REPORT NO. 2013-074
JANUARY 2013

DEPARTMENT OF CORRECTIONS

OVERSIGHT OF SECURITY 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. During the period of our audit, the following individuals served as Secretary:

Ken Tucker	From August 25, 2011
Edwin Buss	From February 14, 2011, through October 6, 2011
Walter McNeil	From February 8, 2008, through February 11, 2011

The audit team leader was Tammy Williams, CPA, and the audit was supervised by Stan Mitchell, CPA. Please address inquiries regarding this report to Christi Alexander, CPA, Audit Manager, by e-mail at christialexander@aud.state.fl.us or by telephone at (850) 487-9069.

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) 487-9175; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

DEPARTMENT OF CORRECTIONS

Oversight of Security Operations and Prior Audit Follow-Up

SUMMARY

This operational audit of the Department of Corrections (Department) focused on the Department's oversight of security operations at State correctional institutions and private correctional facilities. Our audit also included a follow-up on the findings disclosed in report No. 2010-147 related to court-ordered payments.

OVERSIGHT OF SECURITY OPERATIONS

Finding No. 1: The Security Review Committee required by Section 944.151(1), Florida Statutes, did not function as intended by State law.

Finding No. 2: The Department did not have a centralized tracking mechanism in place to ensure that all audits, reviews, and follow-up visits were timely performed and that security deficiencies were timely corrected. Additionally, the Department did not always maintain appropriate documentation or utilize tools to promote the completeness and tracking of Department security oversight efforts.

Finding No. 3: The Department had not performed annual security audits of work release centers in accordance with State law.

INFORMATION TECHNOLOGY

Finding No. 4: Department logical access controls related to a critical information technology application needed enhancement.

PRIOR AUDIT FOLLOW-UP – COURT-ORDERED PAYMENTS

Finding No. 5: Although the Department had implemented some corrective actions related to the court-ordered payment process, deficiencies still existed.

BACKGROUND

The Department operates under the provisions of Section 20.315 and Chapters 944, 945, 946, 948, and 958, Florida Statutes. The purpose of the 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. The Department's mission is to protect the public safety, ensure the safety of Department personnel, and provide proper care and supervision of all offenders under its jurisdiction while assisting, as appropriate, their reentry into society.

According to Department records, the Department operates the third largest state prison system in the United States with more than 23,700 employees and a 2011-12 State fiscal year budget of approximately $2.2 billion.[1] In addition to housing over 100,000 inmates, as of July 2012, the Department supervised approximately 146,000 offenders on active or active-suspense community supervision.[2] To administer community supervision, the Department has divided the State into two Regions, each supported by a Regional Office. The Community Corrections Central Office, located in Tallahassee, provides support, direction, and operational oversight to the Regional Offices and field staff.

[1] Department Web site (http://www.dc.state.fl.us.html).

[2] Active community supervision refers to the supervision of those offenders who are being supervised 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).

As shown in Table 1, during the 2010-11 State fiscal year, there were 140 correctional institutions and facilities Statewide, 70 in each of the Department's two regions.

Table 1
Correctional Institutions and Facilities by Region

Type of Institution	Northern Region	Southern Region	Totals
State Correctional Institutions	30	24	54
Private Correctional Facilities	5	2	7
Work Camps, Forestry Camps, Treatment Center, and Boot Camp	26	15	41
Road Prisons	-	4	4
Work Release Centers	9	25	34
Totals	**70**	**70**	**140**

Source: Department's *2010-11 Agency Statistics*.

FINDINGS AND RECOMMENDATIONS

Oversight of Security Operations

Pursuant to State law,[3] the Department is responsible for the security of correctional institutions and facilities. In the law, the Legislature established that the security of the State's correctional institutions and facilities is critical to ensure public safety and to contain violent and chronic offenders until offenders are otherwise released from the Department's custody pursuant to law. At a minimum, the Secretary of the Department shall appoint a Security Review Committee (Committee) to be composed of the inspector general, the Statewide security coordinator, the regional security coordinators, and three wardens and one correctional officer.

The Committee is to perform the following tasks:

- Establish a periodic schedule for the physical inspection of buildings and structures of each State and private correctional institution to determine security deficiencies. In scheduling the inspections, priority must be given to older institutions, institutions that house a large proportion of violent offenders, and institutions that have experienced a significant number of escapes or escape attempts in the past.
- Conduct or cause to be conducted announced[4] and unannounced comprehensive security audits of all State and private correctional institutions. In conducting the security audits, priority must be given to older institutions, institutions that house a large proportion of violent offenders, and institutions that have experienced a significant number of escapes or escape attempts in the past. At a minimum, the audit must include an evaluation of the physical plant, landscaping, fencing, security alarms and perimeter lighting, and inmate classification and staffing policies. Each correctional institution must be audited at least annually, with the report and general survey findings reported annually to the Governor and the Legislature.
- Adopt and enforce minimum security standards and policies that include, but are not limited to:
  - Random monitoring of outgoing telephone calls by inmates.
  - Maintenance of current photographs of all inmates.
  - Daily inmate counts at varied intervals.
  - Use of canine units, where appropriate.

