by using appropriate administrative, technical, and physical controls and specifically require State agencies to encrypt confidential and exempt information sent by e-mail.

Our review of Department policies and procedures disclosed that Department management had not established policies and procedures specifically requiring the encryption of all e-mails containing confidential or exempt information. In response to our audit inquiry, Department management indicated that the Department automatically encrypts certain e-mails, including those containing information governed by the Health Insurance Portability and Accountability Act (HIPAA), and Department staff have the option of encrypting e-mails containing other confidential and exempt information.

During our audit tests of Department canteen operations and related background check documentation, we noticed 11 separate unencrypted e-mails, generated or forwarded by Department staff that contained the SSNs of 40 individuals. These 11 e-mails were sent or forwarded by Department staff to other Department or Keefe staff 38 times during the period February 2013 through April 2014.

Department policies and procedures requiring the encryption of all e-mails containing confidential and exempt information would provide greater assurance that such information is protected against inappropriate disclosure.

Recommendation: We recommend that Department management enhance policies and procedures to require the encryption of all e-mails which include confidential and exempt information.

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

[12] AEIT Rule 71A-1.006(7), Florida Administrative Code. Effective July 1, 2014, Chapter 2014-221, Laws of Florida, created the Agency for State Technology (AST) within the Department of Management Services and authorized a type two transfer of all records; property; administrative authority; administrative rules in Chapters 71A-1 and 71A-2, Florida Administrative Code; and existing contracts of the Agency for Enterprise Information Technology (AEIT) to the AST.

Finding No. 4: Access Controls

The Department used the Operational Review Report Writer (Report Writer), a stand-alone IT application, to maintain the standards to be evaluated during the conduct of unannounced security audits and operational reviews. The Department also used Report Writer to generate reports for unannounced security audits and operational reviews, corrective action plans, and corrective action plan follow-ups.

The Department limited access to Report Writer to designated employees and contractors through established procedures[13] requiring requests and approvals be submitted through a Web-based application and restricting Report Writer access to users with Department network access. Effective IT access controls include provisions to timely remove employee access privileges when access is no longer needed for the performance of job duties or employment terminations occur. Department procedures specified that, to remove a user's access to an IT application or the Department network, the user's supervisor was to submit a Web-based security access request within 3 business days of a change in job duties or employment termination.

In our report No. 2013-074, finding No. 4, we disclosed that user access to Report Writer was not always timely canceled when employees separated from Department employment. As part of our audit follow-up procedures, we compared the active Report Writer user accounts as of April 21, 2014, to a People First[14] listing of employees who had separated from Department employment during the period July 1, 2012, through April 16, 2014. We found that one former employee's Report Writer user access privileges had not been canceled. In addition, this former employee's network access was not canceled until 54 business days after the employee's date of separation from Department employment. In this instance, a security access request to revoke network access privileges was not timely submitted by the user's supervisor.

Delays in canceling user access privileges increases the risk of inappropriate access to IT resources and unauthorized disclosure, modification, or destruction of Department data and IT resources.

Recommendation: To minimize the risk of compromising Department data and IT resources, we again recommend that Department management ensure that IT access privileges are canceled immediately upon a user's separation from Department employment.

Finding No. 5: Periodic Data Back-Up

Effective data management helps ensure the quality, timeliness, and availability of operational data. Effective data management includes the identification of data requirements and the establishment of effective procedures to manage the media library, backup and recovery of data, and proper disposal of media. AEIT rules[15] require every State agency to develop procedures to ensure that agency data, including unique copies of data stored on workstations and mobile computing devices, is backed up.

We noted that the Department had not established written procedures requiring employees to periodically back up workstation and mobile computing device data to a network server and, in response to our audit inquiry, Department management indicated that the number of employees who did not back up their data could not be determined.

[13] Department Procedure 206.007, *User Security for Information Systems*.
[14] People First is a Web-based, self-service personnel information system utilized by employees, managers, human resource professionals, and retirees to manage most of the State's human resource functions.
[15] AEIT Rule 71A-1.012(2), Florida Administrative Code.

However, Department management also indicated that they would develop written procedures to provide guidance on the backup of data to Department servers.

