

**DEPARTMENT OF MANAGEMENT  
SERVICES AND RELATED ENTITIES**

**NONPUBLIC INFORMATION SAFEGUARDS AND  
REVENUE AND CASH RECEIPTS**

---

Operational Audit

July 2006 through February 2008



## SECRETARY OF DEPARTMENT OF MANAGEMENT SERVICES

The Department is created pursuant to Section 20.22, Florida Statutes. The head of the Department is the Secretary, who is appointed by the Governor and subject to confirmation by the Senate. Secretaries who served during the audit period are shown below.

Secretary	Dates of Service
Tom Lewis, Jr.	March 8, 2005, to January 2, 2007
Linda H. South	From January 3, 2007

The audit team leader was Clint C. Boutwell, CPA, and the audit was supervised by Nancy C. Tucker, CPA. Please address inquiries regarding this report to Nancy C. Tucker, CPA, Audit Manager, by e-mail [nancytucker@aud.state.fl.us](mailto:nancytucker@aud.state.fl.us) or by telephone (850) 487-4370.

This report and other audit reports prepared by the Auditor General can be obtained on our Web site at [www.myflorida.com/audgen](http://www.myflorida.com/audgen); by telephone at (850) 487-9024; or by mail at G74 Claude Pepper Building, 111 West Madison Street, Tallahassee, Florida 32399-1450.

## DEPARTMENT OF MANAGEMENT SERVICES AND RELATED ENTITIES

### Nonpublic Information Safeguards and Revenue and Cash Receipts

#### SUMMARY

This operational audit of the Department of Management Services (Department) and related entities for the period July 2006 through February 2008, and selected actions through July 22, 2008, focused on safeguards over nonpublic information and selected revenue and cash receipt functions. Related entities included: the Division of Administrative Hearings (DOAH), the Florida Commission on Human Relations (FCHR), and the Public Employees Relations Commission (PERC). These entities, by law, are not subject to Department control, supervision, or direction but are assigned to the Department for administrative support and services, as requested.

As summarized below, our audit disclosed that internal controls over the safeguarding of nonpublic information and over revenue and cash receipt processes could be improved.

#### Nonpublic Information Safeguards

##### SSN REPORTING REQUIREMENTS

**Finding No. 1:** The Department and related entities did not timely issue each provider of social security numbers (SSNs) with a written statement stating the purpose for the SSN collection. Additionally, contrary to governing laws, certifications and reports regarding the collection and provision of SSNs were not timely provided to designated government officials.

##### COMMUNICATION OF DEPARTMENT POLICIES

**Finding No. 2:** Key management personnel were not always cognizant of the Department's established policies regarding the protection of nonpublic information. Additionally, the Department did not maintain and make available to management and staff a listing of applicable State and Federal laws and rules relevant to the nonpublic information held by the Department.

##### PROCEDURES AND STANDARD DOCUMENTS

**Finding No. 3:** Department and related entity operating procedures and standard documents could be enhanced to better safeguard nonpublic information.

##### PHYSICAL SECURITY

**Finding No. 4:** Physical security over documents containing nonpublic information was not always sufficient.

##### ACCESS CONTROLS

**Finding No. 5:** The Department, DOAH, and FCHR had not established written procedures for requesting, approving, monitoring, and removing user access privileges for selected information technology systems. Also, user access privileges were not routinely reviewed for continued applicability, and access authorizations were not retained. Additionally, certain logical access controls relating to the management of access privileges needed improvement.

##### POSITIONS OF SPECIAL TRUST

**Finding No. 6:** None of the related entities had developed written policies for designating positions that, because of special trust, responsibility, or sensitive location, require persons occupying the positions to be subject to a level 2 screening as a condition of employment; nor had the related entities so designated all such positions.

<b>Revenue and Cash Receipts</b>
----------------------------------

**CASH COLLECTION CONTROLS**

**Finding No. 7: Cash collection and processing procedures needed improvement.**

**USER ACCESS**

**Finding No. 8: Incompatible duties had been assigned to some employees at DOAH.**

**CHANGE MANAGEMENT**

**Finding No. 9: DOAH had not employed appropriate change management procedures.**

<b>BACKGROUND</b>
-------------------

The Department serves as the administrative arm of State Government. As such, the Department is responsible for:

- Consolidating the State's purchasing power for buying commodities and services and establishing rules and guidelines to ensure a fair, competitive procurement process;
- Serving as the central entity for the construction, operation, maintenance, and security of State-owned facilities;
- Providing telecommunication services to State and local governments to improve efficiency and delivery of services to Florida citizens;
- Administering the Statewide government employee retirement system and monitoring the actuarial soundness of local government retirement systems;
- Developing rules and guidelines to ensure that human resource issues including employee recruitment, promotion, and discipline are fairly and uniformly addressed and implemented; and
- Developing and administering a high-quality, competitive portfolio of employee benefits to allow the State to attract and retain a competent workforce.

As directed by statute,<sup>1</sup> the Department also provides administrative services, as requested, to designated related entities that are not subject to control, supervision, or direction by the Department. During the audit period, the head of each related entity and other relevant information were as follows:

- Division of Administrative Hearings (DOAH)
  - Head: Robert S. Cohen, Director, Chief Judge, appointed October 14, 2003.
  - Authority: Section 120.65, Florida Statutes.
  - Purpose: Adjudicate agency administrative and workers' compensation disputes.
- Florida Commission on Human Relations (FCHR)
  - Head: Derick Daniel, Executive Director, appointed July 21, 2000.
  - Authority: Section 760.04, Florida Statutes.
  - Purpose: Promote fair treatment, equal opportunity and mutual respect among members of all economic, social, racial, religious, and ethnic groups; register exemptions for communities for older persons.
- Public Employees Relations Commission (PERC)
  - Head: Donna Poole, Commission Chair, appointed July 14, 1999.
  - Authority: Section 447.205, Florida Statutes.

<sup>1</sup> Sections 20.22, 120.65, 447.205, and 760.04, Florida Statutes.

- Purpose: Conduct hearings and issue final orders related to labor and employment disputes of employees of State and local governments.

## FINDINGS AND RECOMMENDATIONS

### Nonpublic Information Safeguards

Chapter 119, Florida Statutes, provides that all State records are open for personal inspection and copying by any person and that providing access to public records is a duty of every agency. Citizens are also guaranteed the right to inspect and copy public records by Article 1, Section 24, of the State Constitution. Certain information is designated as exempt from disclosure under Chapter 119, Florida Statutes, or as confidential by Federal regulations or other State laws. Such information, referred to as nonpublic information in our report, includes but is not limited to:

- Social security numbers (SSNs) of current and former agency employees;
- Records protected under the Federal Health Insurance Portability and Accountability Act (HIPAA);
- Debit, credit, charge, or bank account numbers;
- Security system and building plans of State buildings; and
- Internal policies and procedures relating to information technology resources that, if disclosed, could facilitate the unauthorized modification, disclosure, or destruction of data or information technology resources.
- Home addresses, telephone numbers, and photographs of individuals in certain professions, such as law enforcement personnel and judges.

Safeguards over nonpublic information encompass the protection of such information, and the systems where the information resides, from a wide spectrum of threats and risks. Implementing appropriate security measures and controls to provide for the confidentiality, integrity, and safeguard of such information, regardless of its form (electronic, print, or other media) is critical to ensure protection against unauthorized access, use, disclosure, modification, or destruction.

As enumerated in the findings below, safeguards over nonpublic information held by the Department, DOAH, FCHR, and PERC were in some cases ineffective.