[3] Section 944.151, Florida Statutes.
[4] The Department refers to announced security audits as operational reviews.

- Use of escape alarms and perimeter lighting.
- Florida Crime Information Center/National Crime Information Center capabilities.
- Employment background investigations.

- Annually make written prioritized budget recommendations to the Secretary that identify critical security deficiencies at major correctional institutions.
- Investigate and evaluate the usefulness and dependability of existing security technology at the institutions and new technology available and make periodic written recommendations to the Secretary on the discontinuation or purchase of various security devices.
- Contract, if deemed necessary, with security personnel, consulting engineers, architects, or other security experts the Committee deems necessary for security audits and security consulting services.
- Establish a periodic schedule for conducting announced and unannounced escape simulation drills.
- Maintain and produce quarterly reports with accurate escape statistics.
- Adopt, enforce, and annually evaluate the emergency escape response procedures, which at a minimum must include the immediate notification and inclusion of local and State law enforcement through a mutual aid agreement.
- Submit in an annual legislative budget request a prioritized summary of critical repair and renovation security needs.

As part of our audit, we evaluated Department actions related to the oversight of security operations at the State's correctional institutions and facilities as well as Department compliance with applicable provisions of State law. The results of our audit procedures are discussed in finding Nos. 1 through 3.

Finding No. 1: Security Review Committee

As previously noted, the Department is responsible for the security of the correctional institutions and facilities. In years past, the Department Secretary had appointed, as required by State law,[5] a Security Review Committee (Committee) to oversee Department compliance with applicable laws, rules, and guidelines related to oversight of security operations at the institutions and facilities. However, according to Department management, an organized Committee had not met since December 2008.

In response to our audit inquiries, Department management stated that the Committee was no longer active due to budgetary constraints and that the Department's Bureau of Security Operations and Regional Offices had each assumed some of the Committee's responsibilities. However, the assignment of Committee responsibilities to other areas of the Department may not provide the overall, comprehensive oversight of security operations contemplated in State law.

Recommendation: We recommend that Department management ensure that the Security Review Committee function as intended by State law or seek revision to Section 944.151, Florida Statutes.

Finding No. 2: Annual Security Audits of State Correctional Institutions and Private Correctional Facilities

Pursuant to State law,[6] the Department is to conduct or cause to be conducted security audits of all State and private correctional institutions and facilities; however, the Department of Management Services (DMS) also has a role in

[5] Section 944.151(1), Florida Statutes.
[6] Section 944.151(1)(b), Florida Statutes.

overseeing the State's private correctional facilities' operations. Specifically, the DMS Bureau of Private Prison Monitoring awards contracts to private prison companies and uses on-site monitors to help ensure that the companies operate the correctional facilities in compliance with State correctional policies and contract requirements.

As shown in Table 2, the Department's Bureau of Security Operations is to perform unannounced security audits for both the State and private correctional institutions and facilities. The Bureau of Security Operations is to schedule the audits to occur biennially with the operational reviews scheduled in the alternating years. The Regional Offices are responsible for conducting operational reviews, as well as for performing any necessary follow-up reviews for both the unannounced security audits and operational reviews.

Table 2
Operational Reviews and Unannounced Security Audits
for Private Correctional Facilities and State Correctional Institutions

Type of Monitoring	Private Correctional Facilities		State Correctional Institutions	
	Frequency	To be Performed by	Frequency	To be Performed by
Unannounced Security Audits				
Initial	Annually	Bureau of Security Operations	Biennially	Bureau of Security Operations
Follow-Up	Annually	Bureau of Security Operations	Biennially	Regional Offices
Operational Reviews				
Initial	Annually	DMS Bureau of Private Prison Monitoring	Biennially	Regional Offices
Follow-Up	Annually	DMS Bureau of Private Prison Monitoring	Biennially	Regional Offices
Security Self-Audits				
	Quarterly	Private Facility	Quarterly	State Institution

Source: Department Office of Institutions, Bureau of Security Operations.

As required by State law,[7] the Department adopted minimum security standards and policies to provide benchmarks against which compliance with State law, Department procedures and rules, and national standards (e.g., standards established by the American Academy of Corrections and the National Institute of Corrections) can be measured. The Department incorporated the adopted standards into checklists, maintained by the Department's Bureau of Research and Data Analysis in Report Writer,[8] to be used during the conduct of unannounced security audits and operational reviews.

According to Department records, unannounced security audits require the evaluation of approximately 390 security standards. As shown in Table 3, operational reviews, in contrast, are more comprehensive and, as of March 7, 2012, required the evaluation of 959 standards, including the 390 security standards and 569 standards for other areas of institutional operations.

[7] Section 944.151(1)(c), Florida Statutes.
[8] Report Writer is a stand-alone information technology application developed by the Department to maintain the standards to be evaluated during the conduct of unannounced security audits and operational reviews. The Department also uses Report Writer to generate reports for unannounced security audits and operational reviews, corrective action plans, and corrective action plan follow-ups.

