



Changing Lives to  
Ensure a Safer Florida

FLORIDA  
DEPARTMENT of  
CORRECTIONS

Governor

**RICK SCOTT**

Secretary

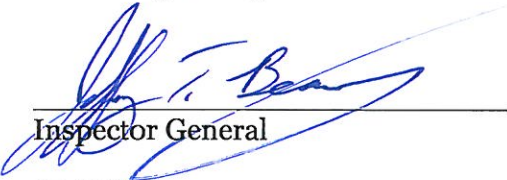
**JULIE L. JONES**

501 South Calhoun Street, Tallahassee, FL 32399-2500

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

**TO:** Julie L. Jones, Secretary  
**FROM:** Jeffery T. Beasley, Inspector General  
**DATE:** July 22, 2015  
**SUBJECT:** FOLLOW-UP AUDIT REPORT #A15032F – AUDITOR GENERAL’S CANTEEN OPERATIONS AND PRIOR AUDIT FOLLOW-UP OPERATIONAL AUDIT, REPORT #2015-087

The Bureau of Internal Audit performed a follow-up audit to the Auditor General’s Canteen Operations and Prior Audit Follow-Up Operational Audit, Report # 2015-087, issued in January 2015. The objectives of the follow-up were to determine if corrective actions were taken on reported audit findings and whether the actions taken corrected or should correct the findings identified in the original report. The scope of the follow-up consisted of obtaining from the Bureaus of Contract Management and Monitoring, Finance and Accounting, and Security Operations and the Offices of Information Technology and Community Corrections a written response along with documentation of corrective action taken to implement the audit recommendations. The Bureau of Internal Audit has evaluated the follow-up responses and will continue to follow-up on two of the six findings identified in the original report.

  
Inspector General

JB/PS/kj  
Attachment

Stacy Arias, Chief of Staff  
Timothy Cannon, Deputy Secretary of Institutions  
Kimberly Banks, Chief Financial Officer  
Ricky Dixon, Assistant Secretary of Institutions  
Jenny Nimer, Deputy Secretary of Community Corrections  
Lincoln Quinton, Director of Information Technology  
Kelley Scott, Director of Administration  
Richard Comerford, Director of Institutional Support  
Michael Deariso, Chief of Finance and Accounting  
William Smith, Chief of Contract Management and Monitoring  
Wes Kirkland, Chief of Security Operations  
Shari Britton, Chief of Probation & Parole Field Services and Interstate Compact  
Kenneth Sumpter, Deputy Inspector General  
Office of the Chief Inspector General  
Joint Legislative Auditing Committee

*FLORIDA DEPARTMENT OF CORRECTIONS*

***Follow-up of Auditor General's Report 2015-087  
Department of Corrections  
Canteen Operations and Prior Audit Follow-up  
Operational Audit***

*Jeffery T. Beasley, Inspector General**Report #A15032F**Paul R. Strickland, Chief Internal Auditor**July 22, 2015***BACKGROUND**

State law 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.

In January 2015, the Office of the Auditor General published Report # 2015-087, Department of Corrections, Canteen Operations and Prior Audit Follow-up, Operational Audit.

**OBJECTIVES**

The follow-up objectives were to determine:

- if corrective actions were taken on reported audit findings; and
- whether the actions taken corrected or should correct the findings in the original audit report.

**SCOPE AND METHODOLOGY**

A request was made to the Bureaus of Contract Management and Monitoring, Finance and Accounting, Security Operations, and the Offices of Information Technology and Community Corrections for a written response of corrective action taken to implement the audit recommendations.

## RESULTS OF AUDIT

### **Finding No. 1: Annual background check re-screenings were not always timely performed for canteen contractor staff.**

**Recommendation:** Department management ensure that annual background check re-screenings are timely conducted for applicable Keefe staff.

**Management's Original 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 Investigations (FBI)), and results must be 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.”*

**Management's Follow-Up Response:** *The Bureau of Contract Management and Monitoring corrective actions have been implemented by the Department for all facilities. A current list of approved vendors/contractors is maintained by the Bureau on the DC Web and updated monthly. Our actions strengthen the security of our facility operations and ensure public safety.*

**Bureau of Internal Audit Comments:** *The Bureau of Contract Management and Monitoring has taken steps to address the finding. Audit staff verified that there is a list of approved contractors on the DC website. This finding was in regards to the Keefe Inmate Canteens contract. A review of the current contractors list dated 6/30/2015 for Trinity Services, the current inmate canteen contract, disclosed that all staff are current on background screenings. In addition, audit staff judgmentally selected three original contracts and verified that the language excerpt provided in the original response was contained in the contracts. No further follow-up will be conducted.*