#### **Finding No. 1: SSN Reporting Requirements**

Pursuant to Section 119.071(5), Florida Statutes, State agencies may not collect an individual's SSN unless the agency is authorized by law to do so and has stated in writing the purpose for collecting the number. Agencies are required to provide written notification to the individual whose SSN is collected regarding the purpose for its collection. SSNs collected by an agency may not be used by that agency for any purpose other than the purpose provided in the written notification. The law further provides that SSNs held by an agency are confidential and exempt from public inspection. Each agency is required to review and certify by January 31, 2008, its compliance with the statute to the President of the Senate and Speaker of the House of Representatives.

Additionally, pursuant to Section 119.071(5), Florida Statutes, State agencies may not deny a commercial entity access to SSNs for commercial activities as long as the entity makes a written request that explains how the SSNs will be used in the performance of the commercial activities. State agencies are required to file with the Executive Office of the Governor, President of the Senate, and Speaker of the House of Representatives by January 31 of each year a report that identifies all commercial entities that have requested SSNs during the preceding calendar year and the specific

purposes stated by each entity regarding its need for SSNs. If no disclosure requests were made, the agency is to so indicate.

As part of our audit, we inquired whether the Department and the related entities had established procedures for providing written notifications for the collection of SSNs or for responding to commercial entity requests for SSNs. We also requested documentation demonstrating compliance with the reporting requirements of Section 119.071(5), Florida Statutes. As summarized in Table 1, our audit disclosed that the Department, DOAH, FCHR, and PERC collected the SSNs of their respective employees, customers, and clients in the normal course of business, but the Department and these entities did not timely provide individuals with written notifications of the purpose for collecting the SSNs or file the statutorily required certifications or reports.

**Table 1**  
**SSN Collection, Provision, and Reporting Requirements**

Criteria	Department	DOAH	FCHR	PERC
Written procedures for providing written statements for collection of SSN?	Yes, effective April 2008	Under development	None	Under development
Certified compliance with Statute by January 31, 2008?	No	No	No	No
Date certification filed.	May 2, 2008	May 7, 2008	May 8, 2008	None filed*
Written procedures for responding to requests for SSNs from commercial entities?	None	None	None	None
Filed report on commercial entities by January 31, 2008?	No	No	No	No
Date report filed.	July 22, 2008	None filed*	None filed*	None filed*

\* As of June 19, 2008.

---

**Recommendation:** To comply with State law, DOAH, FCHR, and PERC should take immediate action to file applicable certifications and reports. The Department and related entities should develop written procedures for safeguarding access to SSNs including, as applicable, provisions for providing written notifications to individuals when SSNs are collected and for obtaining written explanations from commercial entities explaining how the entities will use any SSNs provided.

---

**Finding No. 2: Communication of Department Policies**

To ensure that comprehensive safeguards over nonpublic information are in place, State agencies should adopt and communicate to staff, written overall policies that address the collection, storage, dissemination, and disposal of nonpublic information. Such policies should include, at a minimum:

- The maintenance of a comprehensive listing of those programs, activities, and functions that collect, store, disseminate, and dispose of nonpublic information including the type, format, and location of the nonpublic information and any information systems utilized to store such nonpublic information;

- A compendium of applicable laws and rules that designate information that is nonpublic and that regulate the collection, storage, dissemination, and disposal of the nonpublic information;
- A description of the logical and physical security safeguards to be maintained over nonpublic records; and
- Those positions responsible for ensuring that safeguards over nonpublic information remain in place.

In response to our inquiries regarding policies relevant to nonpublic information safeguards, the Department provided the documents listed in Table 2.

**Table 2**  
**Department Policies**  
**Related to Nonpublic Information**

Document	Contents
Public Records Manual	General guidance for responding to public records requests.
Policy No. HR 08-110	Guidelines for handling employee-related nonpublic information.
Policy No. 98-106	Guidelines for retention and disposal of hardcopy records containing nonpublic information.
Information Technology Administrative Policy No. 9.07, Data Classification	Requires agency information owners to classify data as public or confidential; employ due diligence to protect confidential information; and maintain a list of State and Federal statutes and laws relevant to confidential information.
Information Technology Administrative Policy Nos. 7.04, 9.05, 9.08 through 9.12, 9.15, and 9.16	Describes IT general controls: for example, network access, password, e-mail usage, equipment usage, mobile device usage, surplus property disposal, disaster recovery, and physical security policies.
Information Technology Administrative Policy Nos. 9.13, 9.14, 9.19, and 9.22	Describes the Department's security policies related to IT resources and data.

Source: Department staff.

Collectively, these documents appear to provide reasonable guidance necessary to ensure nonpublic information is adequately safeguarded. However, staff awareness of, and compliance with, the provisions of these various policies could be improved as described below:

- During our initial interviews of nine Division Directors, none were cognizant of any Departmentwide policies related to safeguarding nonpublic information or any listing of nonpublic information collected and used during the Department's normal course of business. Only 1 of 9 Directors initially acknowledged awareness of Administrative Policy 9.07. Additionally, only 3 of 9 Division Directors provided written policies or procedures that were relevant to nonpublic information safeguards specific to their Division and that satisfied the data classification requirements of Administrative Policy 9.07.
- Contrary to the Department's *Information Technology Administrative Policy No. 9.07*, no listing of State and Federal statutes and rules relevant to Department nonpublic information was maintained. Such a listing would enable Department staff to identify the nonpublic information they are exposed to in fulfilling their responsibilities.

Communication of and adequate training in the application of Department policies are essential to reasonably ensuring the effectiveness of such policies and procedures.

---

**Recommendation:** The Department should take steps to ensure its staff is aware of policies regarding nonpublic information safeguards. Such steps may include consolidating the individual policies, and providing ready access to and sufficient training on such policies. Additionally, the Department should identify and maintain a listing of applicable State and Federal statutes and rules relevant to nonpublic information collected or maintained by the Department.

---



---

### **Finding No. 3: Procedures and Standard Documents**

---

Comprehensive operating procedures provide a framework for employees to perform designated tasks efficiently and effectively; provide management a mechanism to control, monitor, and modify operations; and facilitate knowledge sharing among employees. To maintain maximum utility, procedures and standard documents should regularly be reviewed and updated for changes in laws, management objectives, and advances in technology. During our audit, we noted deficiencies in certain operating procedures and documents that may have impacted the safeguarding of nonpublic information, as described below:

- Within the Department, the Division of Retirement (DOR) Mail Center procedures included writing applicable SSNs on checks received from Florida Retirement System members prior to providing the checks to the Bureau of Financial Management Services for deposit. This practice increased members' exposure to the risk of identity theft. Subsequent to our inquiries, the Department amended DOR Mail Center procedures and ceased writing member SSNs on member checks received.
- Standard documents or templates created by the Department and used for drafting State Purchasing Agreements and Alternate Contract Source documents did not include clear and comprehensive security clauses prohibiting the disclosure of nonpublic information by vendors. Purchasing officials at State agencies and other governmental entities rely upon the Department to ensure that standard documents and templates contain elements that provide legal protection from known or anticipated risks.
- Contrary to Department rules,<sup>2</sup> DOAH did not have a written policy detailing the steps to be taken upon the disposal of surplus computer hard drives. Specifically, DOAH had not established written procedures for cleansing or destroying electronic media within information technology (IT) equipment that was to be disposed. Unless appropriate procedures are followed to physically destroy or cleanse electronic media, the data contained therein may be recovered using specialized software, increasing the risk that nonpublic information, should it still reside on the electronic media, will be inappropriately disclosed.
- The respective operating procedures of DOAH and FCHR included procedures for identifying and redacting specific nonpublic information from closed case files to prevent inappropriate disclosure should the files be made available pursuant to public records requests. However, DOAH and FCHR did not have procedures to address requests for employee-related nonpublic information, identification of potentially exempt home addresses, or physical security of documents containing nonpublic information.
- PERC staff stated that while they did not have written procedures addressing safeguards over nonpublic information, PERC's policy was to defer public records requests to the PERC Office of General Counsel, which would review and redact any nonpublic information contained in the requested information prior to making it available. However, absent written procedures to provide guidance to personnel on protecting nonpublic information, such nonpublic information may not be appropriately identified and safeguarded.