Table 3
Security and Operational Standards as of March 7, 2012

Components	Number of Security Standards	Number of Operational Standards
Security	390	390
Construction and Maintenance	-	16
Personnel and Staff Development	-	19
Environmental Health, Fire, and Occupational Safety	-	110
Fiscal Management	-	140
Classification	-	71
Information Technology	-	40
Grievances, Incident Reporting, and Random Drug Testing	-	39
Programs	-	134
Totals	**390**	**959**

Source: Department Office of Institutions, Bureau of Security Operations.

According to Department management, if findings are noted during an unannounced security audit, operational review, follow-up to an unannounced security audit, or follow-up on an operational review, the findings are to be entered into Report Writer and a report of findings is to be prepared and submitted to the warden of the correctional institution and appropriate Department management for review and approval. However, if no findings are noted during an audit, review, or follow-up, then a report will not be prepared. A summary of Department procedures for unannounced security audits, operational reviews, and follow-ups to the audits and reviews is included in this report as **EXHIBIT A**.

In response to the findings noted during unannounced security audits, operational reviews, follow-up to unannounced security audits, and follow-up on operational reviews, wardens are to prepare corrective action plans (CAPs). CAPs are to be submitted to the Regional Director and the Assistant Secretary for Institutions for review and approval.

As shown in Table 2, State and private correctional institutions and facilities are also required to conduct quarterly security self-audits, each of which are to address specific standards in accordance with Department procedures.[9] As evidence of the conduct of self-audits, wardens are to submit a Certification of Compliance form to the Regional Director no later than 20 working days after the end of the quarter. Copies of the Certification of Compliance forms are to be maintained in the Regional Office files for 5 calendar years.[10]

Due to the large number and various types of correctional institutions and facilities, it is important that the Department utilize tools that promote the completeness and tracking of security oversight efforts. As part of our audit, we evaluated the tools and procedures utilized by the Department, as well as documentation of Department monitoring efforts for ten unannounced security audits and ten operational reviews. We also requested for review, Certification of Compliance forms documenting the quarterly security self-audits conducted at the State's correctional institutions and facilities, annexes, work camps, forestry camps, and work release centers. As described below, our audit procedures disclosed areas in which the Department could improve the documentation and tracking of its audits and reviews:

- A comprehensive centralized tracking mechanism would assist the Department in managing the progress and status of audits and reviews (e.g., institutions and facilities audited and reviewed, initial dates of audits and

[9] Department Procedure No. 602.040(2)(b).
[10] Department Procedure No. 602.040.

reviews, dates of follow-up audits and reviews, links to reports, staff involved, etc.), as well as in establishing priorities, deadlines, and work objectives. While the Bureau of Security Operations maintained a tracking log for unannounced security audits and each Regional Office maintained a tracking log for operational reviews and unannounced security audit follow-ups, there was no centralized tracking or oversight performed by the Department to ensure that security deficiencies were being timely corrected. Moreover, there was no formal notification process in place whereby the Bureau of Security Operations and the Regional Offices communicated recurring security deficiencies.

- Improved documentation of Department security oversight efforts would bolster transparency and accountability. Our test of audit and review documentation disclosed that the Department did not retain the documentation of its security oversight efforts (e.g., documentation evidencing review of reports and files, inventory verification, direct observations, discussions with managers, inmate and staff interviews, etc.) needed to adequately track the results of those efforts. Since reports are only to be prepared if findings are noted, the Department had no evidence showing that audits and reviews of all institutions and facilities had been conducted. Specifically:

  Unannounced Security Audits

  - The Department could not provide documentation demonstrating that, for five unannounced security audits, the wardens had timely submitted a CAP or Regional Office personnel had timely performed follow-up visits. Department procedures[11] required that deficiencies noted during an audit be corrected within 90 days of the warden receiving the approved CAP from the Bureau of Security Operations. In response to our audit inquiry, Department management indicated that, for three of the five audits, follow-up visits were conducted; however, no reports were produced. For the other two audits, the Department could not provide documentation to demonstrate that the follow-up visits had occurred.

  - Department procedures[12] provide that, for State correctional institutions, the Regional Director must follow-up within 90 days of the approved CAP to ensure that the corrective actions taken achieved and maintained the desired results. Although follow-up reports produced by the Department for five unannounced security audits indicated that repeat findings were detected, Department management indicated that repeat findings were not followed up on until the next year's audit was performed. Examples of the repeat findings disclosed in these reports included significant deficiencies related to security and locking systems, staff training, and inmate visitation.

  Operational Reviews

  - The Department could not provide documentation demonstrating that nine of the ten operational review reports had been sent to the Assistant Secretary of Institutions for his review and approval.

  - None of the ten operational review reports we reviewed had been received by the Bureau of Research and Data Analysis and, therefore, the report information had not been input into Report Writer.

  - As of August 2012, four of the ten operational review CAPs had not been signed by the Regional Director to evidence his timely review and approval. In addition, documentation was not available to demonstrate that any further action had been taken to ensure that any corrective actions taken had achieved and maintained the desired results.