According to Department property records as of October 31, 2014, the Department had 1,280 workstations and laptop computers, as well as a large number of other mobile computing devices (e.g., tablets and smartphones), each with the potential to have unique data stored on it. Absent implementation of procedures requiring that Department data, including data stored on workstations and laptops and other mobile computing devices, is timely and appropriately backed up, the Department has reduced assurance that data stored on such devices will be available to support Department operations.

Recommendation: We recommend that Department management implement procedures to require that data stored on Department workstations and laptops and other mobile computing devices be timely and appropriately backed up.

Court-Ordered Payments

Offenders are sometimes required by courts to make restitution payments to victims and to reimburse counties and other parties for incurred costs. Inmates are required to make the restitution payments if they are employed while imprisoned, and community offenders must satisfy restitution payments as a condition of their probation.[16] The Department is tasked with collecting inmate restitution payments and remitting appropriate amounts to parties as described in court orders.

Finding No. 6: Payee Account Changes

The Court-Ordered Payment System (COPS) is an ancillary application of the Department's Offender Based Information System (OBIS) and is used to track the collection and payment of offender monetary obligations imposed by the court or releasing authority. Department staff enter the original court order information, including payee information and amounts due to each payee, into COPS and, pursuant to Department policies and procedures, no changes or updates to payee account information may be made without supervisor approval on a Change Order form.

In our report No. 2013-074, finding No. 5, we disclosed that moneys collected from offenders were not always timely disbursed to the designated beneficiaries (e.g., victims, courts, and State agencies) in accordance with governing laws. As part of our audit follow-up procedures, we examined Department records for 20 undisbursed amounts in COPS and noted that, for 14 of the amounts, changes to payee account information had been made during the period July 2012 through February 2014. However, Department staff could not provide the approved Change Order forms for 9 of the 14 changes. In response to our audit inquiry, Department management provided various explanations, such as, staff did not always create the Change Order forms as required, the change was made in error, or the applicable Change Order form could not be located.

Documentation of supervisory approval of changes to payee account information would better demonstrate that only authorized changes are made to payee account information in COPS. Unauthorized changes to payee account information may result in victims and other applicable parties not receiving court-ordered restitution and payments.

[16] Sections 945.091(6)(a), 946.002(2)(b), and 948.03(1)(f), Florida Statutes.

Recommendation: We recommend that Department management ensure that only those changes supported by a properly completed and approved Change Order form are made to payee account information in COPS. We also recommend that Department management ensure that Change Order forms are appropriately maintained.

PRIOR AUDIT FOLLOW-UP

Except as discussed in the preceding paragraphs, the Department had taken corrective actions for the findings included in our report No. 2013-074.

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 February 2014 through August 2014 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 canteen operations, correctional officer training, expenditures, and oversight of security operations. 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 other 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 identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

Our audit also included steps to determine whether management had corrected, or was in the process of correcting, all deficiencies noted in our report No. 2013-074.

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:

- Performed inquiries, observations, and inspections of documents and records to obtain an understanding of correctional officer training requirements. Determined whether the Department had sufficient controls to ensure correctional officers and correctional probation officers (officers) received adequate training to safeguard the Department, its employees, inmates, and the general public.
- Examined Department records for 40 correctional officers hired during the period July 2012 through February 2014 to determine whether the officers received 40 hours of new employee orientation in accordance with the Adult Correctional Institutions Manual of Standards.
- Examined Department records for 40 correctional officers employed as of June 28, 2013, to determine whether the training the officers received satisfied the requirements of all applicable laws and regulations.
- Analyzed Department training summary reports for the period July 2012 through June 2014 to determine whether the Department as a whole had met the applicable training requirements.
- From the population of 938,609 expenditures, totaling $1,820,856,883, made during the period July 2012 through June 2013 and included in per diem calculations, examined Department records for 203 expenditures, totaling $23,454,892, to determine whether the expenditures were in the correct amounts and appropriately included in the per diem calculations.
- From the population of 204,758 expenditures, totaling $484,678,895, made during the period July 2012 through June 2013 and excluded from per diem calculations, examined Department records for 25 expenditures, totaling $152,367,969, to determine whether the expenditures were properly excluded from the per diem calculations.
- Analyzed Department expenditure data for the 2010-11, 2011-12, and 2012-13 fiscal years to determine if there were any significant unexpected changes or trends in Department expenditures and evaluated the reasonableness of explanations for such changes or trends.
- Examined documentation for one month of canteen purchases, totaling $4,816, made by 38 inmates during the period July 2012 through February 2014 to determine whether the purchases were made in accordance with applicable rules and guidelines, and charged to the inmates in the correct amounts.
- Obtained an understanding of selected information technology (IT) controls related to the operation of the Inmate Trust Fund, assessed the relative control risks, evaluated whether selected general and application IT controls were in place, and tested the effectiveness of the controls.
- Examined Department records for 114 inmate bank accounts that were open during the period July 2012 through February 2014 to determine whether deposits, withdrawals, and administrative fees were processed accurately and in accordance with applicable laws and regulations.