---

**Recommendation:** To appropriately safeguard SSNs and other nonpublic information:

- The Department should periodically review all operating procedures to ensure that nonpublic information is only collected and used to the extent necessary for the performance of Department duties and responsibilities.

---

<sup>2</sup> Department of Management Services Rule 60DD-2.009, Florida Administrative Code



- The Department should enhance its procedures to ensure that clear and unambiguous security clauses prohibiting disclosure of nonpublic information by vendors is included in all Department standard documents and templates used for procuring goods and services.
- DOAH should develop detailed written procedures for ensuring that electronic media within surplus IT equipment is completely destroyed or cleansed when the equipment is surplus.
- DOAH and FCHR should enhance existing procedures to ensure that all nonpublic information obtained during the normal course of business is identified and that appropriate safeguards are employed to protect such information.
- PERC should implement written procedures to identify all nonpublic information obtained in fulfillment of PERC responsibilities and clarify the safeguards to be employed to protect such information.

---



---

#### **Finding No. 4: Physical Security**

---

In order to accomplish its varied administrative and operational responsibilities, the Department maintains many documents that contain a diverse mix of nonpublic information that is exempt from public disclosure in accordance with law,<sup>3</sup> including but not limited to:

- State building plans;
- Procurement information in bid files that may contain exempt proprietary information;
- Minority vendor certification files that may contain SSNs and bank account numbers;
- Employee applications that may contain SSNs and exempt home addresses;
- Travel reimbursement forms that may contain SSNs and exempt home addresses;
- Purchasing card applications that may contain SSNs and other exempt personal information; and
- FLAIR reports that may contain SSNs.

With such an array of documents containing nonpublic information, it is incumbent upon the Department to implement procedures to safeguard such documents from unauthorized disclosure or alteration.

As noted in finding No. 2, during the audit period, the Department implemented various IT policies that addressed physical security over documents containing nonpublic information. Additionally, the Department included physical security of such documents in security awareness training provided to all employees. Employees were instructed to secure their workspace, lock up sensitive files and diskettes, and lock filing cabinets when unattended. However, during our inspection of areas containing documents that included nonpublic information, we noted that building plans for private prison facilities were stored in an office with no door lock. Subsequent to our inspection and inquiries, the Department installed a lock on the office door.

Our audit also disclosed additional instances of physical security deficiencies. These issues are not disclosed in this report to avoid further compromising the security of such documents. However, appropriate Department personnel have been notified.

The Department has invested in perimeter building security and visitors are required by receptionists to sign registers and be escorted within the building. However, while these measures provide some protection against misuse of nonpublic information from external parties, they do not provide protection against such misuse from unauthorized employees, contractors, or other individuals granted unrestricted access.

---

<sup>3</sup> Section 119.071, Florida Statutes.

**Recommendation:** To prevent unauthorized access to documents containing nonpublic information, the Department should enhance its procedures to ensure such information is secured behind locked doors or in locked cabinets when not in use.

**Finding No. 5: Access Controls**

The objective of security controls is to protect the integrity, confidentiality, and availability of information systems data and resources. Effective security controls include access controls that ensure users have only the access privileges needed to perform their duties, access to sensitive resources is limited to authorized users, and users are restricted from performing incompatible functions. Access controls also include the use of individual user identification codes and passwords which allow user activities to be attributed to the responsible user. Effective access controls also include a periodic review of the appropriateness of the access rights granted to employees.

To facilitate the performance of assigned responsibilities, the Department, DOAH, FCHR, and PERC maintained IT systems that, in some cases, contained nonpublic information. Our review of access controls for selected systems disclosed the following deficiencies at one or more entities:

- No written procedures for requesting, approving, assigning, monitoring, and removing user access privileges were maintained during our audit period. Written procedures provide assurance that user access privileges are consistently communicated and applied.
- No periodic reviews of user access privileges were conducted. Such reviews help ensure that privileges remain commensurate with employee job duties.
- User access authorization forms were not retained. Without such documentation, whether user accounts were appropriate and authorized cannot be readily determined.

The access control deficiencies are summarized by entity system in Table 3:

**Table 3  
Information Systems Access Controls**

Control	Department			DOAH	FCHR
	Legal Case Tracking System	Business Aircraft Record Tracking	Facilities Access Communications Tool	Case Management System	Case Management System
Written procedures for approving, monitoring, and removing access maintained?	No	No	No	No	No
User access privileges periodically reviewed?	Yes	Yes	No	No	Yes
Access authorizations retained?	Yes	No	Yes	Yes	Yes

Certain other logical access controls relating to the management of access privileges, in addition to the matters discussed above, needed improvement at the Department, DOAH, and FCHR. Specific details of these issues are not disclosed in this report to avoid the possibility of compromising information security. However, appropriate entity personnel have been notified of these issues.

Without adequate security controls, the integrity, confidentiality, and availability of data and resources may be compromised, increasing the risk that Department information and resources may be subject to improper disclosure, destruction, theft, or modification.

---

**Recommendation:** To minimize the risk of compromising data and system resources, the Department, DOAH, and FCHR should establish and implement written procedures that address requesting, approving, assigning, reviewing, and removing user access privileges for the selected systems. Further, these entities should strengthen IT logical access controls related to the management of access privileges.

---



---

#### **Finding No. 6: Positions of Special Trust**

---

State law<sup>4</sup> provides that each employing agency is required to designate those employee positions that, because of the special trust, responsibility, or sensitive location of those positions, require that persons occupying those positions be subject to a security background investigation as a condition of employment. The law<sup>5</sup> also provides that such security background investigations, designated as level 2 screenings, shall include fingerprinting to be used for Statewide criminal and juvenile records checks through the Florida Department of Law Enforcement, and Federal criminal records checks through the Federal Bureau of Investigation, and may include local criminal records checks through local law enforcement agencies.

Although specific personnel, such as administrative law judges at DOAH, had been subjected to level 2 screenings, our audit disclosed that DOAH, FCHR, and PERC had not developed policies for identifying positions of special trust and had not designated any positions as such. As enumerated in this report, DOAH, FCHR, and PERC collect, process, store, disseminate, and dispose of nonpublic information in the course of their regulatory responsibilities. Absent written policies that designate positions with access to nonpublic and sensitive information as positions of special trust, the risk is increased that appropriate background checks will not be conducted. Additionally, without level 2 screenings, the risk is increased that a person could be inappropriately employed in a position with access to nonpublic information.

---

**Recommendation:** To ensure that persons occupying positions of special trust, responsibility, or sensitive location, are subject to a level 2 screening as required by law, DOAH, FCHR, and PERC should each:

- Establish written policies clearly identifying such positions.
  - Verify that all employees occupying positions of special trust have been subjected to level 2 screenings.
- 

<b>Revenue and Cash Receipts</b>
----------------------------------

Our audit of Department revenues and cash receipts focused primarily on selected cash<sup>6</sup> receipts of the Division of State Group Insurance (DSGI), the Division of Administration, Bureau of Financial Management Services (BFMS), and the Division of Retirement (DOR). Regarding related entities, our audit primarily focused on DOAH cash receipts for invoiced services totaling approximately \$831,326 and FCHR cash receipts for 55+ housing community registrations totaling approximately \$29,260 during the audit period.

<sup>4</sup> Section 110.1127, Florida Statutes.

<sup>5</sup> Section 435.04(1), Florida Statutes.

<sup>6</sup> When used in this report, the term cash means cash and cash equivalents, such as checks and money orders.