  - The Department could not provide documentation demonstrating that required follow-up visits were conducted for three operational reviews. Such follow-ups were due in July 2011, August 2011, and April 2012. Pursuant to Department procedures,[13] follow-up visits were to be conducted within 180 days of the operational review to determine if corrective actions had been taken. Additionally, these operational reviews were not shown on the Regional Office tracking logs provided for our review.

[11] Department Procedure No. 602.040(5)(j)1.d.
[12] Department Procedure No. 602.040(5)(k).
[13] Department Procedure No. 602.040(4)(i)1.a.

Quarterly Security Self-Audits

- We requested documentation for quarterly security self-audits from 80 institutions (35 institutions, 12 annexes, 28 work and forestry camps, and 5 work release centers) for fiscal year 2010-11 and the first two quarters of the 2011-12 fiscal year. For the 2010-11 fiscal year and the first two quarters of the 2011-12 fiscal year, the Department was unable to provide evidence of the performance of all the quarterly security self-audits for 53 institutions. As a result, all of the standards may not have been addressed quarterly as required by Department procedures.[14]

- In addition, the Director for the Northern Region had not received 30 quarterly security self-audits due from five private correctional facilities during the period July 1, 2010, through December 31, 2011.

➢ Well-designed monitoring tools allow for quality, consistency, and completeness when evaluating compliance with standards. Although the Department utilized Report Writer to maintain the standards and prepare checklists to be used when conducting operational reviews and unannounced security audits, we noted that:

- Although required by State law,[15] the Department did not incorporate into Report Writer or the checklists standards for the random monitoring of outgoing telephone calls by inmates, maintenance of current photographs of all inmates, and employment background investigations for institution employees. In addition, the checklists used for the operational reviews and unannounced security audits did not include security standards for inmate classification as required by State law.[16]

- Report Writer was not designed to perform automated reconciliations to verify checklist completeness, as a result, the number of standards reported on did not always agree with the number of current approved standards.

- For six of ten operational reviews, Report Writer did not correctly calculate the number of standards that were in compliance. As a result, the statistical and narrative information presented in the report may have been inaccurate.

- Although the Department had prescribed forms which provided for all of the necessary information and approvals required to update the standards in Report Writer, these forms were not always utilized. Instead, revisions to operational review standards were generally submitted via e-mail and retained in an individual staff member's e-mail account. As a result, a historical record of the revisions was not maintained in a central location that provided for independent verification of the accuracy and appropriateness of the revisions.

- In some instances, pertinent information regarding the conduct of the audits or reviews was not entered and maintained in Report Writer. The Report Writer application did not require the completion of certain fields, therefore, the team members' names and titles along with the components reviewed were not always entered, making it difficult to identify who conducted the various components of the audit or review.

- The Department electronically transmitted operational review reports between staff members and did not always retain the related e-mail transmittals. As a result, the persons who prepared and approved the reports were not always readily identifiable.

Well-designed monitoring tools should include all of the information necessary to adequately track the timing and results of oversight efforts, such as the dates the monitoring was conducted, noncompliance issues cited, dates corrective actions were taken, and a description of any follow-up monitoring activities. Including this information in the tools would help ensure accountability and promote efficient, timely, accurate, and complete reporting of audit or review results.

[14] Department Procedure No. 602.040(2).
[15] Section 944.151(1)(c), Florida Statutes.
[16] Section 944.151(1)(b), Florida Statutes.

Absent sufficient security oversight procedures and adequate documentation demonstrating the conduct of timely and sufficient security audits and operational reviews, there is an increased risk that significant deficiencies may go undetected or unreported. As a result, those deficiencies may not be timely corrected. Additionally, the Department may not be able to demonstrate compliance with State law[17] requiring the annual reporting of general survey findings resulting from announced and unannounced comprehensive security audits to the Governor and the Legislature.

Recommendation: We recommend that the Department enhance its security oversight procedures by:

- **Establishing a centralized tracking mechanism to ensure that all audits, reviews, and follow-up visits are timely performed and that security deficiencies are timely corrected.**
- **Improving documentation and reporting to evidence that all audits and reviews of institutions and facilities have been conducted.**
- **Improving its monitoring tools to better document the consistent and complete evaluation of institution and facility compliance with security and operational standards.**

Finding No. 3: Work Release Centers

As previously discussed, State law[18] requires that security audits be performed of all correctional institutions at least annually. State law[19] defines correctional institutions to include any prison, road camp, prison industry, prison forestry camp, or any prison camp or prison farm or other correctional facility, temporary or permanent, in which prisoners are housed, worked, or maintained, under the custody and jurisdiction of the Department.

For 20 work release centers, we reviewed the records of security audits conducted for the 2010-11 and 2011-12 fiscal years. We noted that each of the 20 work release centers received biennial operational reviews that included the security component; however, no security audits were performed during the alternate years. As a result, during 2010-11 and 2011-12 fiscal years, 11 and 9 of the centers, respectively, did not receive a security audit by staff independent of the operation or management of the centers. Our review of Department procedures disclosed that, while biennial operational reviews were required, the procedures specifically exempted work release centers from unannounced security audits.

As work release centers were not subject to unannounced security audits and, as noted in finding No. 2, quarterly security self-audits were not always performed, the Department cannot demonstrate that the work release centers met the minimum security standards.