- Examined documentation for 25 Inmate Trust Fund grievances made during the period July 2012 through February 2014 to determine whether the Department appropriately investigated the grievances.
- Analyzed weekly inmate canteen purchase data for the period July 2012 through February 2014 to determine whether an inmate's weekly canteen purchases exceeded the $100 purchase limit.
- Analyzed Department data and records for 20 quarterly catalog purchases that exceeded $75 during the period July 2012 through February 2014 to determine whether the purchases were reasonable and did not violate Department rules.
- Analyzed MP3 program purchase data for the period July 2012 through February 2014 to determine whether the Department received the appropriate amount of MP3 program commissions from Keefe.
- Examined documentation related to 20 months of canteen per diem revenue, totaling $50,664,457, due from Keefe for the period July 2012 through February 2014 to determine whether the Department received the correct amounts.
- Examined Department monitoring records related to the Department's canteen operation services contract with Keefe to determine whether the Department monitored Keefe's performance in accordance with Department procedures.
- Examined Department records for 132 Keefe employees performing services pursuant to the Department canteen operation services contract during the period July 1, 2012, through May 1, 2014, to determine whether the Department had timely obtained and reviewed initial background screenings and subsequent annual rescreenings for the Keefe employees.
- Examined Department records for 25 inmate canteen operators employed during the period July 2012 through February 2014 to determine if the inmate was approved by the Inmate Classification Team as an inmate canteen operator prior to beginning work.
- Performed walkthroughs of canteens at two Department correctional institutions to gain an understanding of canteen operations and controls and to determine whether the controls were properly designed and implemented.
- Evaluated Department actions taken to correct the deficiencies noted in our report No. 2013-074. Specifically, we:
    - Examined Security Review Committee meeting notes from May 2013 through May 2014 and other related documentation to determine whether the Department had reestablished the Security Review Committee and complied with the provisions of Section 944.151, Florida Statutes.
    - Examined Department records for seven unannounced security audits and three operational reviews performed during the period January 2013 through May 2014 to determine whether the Department was timely conducting audits and reviews of correctional institutions and other correctional facilities.
    - Examined Department records for 20 Report Writer active users as of April 21, 2014, to determine whether the users' access was appropriately granted.
    - Compared an April 2014 listing of 391 active Report Writer users to a listing of employees who had separated from Department employment during the period July 1, 2012, through April 16, 2014, and determined whether the former employees' Report Writer access had been timely canceled.
    - Selected from the 11,604 Court-Ordered Payments System (COPS) accounts with undisbursed funds, totaling $1,727,606 as of June 5, 2014, 20 accounts with undisbursed funds totaling $123,626 and examined Department records to determine whether the undisbursed funds were timely investigated.
    - Examined Department records for ten COPS accounts not charged administrative fees during the period July 1, 2012, through June 10, 2014, to determine whether the Department had appropriate justification for not collecting the statutorily provided 4 percent administrative processing fee.

- Observed, documented, and evaluated the effectiveness of selected Department processes and procedures for:
  - Department purchasing and cash management activities.
  - The management of Florida Single Audit activities in accordance with State law.
- 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 January 12, 2015, the Secretary of the Department provided a response to our audit findings and recommendations. The Secretary's response is included as **EXHIBIT A**.

EXHIBIT A
MANAGEMENT'S RESPONSE

FLORIDA
DEPARTMENT of
CORRECTIONS

Changing Lives to Ensure a Safer Florida

Governor
RICK SCOTT

Secretary
JULIE L. JONES

501 South Calhoun Street, Tallahassee, FL 32399-2500

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

January 12, 2015

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

Dear Mr. Martin:

In accordance with Section 11.45(4)(d), Florida Statutes, I am enclosing the Department's response to the preliminary and tentative findings and recommendations contained in the audit of the Department of Corrections, Canteen Operations and Prior Audit Follow-Up. This response reflects the specific action taken or contemplated to address the findings cited in your report.