---



---

**Finding No. 7: Cash Collection Controls**


---



---

Our review of cash collection and processing procedures disclosed various control deficiencies as discussed below. Details of these deficiencies are described by entity and issue in **APPENDIX A**.

- Written procedures did not always address key controls and processes, such as:
  - The immediate restrictive endorsement of checks at the point of collection. Such controls limit the negotiability of checks should they become lost or diverted and help deter theft.
  - The proper handling of deposits and the recording of related transactions. Such procedures serve to reasonably ensure the timely deposit of all amounts received, the accuracy and completeness of accounting records, and the safeguarding of State assets.
- Deposit reconciliations were not always performed in a manner consistent with written procedures. Reconciliations of listings of cash receipts to deposit records provide management a means to safeguard revenues, deter fraud, and timely detect errors.
- Staff sometimes performed incompatible duties related to cash receipts. For example, duties involving the collection of revenues and the maintenance of accounting records were sometimes assigned to the same employee.
- Check logs and other receipt documentation were not always accurate, secured, or adequate to establish accountability at the initial point of receipt and to provide a basis for reconciling receipts to deposits and customer accounts. The failure to adequately document cash receipts decreases management's ability to reasonably ensure that such receipts were deposited timely, an appropriate separation of duties was maintained, and recorded revenue transactions are complete. Failure to restrict check logs to authorized personnel limits the effectiveness of the controls afforded by the use of such logs and increases the risk that errors or improprieties may occur and not be detected in a timely manner.
- Electronic payments, such as journal transfers or electronic funds transfers (EFTs), were not always encouraged for large, recurring receipts. Utilizing electronic payments generally increases efficiency, reduces processing costs, and limits the risk of loss associated with paper checks.
- Checks were not always deposited timely as required by Florida law.<sup>7</sup> The failure to timely deposit moneys received into the State Treasury delays the availability of the funds for use and increases the risk of loss.

---



---

**Recommendation:** To adequately safeguard State moneys, the Department and related entities should enhance control procedures by addressing the deficiencies noted.

---



---



---



---

**Finding No. 8: User Access**


---



---

In the IT environment, access controls can be used to reasonably ensure an appropriate division of roles and responsibilities. Such controls work by limiting system access privileges to only what is needed to perform assigned duties and by avoiding the assignment of incompatible duties to staff. The failure to appropriately separate incompatible duties increases the risk that the integrity of critical production data will be compromised.

DOAH's internal accounting system (System) included hearing hours and travel expense data input by administrative law judges and other assigned staff. The System, and the data therein, was used to generate invoices for services provided to cities, counties, or independent governmental entities. According to management, original case files are destroyed after the cases are closed, rendering the System as the only permanent record of cases, hearing hours, and travel expenses.

---

<sup>7</sup> Section 116.01, Florida Statutes, requires that all funds received by a State officer be deposited into the State Treasury not later than 7 working days from the close of the week in which the officer received the funds.

Our review of access capabilities related to the System disclosed that, in addition to administrative law judges, unlimited System access privileges were provided to contracted programmers as well as accounting, IT, budget, and clerk staff. These privileges provided capabilities to update production data which, in some cases, were incompatible with assigned duties.

Subsequent to audit inquiry, management revoked the update access of certain staff. However, programmers, and the Accounting Staff Assistant who handled cash and was responsible for generating invoices and updating customer accounts for moneys received, continued to have access allowing the update of production data.

Authorizing unlimited and ongoing access to production data by programmers and allowing update capabilities to the Accounting Staff Assistant increase the risk of error and unauthorized disclosure, modification, or destruction of data.

---

**Recommendation:** DOAH should reassign the conflicting duties assigned to the Accounting Staff Assistant and periodically review user access privileges to ensure access is limited to that required by employees to perform their assigned duties. Specifically, programmers, and accounting staff responsible for generating invoices should not have access to update production data.

---



---

### **Finding No. 9: Change Management**

---

Effective change management controls include procedures to ensure that all system and program changes are properly authorized, tested, and approved for implementation and that the change process is adequately documented. To that end, the responsibility for moving approved changes into the production environment should be separated from the responsibility for developing the changes.

While management indicated that no changes were made to the System during our audit period, we noted the following control deficiencies:

- Contracted programmers were able to move modified programs into the System production environment.
- The change management log for the System only documented the date that the last executable program was created. The log did not document specific changes that overwrote the application program, and previous versions of the program executables were not retained. Additionally, documentation of testing and approval of System program changes was not retained.

It is imperative that the change management process is adequately controlled to minimize the risk that unauthorized or erroneous program changes will be made and not timely detected. Without adequate change management policies and procedures, the risk is increased that the integrity of data used to generate billings and track customer accounts will be compromised.

---

**Recommendation:** To ensure that the change management process is adequately controlled and data integrity is not compromised, DOAH should maintain change management logs and evidence of management approval of program changes. Additionally, DOAH should separate the responsibility for moving approved changes into the production environment from the responsibility for developing the changes.

---



---

## **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 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 of the Department, DOAH, FCHR, and PERC focused on safeguards over nonpublic information and internal controls over revenues and cash receipts. The overall objectives of the audit were:

- To evaluate the effectiveness of established internal controls in achieving management's control objectives in the categories of compliance with controlling laws, administrative rules, and other guidelines; the economic and effective operation of State government; the relevance and reliability of records and reports; and the safeguarding of assets.
- To evaluate management's performance in achieving compliance with controlling laws, administrative rules, and other guidelines; the economic, efficient, and effective operation of State government; the relevance and reliability of records and reports; and the safeguarding of assets.
- To identify statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

Our audit included examinations of various records and transactions (as well as events and conditions) occurring during the period July 2006 through February 2008, and selected actions through July 22, 2008.

In conducting our audit work related to safeguards over nonpublic information, we:

- Analyzed auditee staff responses to surveys related to auditee nonpublic information policies and procedures to determine whether management had implemented sufficient written procedures to ensure nonpublic information obtained was identified and protected and to assess staff's awareness of such policies and procedures.
- Examined auditee policies, procedures, and related documents to determine the adequacy of safeguards employed over nonpublic information.
- Tested compliance with written or stated physical security safeguards through unannounced observations to determine whether auditees were employing sufficient physical security measures over documents containing nonpublic information.
- Examined Department-developed standard contract documents for language that adequately addressed confidentiality and nondisclosure of nonpublic information.
- Examined auditee personnel training documents and records to determine the nature and extent of training.
- Analyzed auditee survey responses related to access controls over IT systems identified as containing nonpublic information.
- For eight internal IT systems, tested the use of unique passwords, to verify that access was restricted to authorized users.

In conducting our audit work related to revenues and cash receipts, we:

- Evaluated the effectiveness of each entity's procedures for receiving and processing cash receipts.
- Determined the effectiveness of internal controls over DSGI cash receipts, tested post-tax refund requests and examined documentation of such requests and the related warrants received from the Department of Financial Services.
- Determined the effectiveness of internal controls over Department cash receipts, tested DSGI and BFMS cash receipt transactions and examined documentation of the Department's cash receipt processing procedures.
- Determined the effectiveness of internal controls over DOR cash receipts, tested DOR cash receipt transactions related to employee purchase of retirement credits and examined documentation of the Department's cash

receipt processing procedures, including the calculation of amounts due from the employee and proper recording in the Department’s Integrated Retirement Information System.

- Determined the effectiveness of internal controls over DOAH cash receipts, tested DOAH cash receipt transactions related to amounts invoiced to governmental entities for administrative hearing services and examined documentation to support invoicing and cash receipts controls. Also, we reviewed general controls for IT systems supporting the invoicing process to determine if such controls were sufficient to provide reliable information.
- Determined the effectiveness of internal controls over FCHR cash receipts, tested FCHR cash receipt transactions related to exemption registrations for 55+ housing communities and examined registration and related fee documentation.
- Performed various other audit procedures as necessary to accomplish the objectives of the audit.