Recommendation: We recommend that the Department ensure that a security audit of the work release centers be performed annually in accordance with State law.

Information Technology

Access controls are intended to prevent or detect inappropriate access to information technology resources. Effective access controls include maintaining appropriate documentation of entity actions to authorize, establish, and monitor system access privileges. Examples of appropriate access control documentation include records of authorization of user access privileges requested, approved, and granted by applicable management or system owners; descriptions of

[17] Section 944.151(1)(b), Florida Statutes.
[18] Ibid.
[19] Section 944.02(8), Florida Statutes.

user roles and access privileges provided by the user roles; and documentation that correlates user roles with job functions.

Finding No. 4: Access Controls

As previously noted, Report Writer is an information technology application used by the Department to maintain the standards utilized during the conduct of unannounced security audits and operational reviews and to generate related reports. The Department installed the Report Writer application on the computers of Bureau of Research and Data Analysis staff, as well as on the computers of those staff with responsibility for initiating operational review and security audit reports at the institutions and facilities.

Because the reports of unannounced security audits and operational reviews maintained in Report Writer contain confidential information, all computers with Report Writer installed should be password protected and located in a secure location away from inmates or other unauthorized persons. Reports generated from Report Writer also contain confidential information and should be similarly protected and secured.

According to Department records, there were 2,962 users with access privileges to Report Writer as of March 31, 2012. We performed audit procedures to verify that the access privileges granted to those users were timely canceled upon a user's separation from Department employment. Also, for a limited number of users we performed audit procedures to verify that access privileges granted to those users were properly authorized and commensurate with user job responsibilities. Our audit procedures disclosed that:

- Security Access Request forms that are to be used as a means to add, modify, or remove user access to Department information technology resources, were not always available to support user access privilege authorizations. On April 5, 2012, we requested the Department to provide the Security Access Request forms for 20 Report Writer users. In response to our request, the Department provided a Security Access Request form for one user. Subsequent to our request, the Department removed the access privileges for 17 of the other 19 users.
- Report Writer user access was not always timely canceled when employees separated from Department employment. Our comparison of the listing of 2,962 Report Writer users with Department personnel records showing employee termination dates, identified 56 former employees who still had Report Writer access privileges although they had separated from Department employment. Department procedures[20] state that a request to disable a user's access to information technology resources is to be submitted within 3 business days of the employee's termination from the Department. These 56 former employees' Report Writer access privileges were still active for periods averaging 253 business days and ranging from 4 to 516 business days after the employees' termination dates. Subsequent to our audit inquiry, the Department removed the access privileges for all 56 users.

The confidential nature of the data maintained in Report Writer necessitates controls restricting access to only those users with an authorized purpose. Lack of appropriate access controls increases the risk of unauthorized access and misuse of sensitive Department data.

Recommendation: The Department should strengthen controls for the Report Writer application by ensuring that properly authorized Security Access Request forms are received prior to granting user access and that access is timely canceled after a user separates from Department employment.

[20] Department Procedure No. 206.007.

PRIOR AUDIT FOLLOW-UP

Court-Ordered Payments

As part of our audit, we performed a follow-up on the audit findings disclosed in report No. 2010-147, dated March 2010, which focused on the administration of victim restitution, cost of supervision, and other court-ordered obligations of offenders. Except as discussed below, we found that the Department had taken corrective actions for the findings included in that report.

Finding No. 5: Court-Ordered Payment System

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, including those obligations for victim restitution, fines, court costs, costs of supervision, and electronic monitoring fees. Our audit procedures to evaluate Department corrective actions taken to address the deficiencies noted in report No. 2010-147 disclosed that improvements are still needed. Specifically:

- Enhancements in Department procedures are still needed to ensure that there is sufficient and timely monitoring and follow-up on undisbursed payments. We tested 40 offender accounts to determine whether the amounts deposited by offenders were being timely disbursed to the designated beneficiaries (e.g., victims, courts, and State agencies) in accordance with governing laws. We noted that for 11 offender accounts the Department held payments totaling $100,395 beyond the normal processing time established by Department procedures, typically 5 working days. The number of days between the first undisbursed payment and February 29, 2012, ranged from 142 to 4,285 days. As of June 15, 2012, and subsequent to our audit inquiry, the Department had disbursed $32,403 of the $100,395 (32 percent).
- Although the Department had established policies and procedures to specifically describe the circumstances under which a 4 percent administrative processing fee[21] should not be collected, those procedures were not always followed. For 3 of the 25 accounts without fees that we analyzed, the Department could not demonstrate why an administrative processing fee had not been collected.
- Modifications to COPS are still needed to demonstrate that all database changes are accurate and properly authorized. Such modifications should include the production of edit reports showing all changes to payee information. These reports, if appropriately reconciled to approved change forms, would assist the Department in detecting any unauthorized changes.

Recommendation: We again recommend that the Department take the necessary steps to ensure that funds collected by the Department pursuant to court-order and State law are timely disbursed to appropriate beneficiaries and administrative processing fees are collected when appropriate. In addition, COPS should be modified to produce edit reports identifying database changes. Department staff should utilize the reports to timely reconcile identified changes to approved change forms.