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

Sincerely,

Julie L. Jones
Secretary

Enclosure

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS AUDIT OF THE DEPARTMENT OF CORRECTIONS, CANTEEN OPERATIONS AND PRIOR AUDIT FOLLOW-UP.

Finding No. 1: Annual background check rescreenings were not always timely performed for canteen contractor staff.

Recommendation: We recommend that Department management ensure that annual background check rescreenings are timely conducted for applicable Keefe staff.

Agency Response: *The Bureau of Contract Management and Monitoring has made changes to standard contract language of all new and renewal contracts. Level II background checks are valid for five years and any arrest during that period sends an automatic notification to the Department via FDLE and our ORI terminal. See contract language excerpt:*

"When providing services within a correctional setting, the Contractor shall obtain a Level II background screening (which includes fingerprinting to be submitted to the Federal Bureau of Investigation (FBI)), and results must be submitted to the Department prior to any current or new Contractor staff being hired or assigned to work under the Contract. The Contractor shall bear all costs associated with this background screening." Page 5 Section E.

The Bureau of Contract Management and Monitoring corrective actions have been implemented by the Department for all facilities. Our actions strengthen the security of our facility operations and ensure public safety.

Finding No. 2: The Department did not always collect administrative processing fees for inmate banking services.

Recommendation: We recommend that Department management establish appropriate controls, including procedures to establish inmate account holds, to ensure that administrative processing fees for inmate banking services are collected as provided by State law.

Agency Response*: We concur with the audit finding and are currently implementing the Auditor General recommendation.*

1

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 3: The Department did not always ensure individuals' social security numbers were appropriately protected.

Recommendation: We recommend that Department management enhance policies and procedures to require the encryption of all e-mails which include confidential and exempt information.

Agency Response: *Policies have been changed to prohibit social security numbers from being sent outside the agency un-encrypted. Health Services uses encrypted email to send sensitive health information. All electronic transmission and tape storage of social security numbers is now encrypted.*

Finding No. 4: As similarly noted in our report No. 2013-074, the Department did not always timely cancel information technology user access privileges upon an employee's separation from Department employment.

Recommendation: To minimize the risk of compromising Department data and IT resources, we again recommend that Department management ensure that IT access privileges are canceled immediately upon a user's separation from Department employment.

Agency Response: *The Bureau of Security Operations has been granted access to Department's separated employees' list database which is generated via People First. This database will be compared to the Report Writer user list, to remove access for separated employees.*

The access security section of the Office of Information Technology regularly runs separation reports from PeopleFirst to ensure accounts have been closed. A more concentrated effort of Security Awareness training with the field security coordinators is in the planning stage.

Finding No. 5: The Department had not established written procedures requiring employees to periodically back up Department data stored on workstations and laptops and other mobile computing devices.

Recommendation: We recommend that Department management implement procedures to require that data stored on Department workstations and laptops and other mobile computing devices be timely and appropriately backed up.

Agency Response: *Language has been submitted to policy section to address this finding. It is the standard operating procedure that all data be stored on servers for nightly backup. In the unusual circumstance data is stored on a workstation or laptop hard drive, it is the users responsibility to back the data up manually. Further training will enforce the policy of not storing data on desktops and laptops without a backup procedure in place.*

EXHIBIT A (CONTINUED)
MANAGEMENT'S RESPONSE

Finding No. 6: The Department did not always document that changes to payee account information were approved by management in accordance with Department policies and procedures. A similar finding was noted in our report No. 2013-074.

Recommendation: We recommend that Department management ensure that only those changes supported by a properly completed and approved Change Order form are made to payee account information in COPS. We also recommend that Department management ensure that Change Order forms are appropriately maintained.

Agency Response: *On July 16, 2014, during a statewide meeting with Circuit Administrators, Assistant Regional Directors and Regional Directors, COPS Change Forms was discussed due to deficiencies recently brought to our attention by the auditors. Everyone was reminded of the importance in following COPS procedures, particularly in ensuring COPS change forms are completed, reviewed and signed by a supervisor, and maintained in the active file or imaged upon closure for future reference and documentation. This will ensure that only authorized changes are made to payee accounts and may assist in appropriate distribution of payments.*