**AUTHORITY**

Section 11.45, Florida Statutes, requires that the Auditor General conduct an operational audit of each State agency on a biennial 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 response letters dated from December 11, 2008, to December 18, 2008, the Secretary of the Department of Management Services and the related entity heads concurred with our audit findings and recommendations. All responses are included in Exhibit B. [The Chair of the Public Employees Relations Commission](#) submitted several attachments with her letter. These attachments are not included in Exhibit B, but may be viewed with this report on our Web site, or obtained from the Commission.

**THIS PAGE INTENTIONALLY LEFT BLANK**



**EXHIBIT A  
CASH COLLECTION CONTROLS  
DETAILS OF DEFICIENCIES BY ENTITY**

Deficiency Noted	Department				
	BFMS	DSGI	DOR	FCHR	DOAH
Inadequate written procedures, or procedures not followed.	The accounting codes established for DSGI by BFMS did not include adequate information for recording cash received from open enrollment benefit fair participants.	Procedures and deposit forms did not provide a method for recording restitution in FLAIR. As a result, a settlement check included in our test of ten items was erroneously recorded as a reimbursement rather than as restitution.  Written procedures did not provide for checks to be restrictively endorsed when received. Generally, checks were handled by multiple staff before endorsement.	Written procedures did not require checks to be restrictively endorsed when received.	Contrary to written procedures, FCHR staff did not reconcile the cash receipts log sent to BFMS to the acknowledgements received from BFMS.	Written procedures did not require immediate endorsement of checks collected by the Office of Judges of Compensation Claims. These checks were handled by multiple staff prior to restrictive endorsement and deposit.  Contrary to written procedures, checks were sent to the Staff Assistant who updated the internal accounting system prior to the checks being sent to the Accountant I for deposit preparation.
Incompatible duties performed.		Contrary to Department policy, the employee who prepared vouchers for five of ten premium refund batches tested also received batch reports directly from a contractor courier and the corresponding warrants.			A Staff Assistant created and mailed invoices, collected money from the Clerk's office, had access to update the Clerk's check log, updated customer accounts for cash received, returned checks for billing errors, and reconciled collections of record to amounts deposited per validated deposit slips.
Check logs not accurate, restricted to assigned personnel, or adequately completed.				Multiple electronic log entries existed for one of five 55+ Housing Community registrant receipts included in our testing.	Check log entries displayed evidence of subsequent revision leaving no evidence of original entry (e.g., entries were whited out or typed over). Check logs also contained erroneous dates, such as received dates that preceded check dates.
Electronic payments not encouraged for large, recurring receipts.		During the audit period, DSGI received recurring paper checks totaling approximately \$227.6 million from DOR and approximately \$80.2 million from the University of South Florida.			
Checks not deposited timely.		Of ten receipts tested, one check for \$138,150 was deposited 10 days beyond the statutory deadline.		For two of the five 55+ Housing Community registrant receipts included in our testing, FCHR could not provide evidence of deposit of fees totaling \$40. For the other three registrants, FCHR did not timely deposit fees totaling \$60. The time that elapsed between receipt and deposit ranged from 12 to 32 days.	

**THIS PAGE INTENTIONALLY LEFT BLANK**

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE**



Governor Charlie Crist

Office of the Secretary  
4050 Esplanade Way  
Tallahassee, Florida 32399-0950  
Tel: 850.488.2786  
Fax: 850.922.6149  
[www.dms.MyFlorida.com](http://www.dms.MyFlorida.com)

Secretary Linda H. South

December 18, 2008

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

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, this is our response to your report of the *Department of Management Services and Related Entities, Nonpublic Information Safeguards and Revenue and Cash Receipts*.

Our response corresponds with the order of your tentative and preliminary findings and recommendations contained in the draft report.

If further information is needed concerning our response, please contact Steve Rumph, Inspector General, at 488-5285.

Sincerely,

Linda H. South  
Secretary

Attachment

cc: Ken Granger, Deputy Secretary  
Debra Forbess, Director of Administration  
Mathew Minno, Deputy General Counsel  
Charles Covington, Director of State Purchasing  
Michelle Robleto, Director of State Group Insurance  
Sarabeth Snuggs, Director of Retirement

We serve those who serve Florida.

**EXHIBIT B  
MANAGEMENT’S RESPONSE (CONTINUED)**

Mr. David W. Martin, CPA  
December 18, 2008  
Attachment Page 1

**Department of Management Services’ Response  
To the Auditor Generals’ Operational Audit of  
The Department of Management Services and Related Entities,  
Nonpublic Information Safeguards and Revenue and Cash Receipts**

**Nonpublic Information Safeguards**

**Finding No. 1: SSN Reporting Requirements**

The Department and related entities did not timely issue each provider of social security numbers (SSNs) with a written statement stating the purpose for the SSN collection. Additionally, contrary to governing laws, certifications and reports regarding the collection and provision of SSNs were not timely provided to designated government officials.

**Recommendation:**

The Department and related entities should develop written procedures for safeguarding access to SSNs including, as applicable, provisions for providing written notifications to individuals when SSNs are collected and for obtaining written explanations from commercial entities explaining how the entities will use any SSNs provided.

**Response:**

**Concur:** As noted in the report, effective April 2008, the department provides written notification to individuals about the purpose for collecting their SSN. In addition, the department will revise Administration Policy 94-102 - Public Records Request to require written explanations from commercial entities of how they will use any SSNs provided. The revision is expected to be completed by March 31, 2009.

**Finding No. 2: Communication of Department Policies**

Key management personnel were not always cognizant of the Department’s established policies regarding the protection of nonpublic information. Additionally, the Department did not maintain and make available to management and staff a listing of applicable State and Federal laws and rules relevant to the nonpublic information held by the Department.

**Recommendation:**

The Department should take steps to ensure its staff is aware of policies regarding nonpublic information safeguards. Such steps may include consolidating the individual policies, and providing ready access to and sufficient training on such policies. Additionally, the Department

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

Mr. David W. Martin, CPA  
December 18, 2008  
Attachment Page 2

should identify and maintain a listing of applicable State and Federal statutes and rules relevant to nonpublic information collected or maintained by the Department.

**Response:**

**Concur:** The department has posted its Administration and Human Resource Policies regarding "nonpublic" information to the department's website and intranet site. Relevant Information Technology Administrative Policies will be posted to the department's intranet site by June 30, 2009.

Information concerning the handling of "nonpublic" information will be featured in future articles of the department's newsletter, the *DMS Difference*. In addition, the Office of the General Counsel (OGC) will compile a list of the more frequently encountered laws and rules for inclusion in the OGC's Public Records Manual. However, the OGC still maintains that the *Government in the Sunshine Manual* is the best resource for comprehensive information on public records law. These actions should be completed by March 31, 2009.

**Finding No. 3: Procedures and Standard Documents**

**Department and related entity operating procedures and standard documents could be enhanced to better safeguard nonpublic information.**

**Recommendation:**

To appropriately safeguard SSNs and other nonpublic information:

- The Department should periodically review all operating procedures to ensure that nonpublic information is only collected and used to the extent necessary for the performance of Department duties and responsibilities.
- The Department should enhance its procedures to ensure that clear and unambiguous security clauses prohibiting disclosure of nonpublic information by vendors is included in all Department standard documents and templates used for procuring goods and services.

**Response:**

To appropriately safeguard SSNs and other "nonpublic" information:

- **Concur:** The department annually certifies to the Senate President and Speaker of the House of Representatives its compliance with statutory requirements regarding the collection of SSNs. In addition, the Division of Administration performs an annual review of department policies and procedures. Such review helps ensure that the department collects only that "nonpublic" information which is necessary to carry out department duties and responsibilities.