[21] Section 945.31, Florida Statutes, provides that the Department may collect from persons in its custody or under its supervision, an administrative processing fee in an amount equal to 4 percent of the gross amounts of victim restitution and other court-ordered payments to help offset the cost of Department services. A court order may, however, specify that the fee is not to be collected.

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 2012 to August 2012 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 Department oversight of security operations at State and private correctional institutions and facilities. 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 disclosed in report No. 2010-147.

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 examined various records and transactions (as well as events and conditions) occurring during the period July 2010 through February 2012. Specifically, we:

- Reviewed Department policies, examined procedures, and interviewed Department staff to ascertain whether the Department had established controls relevant to the oversight of State and private correctional institutions' and facilities' security and operations. To evaluate the effectiveness of the established controls, we:
    - Tested 10 unannounced security audits from the 106 audits performed for the correctional institutions and facilities the Department is responsible for auditing. The audits tested included those conducted for 4 private facilities and 6 State-operated institutions.
    - Tested 10 operational reviews from the 133 reviews performed for the State-operated correctional institutions the Department is responsible for reviewing. We also reviewed Department actions regarding noted deficiencies.
    - Selected 85 correctional institutions and facilities (35 institutions, 12 annexes, 28 work and forestry camps, 5 work release centers, and 5 private facilities) and reviewed available documentation of security self-audits performed during the 2010-11 fiscal year and first two quarters of the 2011-12 fiscal year.
- Obtained an understanding of the general and application controls for Report Writer. Specifically, we:
    - Performed audit procedures to verify that the access privileges granted to 20 of the 2,962 Report Writer users as of March 31, 2012, were properly authorized and commensurate with user job responsibilities.
    - Compared the access privileges for the 2,962 Report Writer users to employee termination dates in Department personnel records to determine whether the Department had timely canceled Report Writer access for those users who had separated from Department employment.
    - Re-performed Report Writer calculations for 10 of 133 operational review summary reports to verify the accuracy of the calculated number of standards reviewed.
- Evaluated actions taken by the Department to correct the deficiencies disclosed in report No. 2010-147 related to the Court-Ordered Payment System (COPS). Specifically, we:
    - Reviewed the Department's 6-month response regarding the status of corrective actions for each finding disclosed in report No. 2010-147.
    - Reviewed Department procedures to determine whether they adequately addressed the sufficient and timely monitoring of undisbursed payments.
    - Evaluated whether the COPS training provided to Department staff was sufficient to mitigate future undisbursed payments and ensure the proper collection of administrative fees.
    - Determined whether the Department had enhanced its procedures to timely disburse to the designated beneficiaries in accordance with governing laws the amounts deposited by offenders, by reviewing undisbursed payments totaling $100,395 for 40 of the 35,126 offender accounts.
    - Analyzed undisbursed payments to identify offender funds that were not claimed within one year after supervision was terminated and victim restitution payments that were not claimed within one year after the offender's supervision was terminated. We also analyzed payments that were not identified and claimed one year after they were received to determine if amounts were identified and considered for deposit or transferred to the General Revenue as required by State law.

- Reviewed Department policies and procedures and tested 25 offender accounts for which administrative processing fees had not been collected to determine whether the Department had established and implemented procedures related to the collection of administrative processing fees.
- Reviewed Department policies and procedures to determine whether the Department had established and implemented procedures to detect unauthorized changes to COPS.

- Performed various other auditing procedures, including analytical procedures, as necessary, to accomplish the objectives of the audit.
- Communicated on an interim basis with applicable Department management to ensure the timely resolution of issues involving controls and noncompliance.
- Prepared and submitted for management response the findings and recommendations that are included in this report and which describe those 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 December 19, 2012, the Secretary of the Department concurred with our audit findings and recommendations. The Secretary's response is included as **EXHIBIT B**.

EXHIBIT A
SUMMARY OF DEPARTMENT PROCEDURES FOR OPERATIONAL REVIEWS AND UNANNOUNCED SECURITY AUDITS

Tasks Required by Department Procedures	Organizational Area or Position Responsible					
	Bureau of Security Operations	Regional Office	Warden	Regional Director	Assistant Secretary for Institutions	Bureau of Research and Data Analysis
Schedule initial operational reviews.	OR					
Schedule initial unannounced security audits.	USA					
Perform initial operational review.		OR				
Perform initial unannounced security audit.	USA					
Meet with warden to discuss preliminary findings.	USA	OR				
Compile a cover letter detailing any repetitive findings from previous unannounced security audit, including a request for a corrective action plan (CAP) within 30 days of receipt of the report.	USA					
Forward the completed report of findings, executive summary, and cover memo within 10 working days to the Assistant Bureau Chief of Security Operations for review.	USA					
Make any needed changes to the completed report of findings, executive summary, and cover memo and forward them to the Chief of Bureau of Security Operations.	USA					
Make any final corrections to the completed report of findings, executive summary, and cover memo and forward them to the Assistant Secretary for Institutions for signature.	USA					
Forward a copy of the approved report of findings and executive summary to the warden.	USA			OR		
Develop a CAP for each finding within 30 working days of receipt of the report.			OR USA			
Forward the CAP to the Regional Director.			OR USA			
Review and approve the CAP.				OR USA		
Forward a copy of the CAP to the Assistant Secretary of Institutions.				OR USA		
Ensure corrective action measures are completed or implemented within 90 days of the plan's approval.			OR USA			
Follow-up within 180 days on standards previously found in non-compliance to ensure corrective actions taken achieve and maintain the desired results.				OR		
If necessary, forward a follow-up review report to the Assistant Secretary of Institutions.				OR		
Review follow-up review report.					OR	
Ensure all areas of continued deficiency are reported to the Department Secretary.					OR	
Forward a follow-up review report to the Bureau of Research and Data Analysis for entry in Report Writer.					OR	
Enter operational follow-up review report in Report Writer.						OR