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

**Recommendation:** 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.

**Management's Original Response:** *We concur with the audit finding and are currently implementing the Auditor General recommendation.*

**Management's Follow-Up Response:** *The Department modified the procedure of collecting of 1% weekly fee for gross canteen sales by placing a hold on an inmate's account for any uncollected balance and subsequently satisfying the hold from the inmate's next deposit. This programming change went into effect on March 9, 2015 and corrects the issue identified in the finding.*

**Bureau of Internal Audit Comments:** *The Bureau of Finance and Accounting has taken steps to address the finding. Audit staff obtained a sample of inmate accounts and confirmed that liens are being placed on the inmate bank account for bank processing fees when an inmate's account has a zero balance. For those inmates for whom a deposit was made had a deduction for the amount owed. No further follow-up necessary.*

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

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

**Management's Original 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.*

**Management's Follow-Up Response:** *Verified with the SSRC, all data is encrypted at rest and also during backup tape transit. OIT has installed encrypted email (Iron Port). Iron port is currently being used by health services staff to send sensitive and confidential information outside of the Department. According to Security Operations it is standard operating procedure that any user sending sensitive and confidential information outside the Department should acquire an account on the encrypted email server. OIT verified with Security Operations the sending of sensitive and confidential information via un-encrypted email has ceased. The Department is also seeking funding to move the email system to Microsoft Office 365. This will give the Department more options for encrypting email.*

**Bureau of Internal Audit Comments:** *The Office of Information Technology has taken steps to address the finding. No further follow-up will be conducted.*

**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:** Department management ensure that IT access privileges are canceled immediately upon a user's separation from Department employment to minimize the risk of compromising Department data and IT resources.

**Management's Original 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 People First to ensure accounts have been closed. A more concentrated effort of Security Awareness training with the filed security coordinators is in the planning stage.*

**Management's Follow-Up Response:** *The Bureau of Security Operations compares the list of separated employees with the Report Writer Program database weekly. Security Operations with the corporation of OIT has developed a program that will compare the list of separated employees to the approved user list for the Report Writer Program. This program removes user permissions to prevent them from using the Report Writer Program after separation.*

**Bureau of Internal Audit Comments:** *The Bureau of Security Operations has taken steps to address the finding. Audit staff observed the process implemented by the Bureau of Security Operations. No further follow-up is necessary.*

**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:** 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.

**Management's Original Response:** *Language has been submitted to the 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 circumstances data is stored on a workstation or laptop hard drive, it is the user's 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.*

**Management's Follow-Up Response:** *The following language was submitted to be included in Policy 206.077 on March 5, 2015. "It is not recommended users store any data on their workstation or laptop local C: drive. All data should be stored on the users' assigned server. If data is stored on a device's local drive, it is the responsibility of the user to ensure the data is backed up to their assigned server on a weekly basis."*

***Bureau of Internal Audit Comments:*** *The Office of Information Technology is taking steps to address the finding. DC Procedure 206.007, User Security for Information Systems, is in review for update referenced in the follow-up response. Once finalized, the action taken should correct the finding in the original report. Further follow-up is necessary and will be conducted.*

**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:** 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. Also, Department management ensure that Change Order forms are appropriately maintained.

***Management's Original 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 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.*

***Management's Follow-Up Response:*** *Since July 2014, the following actions have occurred within Community Corrections to improve the approval process and maintenance of COPS change forms:*

- 1. In October 2014, statewide COPS Training classes began with 4 unique classes being held in each circuit for officers, support staff, supervisors and an advanced class for staff who handle COPS Exceptions and complicated COPS issues. The training is ongoing and will conclude in October 2015. The training is being presented in each circuit at one or more locations by three (3) COPS experts in Central Office. During this in-depth training, the trainers are reminding staff that all COPS change forms must be reviewed and approved by a supervisor and maintained (in the offender file or electronically - scanned) for future reference and auditing purposes.*
- 2. The COPS Technical Manual has been updated to a more user friendly, updated version effective May 21, 2015.*
- 3. Discussions have been held to consider adding COPS (and OBIS) as an "Issues" workgroup for a group of field staff to review current COPS processes and discuss ways to improve them.*

***Bureau of Internal Audit Comments:*** *The Office of Community Corrections has taken steps to address the finding. As stated in the Office of Community Corrections response training is ongoing and expected to be completed in October 2015. Upon completion of the training, audit staff will conducted further follow-up to see if the action taken corrected the finding cited in the report.*

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