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

Mr. David W. Martin, CPA  
December 18, 2008  
Attachment Page 3

- **Concur:** State Purchasing Agreement and Alternate Contract Source vendors are required to comply with all applicable state laws, including those prohibiting disclosure of "nonpublic" information. Thus, vendor compliance with state information security requirements for State Purchasing Agreements is addressed generally in Purchasing Form 7722, which is incorporated by Rule 60A-1.025, Florida Administrative Code. These requirements are also addressed generally in the Alternate Contract Source Terms and Conditions rider (Purchasing Form 7102 incorporated by Rule 60A-1.047, Florida Administrative Code) which is executed by the department and the vendor. However, the Division of State Purchasing will strengthen the security provisions of these forms. As any substantive changes must proceed through the rulemaking process it is anticipated that the revisions will be completed by January 1, 2010.

**Finding No. 4: Physical Security**

**Physical security over documents containing nonpublic information was not always sufficient.**

**Recommendation:**

To prevent unauthorized access to documents containing nonpublic information, the Department should enhance its procedures to ensure such information is secured behind locked doors or in locked cabinets when not in use.

**Response:**

**Concur:** Department offices are located in secure facilities. In addition, the department's Administration Policy 94-102 - Public Records Request and Human Resource Policy 06-110 - Misuse of Information and Data both require that each program area establish procedures for keeping exempt records from disclosure. Human Resource Policy 06-110 further requires that employees comply with established protection and control procedures and protect information and data being used. As a condition of employment, staff are required to sign an acknowledgement form that they are aware of, and agree to the requirements of the policy. The department will feature reminders about the safeguarding of "nonpublic" information in future issues of the *DMS Difference* and in email communications to all employees. The department will also enhance existing policies to include a requirement that employees secure "nonpublic" documents behind locked doors or in locked cabinets after work hours or when not in use for extended periods of time during the work day.

**Finding No. 5: Access Controls**

**The Department and related entities had not established written procedures for requesting, approving, monitoring, and removing user access privileges for selected information technology systems. Also, user access privileges were not routinely reviewed for continued applicability, and access authorizations were not retained.**

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

Mr. David W. Martin, CPA  
December 18, 2008  
Attachment Page 4

**Additionally, certain logical access controls relating to the management of access privileges needed improvement.**

**Recommendation:**

To minimize the risk of compromising data and system resources, the Department, DOAH, FCHR, and PERC should establish and implement written procedures that address requesting, approving, assigning, reviewing, and removing user access privileges for the selected systems. Further, the Department, DOAH, and FCHR should strengthen IT logical access controls related to the management of access privileges.

**Response:**

**Concur:** The department recognizes that a more formal process for requesting user access is consistent with good security practices. Therefore, the department will implement an automated process to request and remove user access to systems under the direct control of the department's divisions. This process will log all user access requests (access and removal) authorized by the division's system owner. In addition, the department will establish a schedule for reviewing user access rights. These new procedures are scheduled for implementation by June 30, 2009.

**Revenue and Cash Receipts**

**Finding No. 7: Cash Collection Controls**

**Cash collection and processing procedures needed improvement.**

**Recommendations:**

To adequately safeguard State moneys, the Department and related entities should enhance control procedures by addressing the deficiencies noted.

**Bureau of Financial Management Services (BFMS)**

- The accounting codes established for DSGI did not include adequate information for recording cash received from open enrollment benefit fair participants.

**Division of State Group Insurance (DSGI)**

- Procedures and deposit forms did not provide a method for recording restitution in FLAIR. As a result, a settlement check included in our test of ten items was erroneously recorded as a reimbursement rather than as restitution.

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

Mr. David W. Martin, CPA  
December 18, 2008  
Attachment Page 5

- Written procedures did not provide for checks to be restrictively endorsed when received. Generally, checks were handled by multiple staff before endorsement.
- Contrary to Department policy, the employee who prepared vouchers for five of ten premium refund batches tested also received batch reports directly from contractor courier and the corresponding warrants.
- During the audit period, DSGI received recurring paper checks totaling approximately \$227.6 million from DOR and approximately \$80.2 million from the University of South Florida.
- Of ten receipts tested, one check for \$138,150 was deposited 10 days beyond the statutory deadline.

**Division of Retirement (DOR)**

- Written procedures did not require checks to be restrictively endorsed when received.

**Responses:**

**Bureau of Financial Management Services**

- **Concur:** During the course of the Auditor General's review, the Bureau of Financial Management Services established a separate object code specifically for recording reimbursements from open enrollment benefit fair participants.

**Division of State Group Insurance**

- **Concur:** During 2007, the division's accounting section developed Standard Office Procedures (SOP). SOP 500-34 was updated June 2008 and includes specific procedures for the handling of settlement checks. The checks are kept in the DSGI safe until they are approved for deposit by the OGC. The Chief of BFMS then provides DSGI with written instructions on the appropriate account in which to deposit the funds. Each settlement check is processed individually.
- **Concur:** The division will establish a new SOP requiring the employee that initially receives mail from the Post Office and the Courier to immediately restrictively endorse checks intended for DSGI. Checks delivered to DSGI in error will not be restrictively endorsed. However, all checks received by DSGI will be logged and reconciled on a monthly basis. Anticipated completion of the new SOP is December 31, 2008.
- **Concur:** Warrants are received by DSGI from BFMS, not directly from a contract courier as stated. However, SOP 500-40 addresses separation of duties for activities



**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

Mr. David W. Martin, CPA  
December 18, 2008  
Attachment Page 6

performed by the Accounting Section staff. Management routinely meets with staff to ensure that procedures are followed as written. In addition, management will randomly monitor operations to ensure that procedures are followed.

- **Concur:** BFMS has been coordinating with the Division of Retirement to implement a monthly payment by journal transfer rather than issuing state warrants. In addition, DSGI has provided information to the University of South Florida (USF) on several occasions about the electronic payment option and has held phone conversations with the Payroll Director to encourage its use. USF has decided at this time to not use the electronic payment option. However, the division will continue to encourage both the Division of Retirement and USF to use the journal transfer or electronic payment options.
- **Concur:** The division will revise SOP 500-34 to establish a timeframe for the deposit of all checks, including those checks that require further review before deposit. Anticipated completion of this revision is December 31, 2008.

**Division of Retirement**

- **Concur:** The Division of Retirement has revised its written procedures to require restrictive endorsement upon receipt of checks in the division's mail center.

**EXHIBIT B**  
**MANAGEMENT’S RESPONSE (CONTINUED)**

**State of Florida**  
**Division of Administrative Hearings**

**Charles J. Crist, Jr.**  
Governor



**Harry L. Hooper**  
Deputy Chief  
Administrative Law Judge

**Robert S. Cohen**  
Director and Chief Judge

**David W. Langham**  
Deputy Chief Judge  
Judges of Compensation Claims

**Claudia Lladó**  
Clerk of the Division

December 11, 2008

David Martin  
Auditor General  
Room G74, Claude Pepper Building  
111 West Madison Street  
Tallahassee, Florida 32302

Dear Mr. Martin:

In connection with your Operational Compliance Audit of the Florida Department of Management Services and Related Entities, on Nonpublic Information Safeguards and Revenue and Cash receipts, for the period July 2006 through February 2008, the following is information concerning the findings referenced and the actual or proposed corrective actions taken respectively.

**Finding No. 1: SSN Reporting Requirements**

The Division of Administrative Hearings (DOAH) instituted a policy on July 9, 2008, to comply with Subsection 119.071(5), Florida Statutes, with regard to informing employees of the need to collect social security numbers. Additionally, DOAH filed certification to the appropriate entities on May 7, 2008, and will comply henceforth annually.