Legend: OR = Operational Review.
USA = Unannounced Security Audit.
Source: Department procedures.

EXHIBIT B
MANAGEMENT'S RESPONSE

FLORIDA
DEPARTMENT of
CORRECTIONS

Governor
RICK SCOTT

Secretary
MICHAEL D. CREWS

An Equal Opportunity Employer

501 South Calhoun Street, Tallahassee, FL 32399-2500

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

December 19, 2012

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 Operational Audit of the Department of Corrections, Oversight of Security 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,

Michael D. Crews
Secretary

Enclosure

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

RESPONSE TO PRELIMINARY AND TENTATIVE AUDIT FINDINGS AUDIT OF THE DEPARTMENT OF CORRECTIONS – OVERSIGHT OF SECURITY OPERATIONS AND PRIOR AUDIT FOLLOW-UP.

Oversight of Security Operations

Finding No. 1: The Security Review Committee required by Section 944.151(1), Florida Statutes, did not function as intended by State law.

Recommendation: We recommend that Department management ensure that the Security Review Committee function as intended by State law or seek revision to Section 944.151, Florida Statutes.

Agency Response: *The Bureau of Security Operations conducted Security Review Committee Meetings on a quarterly basis from July 1995 – December 2007. Due to budgetary constraints meetings were discontinued by order of the Secretary in January 2008. We have continued to insure that all of the Committee's required activities as described in 944.151 are being accomplished through other means and have incorporated the requirements into various Department Procedures to codify and mandate compliance. The Bureau of Security Operations will make a recommendation to the Office of the Secretary that we reestablish the Security Review Committee and resume meetings effective April 1, 2013 utilizing conference calling and other technology options to avoid travel costs.*

Finding No. 2: The Department did not have a centralized tracking mechanism in place to ensure that all audits, reviews, and follow-up visits were timely performed and that security deficiencies were timely corrected. Additionally, the Department did not always maintain appropriate documentation or utilize tools to promote the completeness and tracking of Department security oversight efforts.

Recommendation: We recommend that the Department enhance its security oversight procedures by:

- Establishing a centralized tracking mechanism to ensure that all audits, reviews, and follow-up visits are timely performed and that security deficiencies are timely corrected.

- Improving documentation and reporting to evidence that all audits and reviews of institutions and facilities have been conducted.

- Improving its monitoring tools to better document the consistent and complete evaluation of institution and facility compliance with security and operational standards.

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Agency Response: *The Bureau of Security Operations, in conjunction with the Office of Information Technology, began preliminary development of an improved Report Writer system on June 28, 2012. Hands-on development of the software began on July 12, 2012. The project was slated to be completed on March 31, 2013; however, we are attempting to complete the project and begin roll-out of the system by December 31, 2012. This new system will allow for a centralized tracking mechanism to ensure that all audits, reviews, and follow-up visits are performed in a timely manner and that security deficiencies are promptly corrected. Additionally, we will be able to track reviews by management staff and provide additional documentation tracking functions. These issues will be accomplished through the use of a recently dedicated position (CSAC, #13251). The staff member chosen for this newly created position begins work on January 1, 2013 and will also act as statutory compliance officer. Also, with the addition of two (2) additional security auditors (CSC, #'s 06072 & 09130), the Bureau of Security Operations will resume centralized oversight and coordination of the Operational Review process. This process was decentralized and placed in the Regional Offices under a prior administration.*

In order to address additional concerns listed in the Report relating to audit documentation, we will institute the practice of audit team members documenting and retaining for review as needed the basis for their finding determinations for all of the standards as opposed to our previous practice of documenting and reporting "by exception" only those instances where a deficiency was noted. This reporting methodology was utilized for expediency in light of the limited staffing resource available with which to accomplish all of these audit duties. This information will be scanned and stored on secure servers and the hard copies maintained by the Bureau of Security Operations.

The maintenance of current inmate photographs is a Classification issue currently addressed in Procedure 601.220.

The employment background investigation is a Personnel function under the authority of Florida Statute 110.1127, Procedure 208.049 and documented on Form DC2-897.