**Finding No. 3: Procedures and Standard Documents**

DOAH has developed written procedures for ensuring that electronic media within surplus IT equipment is completely destroyed or cleansed when the equipment is surplus.

DOAH has enhanced existing procedures to ensure that all nonpublic information obtained during the normal course of business is identified and that appropriate safeguards are employed to protect such information. Specifically, enhancing procedures in the Clerk’s Office Manual and the Administrative Policies and Procedures Manual identifying nonpublic information and physical security safeguards.

The DeSoto Building, 1230 Apalachee Parkway, Tallahassee, Florida 32399-3060  
Administrative Law (850) 488-9675 • SUNCOM 278-9675 • Fax Filing (850) 921-8453 •  
Fax SUNCOM 291-8453 \*Judges of Compensation Claims (850) 487-1911  
[www.doah.state.fl.us](http://www.doah.state.fl.us)

**EXHIBIT B  
MANAGEMENT'S RESPONSE (CONTINUED)**

David Martin  
December 11, 2008  
Page 2

Finding No. 5: Access Controls

DOAH has drafted written procedures for requesting, assigning, and removing user access privileges. Procedures for periodically reviewing user access privileges are being reviewed.

Finding No. 6: Position of Special Trust

Upon review, DOAH identified all career service, selected exempt, senior management, appointed, and other personal services positions in fact, positions of special trust. DOAH has established written policies and procedures identifying such positions and is currently implementing level 2 screenings on all employees.

Finding No. 7: Cash Collection Controls

DOAH has readdressed and enhanced control procedures as recommended to safeguard cash collections.

Finding No. 8: User Access

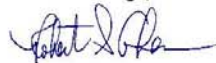
The conflicting duties identified in the audit findings have been re-assigned and procedures for approving updates to production data have been instituted.

Finding No. 9: Change Management

DOAH is reviewing these recommendations and will institute procedures to address the issues raised.

DOAH believes the actions taken are responsive to the findings noted. If you have any questions, please feel free to call.

Sincerely,



Robert S. Cohen  
Director and Chief Judge

RSC/

EXHIBIT B  
MANAGEMENT'S RESPONSE (CONTINUED)



Charlie Crist  
Governor

State of Florida  
Florida Commission on Human Relations  
An Equal Opportunity Employer • Affirmative Action Employer

2009 Apalachee Parkway • Suite 200 • Tallahassee, Florida 32301-4857  
(850) 488-7082  
Web Site <http://fchr.state.fl.us>



Dr. Donna Elam  
Chair

Derick Daniel  
Executive Director

December 17, 2008

Mr. David W. Martin, CPA  
Office of the Auditor General  
The Florida Legislature  
G74 Claude Pepper Building  
111 West Madison Street  
Tallahassee, FL 32399-1470

Dear Mr. Martin:

The Florida Commission on Human Relations has reviewed the Auditor General's report on the tentative findings and recommendations relating to Nonpublic Information Safeguards and Revenue and Cash Receipts for the period July 2006 through February 2008.

We would like to thank you and your staff for their professionalism while working with us to gather information for this report. They made every effort to ensure that the information they gathered was in-depth and comprehensive, and were very responsive to our questions and attentive to our concerns.

On the following pages is our response to this report. We would appreciate you including this response in the final published audit report.

If you have any questions or need further information, please call me at 488-7082.

Sincerely,  
  
Derick Daniel  
Executive Director

DD/

COMMISSIONERS

Gilbert M. Singer, Vice Chair  
Tampa

Gayle Cannon  
Lake City

Onelia A. Fajardo  
Miami

Elena Flom  
Cocoa Beach

Watson Haynes  
St. Petersburg

Anice R. Prosser  
Tallahassee

Billy Whitefox Stall  
Panama City

Patty Ball Thomas  
Tallahassee

Mario Valle  
Naples

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

**Finding #1: SSN REPORTING REQUIREMENTS**

*The Department and related entities did not timely issue each provider of social security numbers (SSNs) with a written statement stating the purpose for the SSN collection. Additionally, contrary to governing laws, certifications and reports regarding the collection and provision of SSNs were not timely provided to designated government officials.*

**Recommendation:** To comply with State law, DOAH, FCHR, and PERC should take immediate action to file applicable certifications and reports. The Department and related entities should develop written procedures for safeguarding access to SSNs including, as applicable, provisions for providing written notifications to individuals when SSNs are collected and for obtaining written explanations from commercial entities explaining how the entities will use any SSNs provided.

**FCHR RESPONSE:**

We concur. On May 16, 2008, we submitted a certificate of compliance with Section 119.071(5)(a)4.a. to President Ken Pruitt and Speaker Marco Rubio. On December 11, 2008, we submitted the certification report for calendar year 2007 to Governor Charlie Crist, President Jeff Atwater, and Speaker Ray Sansom. We will file both required reports for calendar year 2008 on or before the January 31, 2009 deadline.

In addition, the Commission has drafted a policy to address the protection of access to SSNs, as described in the recommendation. Commission employees also receive written notification about the collection and use of their SSNs during new employee orientation at the Department of Management Services.

We have drafted several policies to address audit findings and recommendations noted in the tentative audit report. We recognize that it is vital that our employees fully understand and comply with these policies. Therefore, by April 1, 2009, we will train all staff on the new requirements. We will include these enhanced procedures in our New Employee Orientation. Finally, we will make updates to specific Standard Operating Procedures, as needed.

**Finding #3: PROCEDURES AND STANDARD DOCUMENTS**

*Department and related entity operating procedures and standard documents could be enhanced to better safeguard nonpublic information.*

**Recommendation:** To appropriately safeguard SSNs and other nonpublic information, DOAH and FCHR should enhance existing procedures to ensure that all nonpublic information obtained during the normal course of business is identified and that appropriate safeguards are employed to protect such information.

**FCHR RESPONSE:**

We concur. Prior to the audit, the Commission used a Standard Operating Procedure for Copy Requests, which directed the records clerk to verify that all SSNs were redacted and that information in the Confidential tab was not released. Effective October 9, 2003, we also implemented a Confidential Documents policy, which provided instruction for the proper handling of SSNs and confidential medical information.

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

The Commission has since drafted several policies and forms to more specifically address the identification of all nonpublic information we receive, as well as authorized methods to handle and protect this information. The policies cover the following areas:

- How we will ensure that all SSNs remain confidential and exempt from Florida public records laws;
- How we will require commercial entities to make a written and signed request for SSNs that describes the purpose for the request;
- The requirement to file compliance reports with the appropriate legislative officials by January 31 of each calendar year;
- How we will ensure that confidential information contained in any Commission file is not released to any individual or entity, except as provided by state or federal law;
- Guidelines for ensuring the physical security of documents which contain nonpublic information;
- The collection, use, and protection of confidential health information obtained during the course of an investigation where discrimination on the basis of disability is alleged; and
- How we will secure authorization from the Complainant to share their health information with the opposing party and the Equal Employment Opportunity Commission, the Division of Administrative Hearings, the U.S. Department of Housing and Urban Development, or a court of law upon request.

**Finding #5: ACCESS CONTROLS**

*The Department and related entities had not established written procedures for requesting, approving, monitoring, and removing user access privileges for selected information technology systems. Also, user access privileges were not routinely reviewed for continued applicability, and access authorizations were not retained. Additionally, certain logical access controls relating to the management of access privileges needed improvement.*

**Recommendation:** To minimize the risk of compromising data and system resources, the Department, DOAH, FCHR, and PERC should establish and implement written procedures that address requesting, approving, assigning, reviewing, and removing user access privileges for the selected systems. Further, the Department, DOAH, and FCHR should strengthen IT logical access controls related to the management of access privileges.

**FCHR RESPONSE:**

We concur. We have developed procedures that describe the process for requesting, approving, assigning, reviewing, and removing user access privileges for our Case Management System. In addition, we have enhanced certain security features of our Case Management System to further protect nonpublic information contained therein.

**Finding #6: POSITIONS OF SPECIAL TRUST**

*None of the related entities had developed written policies for designating positions that, because of special trust, responsibility, or sensitive location, require persons occupying the positions to be subject to a level 2 screening as a condition of employment; nor had the related entities so designated all such positions.*

**Recommendation:** To ensure that persons occupying positions of special trust, responsibility, or sensitive location, are subject to a level 2 screening as required by law, DOAH, FCHR, and PERC should each:

- Establish written policies clearly identifying such positions.
- Verify that all employees occupying positions of special trust have been subjected to level 2 screenings.

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

**FCHR RESPONSE:**

We concur. We drafted a procedure to address the designation of positions of special trust. We will ensure that all current employees in positions of special trust undergo a level 2 screening by April 1, 2009, and that all future employees are screened in accordance with the policy.

**Finding #7: CASH COLLECTION CONTROLS**

*Cash collection and processing procedures needed improvement.*

**Recommendation:** To adequately safeguard State moneys, the Department and related entities should enhance control procedures by addressing the deficiencies noted.

**FCHR RESPONSE:**

We concur. We currently abide by a policy which establishes the process for handling all incoming revenue, including the responsibility of the mail clerk to restrictively endorse all checks and money orders immediately upon receipt, with the exception of checks and money orders that are sent to the Commission in error. The Commission is in the process of amending the policy to include specific performance and quality control measures that will address the proper handling of deposits and all revenue received, as well as the recording of related transactions.

The Commission is also in compliance with the following:

- As of July 2008, the Budget Director performs deposit reconciliations by the 15<sup>th</sup> of each month and maintains documentation to verify her compliance. Currently, this is a manual process, but we plan to automate reports that will verify timely reconciliation.
- Check logs are secure and accurate to establish accountability at the initial point of receipt and are adequate for reconciliation purposes.
  - Security:
    - The FCHR Revenue database (or check log) must be installed by a member of the MIS Unit on each employee's computer, after approval by their supervisor.
    - This database is only installed on employees who are authorized to view, enter and/or modify data by virtue of their job function.
    - Additionally, the user's account has to be activated by a member of the MIS Unit.
    - The database is password protected through the user's Windows domain account, and the level of access to view, edit and/or modify data is granted and removed based upon the function of the employee.
    - There are 2 access levels:
      - Administrator
        - Granted to members of MIS Unit
        - Complete access to the system: design, installation, maintenance, technical support, view, edit and modify data
      - User
        - Granted to mail clerk, 2 back up mail clerks, staff assistant (back up deposits), budget director and budget assistant.
        - View, edit and modify data
    - Added privileges for budget director and budget assistant
      - Reports
      - Deposits
      - Deposit Reconciliation

---

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

- Accuracy and Adequacy:
  - On November 14, 2008, a report was created to track the accuracy rate of entries into the Revenue database.
- Between June and November 2008, we have deposited greater than 90% of checks within five working days of receipt. We are working diligently to enhance our reporting capabilities, which will enable us to quickly determine where backlogs occur and to address them immediately.
- Effective August 2008, we began to maintain scanned copies of 55+ related documents. This will allow us to quickly refer to documents as needed, or to provide them upon request.



**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**



STATE OF FLORIDA  
PUBLIC EMPLOYEES RELATIONS COMMISSION

Stephanie Williams Ray  
CHAIR

Charles H. Kossuth, Jr.  
Jessica Enciso Varn  
COMMISSIONERS

December 17, 2008

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

RE: Operational Audit of the Department of Management Services and Related Entities on Nonpublic Information Safeguards and Revenue and Cash Receipts for the period July 2006 through February 2008

Dear Mr. Martin:

We have reviewed the preliminary and tentative audit findings and recommendations from the above-referenced audit included with your letter dated November 18, 2008. The following response reflects the specific actions taken or contemplated to address the deficiencies cited for the Public Employees Relations Commission (PERC):

**Finding No. 1: SSN Reporting Requirements**

**Auditor General Recommendation:** To comply with State law, ...PERC should take immediate action to file applicable certifications and reports. The Department and related entities should develop written procedures for safeguarding access to SSNs including, as applicable, provisions for providing written notifications to individuals when SSNs are collected and for obtaining written explanations from commercial entities explaining how the entities will use any SSNs provided.

**Agency Response:** PERC has taken the following corrective actions to address the foregoing recommendation:

- PERC collects social security numbers from individual vendors (e.g., court reporters), as required by the State of Florida Office of Chief Financial Officer, for payment for services rendered. Prior to this audit recommendation, PERC had

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

Mr. David W. Martin, CPA  
Page 2

not provided written notice to these vendors regarding the purpose for its collection. As a corrective measure, PERC sent such notification to all of its current vendors by letter dated December 15, 2008. (See Attachment 1) In the future, such notification will be included in the standard purchase order created for vendors at the beginning of each fiscal year.

- It is noteworthy that the Department of Management Services (DMS) maintains the official personnel files for PERC employees. It provides employees with a written statement for collection of social security numbers in accordance with section 119.071(5)(a)(2)(a), Florida Statutes. (See Attachment 2)
- PERC has reviewed its collection of social security numbers to determine compliance with the law and certified such compliance to the President of the Senate and the Speaker of the House of Representatives by letter dated December 16, 2008. (See Attachment 3)
- PERC has implemented written procedures effective December 16, 2008, for responding to requests for information pursuant to Chapter 119, Florida Statutes, including requests for social security numbers from commercial entities. (See Attachment 4)
- By letter dated December 12, 2008, PERC reported to the Executive Office of the Governor, the President of the Senate, and the Speaker of the House of Representatives, that no commercial entities had requested social security numbers from the agency during the preceding calendar year. (See Attachment 5)

**Finding No. 3: Procedures and Standard Documents**

**Auditor General Recommendation:** To appropriately safeguard SSNs and other nonpublic information: ... PERC should implement written procedures to identify all nonpublic information obtained in fulfillment of PERC responsibilities and clarify the safeguards to be employed to protect such information.

**Agency Response:** Access to information in the custody and control of PERC, which is exempt from public disclosure (confidential information) or may be exempt (privileged information), can only be obtained by a public records request pursuant to Section 119.07, Florida Statutes. In response to this audit recommendation, PERC memorialized in writing its existing practice for responding to public records requests. (See Attachment 4) In addition, PERC has also added a bold notice in its acknowledgement letter to the parties initiating each case which outlines what is confidential and privileged information and how this information will be processed by PERC. (See Attachment 6)

**EXHIBIT B**  
**MANAGEMENT'S RESPONSE (CONTINUED)**

Mr. David W. Martin, CPA  
Page 3

**Finding No. 6: Positions of Special Trust**

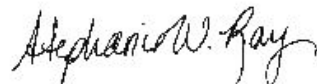
**Auditor General Recommendation:** To ensure that persons occupying positions of special trust, responsibility, or sensitive location, are subject to a level 2 screening as required by law, PERC should:

- Establish written policies clearly identifying such positions.
- Verify that all employees occupying positions of special trust have been subjected to level 2 screenings.

**Agency Response:** In response to this recommendation, PERC has designated all of its positions as those occupying special trust or responsibility due to the quasi-judicial mission of PERC and the employees' access to its Case Management System. PERC has established and implemented a policy for security background investigations and provided it to all PERC employees. (See Attachment 7) All PERC employees have been submitted to level 2 background investigations coordinated by the Department of Management Services, Office of the Inspector General.

On behalf of PERC, I look forward to receiving your final audit findings and recommendations and will implement additional corrective action, as appropriate.

Sincerely,



Stephanie Williams Ray  
Chair

Attachments (7)