In accordance with the mandate of Procedure 602.013, all outgoing Inmate telephone calls are monitored/recorded. Additionally, at the discretion of each Warden and for investigative purposes by the Office of the Inspector General, additional monitoring of inmate telephones may be conducted.

Finding No. 3: The Department had not performed annual security audits of work release centers in accordance with State law.

Recommendation: We recommend that the Department ensure that a security audit of the work release centers be performed annually in accordance with State law.

Agency Response: *The Bureau of Security Operations currently conducts an unannounced security audit of state institutions every other year and private institutions*

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

every year. Using standards that include the same security standards as utilized in the unannounced audits, we augment this process with an operational review of state institutions on those years following an unannounced security audit thus insuring an annual assessment of all institutions as required. Work release centers are the lowest security level of any facility and house inmates who work in the community, unsupervised by Department staff. These facilities have no physical security systems, no perimeter fencing and minimal staffing. Additionally, the inmates housed in these facilities are predominately non-violent and non-sexual offense offenders. This information not withstanding and utilizing additional positions that have been allocated to us for audits and operational reviews, we will begin conducting security assessments of state and private work release centers utilizing an appropriate, abbreviated version of our institutional security standards effective January 1, 2013.

Information Technology

Finding No. 4: Department logical access controls related to a critical information technology application needed enhancement.

Recommendation: The Department should strengthen controls for the Report Writer application by ensuring that properly authorized Security Access Request forms are received prior to granting user access and that access is timely canceled after a user separates from Department employment.

Agency Response: *Since the audit, the Office of Information Technology (OIT) has ensured that access to standard updates is linked to membership in the appropriate LAN security groups. In addition, all users requesting access to the standard updates are required to submit a Security Access Request through their supervisor. The Research & Data Analysis security coordinator must review this request and approve it prior to OIT processing the request. The web-based replacement for Report Writer software will also include security modules that require appropriate LAN group membership for conducting reviews, editing reviews, and editing standards.*

Additionally, effective January 1, 2013, we will have a dedicated CSAC position assigned to track, authorize and delete access for staff to the new Report Writer System.

Prior Audit Follow-Up – Court-Ordered Payments

Finding No. 5: Although the Department had implemented some corrective actions related to the court-ordered payment process, deficiencies still existed.

Recommendation: We again recommend that the Department take the necessary steps to ensure that funds collected by the Department pursuant to court-order and State law are timely disbursed to appropriate beneficiaries and administrative processing fees are collected when appropriate. In addition, COPS should be modified to produce edit reports identifying database changes. Department staff should utilize the reports to timely reconcile identified changes to approved change forms.

3

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

Agency Response: *Undisbursed Funds: Over the past three (3) years, Community Corrections has worked with the Office of Information Technology to enhance Court Ordered Payment System (COPS) programming and reports in order to improve timely disbursement of funds including victim restitution, court costs, and other court ordered monetary obligations. In June 2009, a COPS Exception Summary report was established to track progress made in each circuit on reducing COPS exceptions including undisbursed funds. Each circuit utilizes this report provided weekly to review outstanding COPS exceptions requiring actions. In addition, COPS training has been provided and each region has at least one employee trained as a COPS expert to assist staff with some of the more challenging COPS account issues.*

Due to a large portion of the undisbursed funds being attributed to undeliverable/returned payments to victims, we have asked each State Attorney to provide additional victim identifying information, cell phone numbers, and email addresses that would enable our staff to more quickly and efficiently locate victims in order to forward their restitution payments. We also enhanced our victim information screen in OBIS to store additional victim information received from State Attorney's Offices.

At the beginning of the process in June 2009, total undisbursed funds were $10.2 million. As of November 30, 2012, this amount has been reduced by more than $6.6 million and is now $3.6 million. This represents an overall improvement of 64.3%.

The total breaks down into two categories – situations which will largely self-correct and situations requiring action by the Community Corrections field staff with support from COPS Accounting staff.

In June 2009, the situations which will largely self-correct totaled $3.6 million. As of November 30, 2012 this total has been reduced to $2.3 million, an improvement of 36%.

In June 2009, the situations which require Community Corrections field staff and / or COPS Accounting staff action (otherwise known as "workable" issues) totaled 6.6 million. As of November 30, 2012 this total has been reduced to $1.3 million, an improvement of 79.6%.

Approximately $1.5 million is collected in COPS each week.

As this audit revealed, there are still some delays in disbursing funds due to difficulties in locating victims or delays with responses from the court. Considering the volume of payments returned on a daily basis and competing workload demands, we believe that overall, we are working these exceptions to the best of our ability with the resources we have.

Surcharge: The three (3) cases cited for not charging surcharge were due to staff's lack of understanding COPS processes when payments are being made directly to a payee or

EXHIBIT B (CONTINUED)
MANAGEMENT'S RESPONSE

due to data entry error. Since accounts should not be entered when payments are made directly to a payee and OBIS is programmed to automatically charge surcharge when accounts are entered, this should not occur in the future if staff are following COPS processes.

Edit Reports: The COPS Operational Manual already requires supervisors to review and approve edits to accounts including address changes. Due to the current volume of supervisory workload, no changes have been made to this process to require implementation of edit reports.