DEPARTMENT OF MANAGEMENT Services

Office of Inspector General
Department of Management Services
4040 Esplanade Way, Suite 135
Tallahassee, Florida 32399-0001
Tel: 850.488.5285
Fax: 850.921.3066
www.dms.MyFlorida.com

Governor Charlie Crist

Secretary Linda H. South

MEMORANDUM

DATE: June 23, 2009

TO: Linda H. South, Secretary

FROM: Steve Rumph, Inspector General

SUBJECT: **Six-Month Status Report to Auditor General Report No. 2009-078**

The following is our explanation of the six-month status of findings and recommendations included in the Auditor General's Report No. 2009-078, ***Department of Management Services Nonpublic Information Safeguards and Revenue and Cash Receipts***. Our response addresses the findings and recommendations in the same order as they appear in the report.

Six-Month Status Report

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 1: 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.

Original Response to Recommendation 1: 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.

JLAC
Rec'd 7/2/2009

Current Status of Recommendation 1: The department completed the revision of Administration Policy 94-102 – Public Records Request on June 11, 2009 to include provisions for providing written notifications to individuals when SSNs are collected and for providing SSNs to commercial entities.

OIG Position: ***We agree with the actions taken by the department and recommend this finding be closed.***

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 2: 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.

Original Response to Recommendation 2: 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.

Current Status of Recommendation 2: The department featured articles in the December 2008 newsletter concerning the handling of "nonpublic information. The OGC compiled a list of the more frequently encountered laws and rules and included them in the OGC's Public Records Manual completed March 31, 2009.

It is anticipated that the Information Technology Administrative Policies will be completed and posted on the intranet site by June 30, 2009.

OIG Position: ***We will continue to monitor this recommendation until the Information Technology Administrative Polices have been completed and posted on the intranet site.***

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 3: 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.

Original Response Recommendation 3: To appropriately safeguard SSNs and other "nonpublic" information:

- 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.

- 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.

Current Status of Recommendation 3:

- The department provided the certification of the collection of SSNs to the Senate President and Speaker of the House of Representatives on January 29, 2009.

- The Division of State Purchasing is in the process of strengthening the security provision of the Purchasing Form 7722 and Purchasing Form 7102. These changes will be completed by January 1, 2010.

OIG Position: ***We will continue to monitor this recommendation until the forms are updated and Rule 60A-1.025, Florida Administrative Code has been changed.***

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

Recommendation 4: 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.

Original Response to Recommendation 4: 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.

Current Status of Recommendation 4: The department has updated and published Administration Policy 94-102 – Public Records Request. The department has also included a reminder in the December 2008 issue of the *DMS Difference* and an email regarding training on the policies. Each program area is currently working to complete procedures for their area.

OIG Position: ***We will continue to monitor this recommendation until each program area has a procedure for the safeguarding of confidential information.***

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

Recommendation 5: 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.

Original Response to Recommendation 5: 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.

Current Status of Recommendation 5: The department is in the process of creating and implementing new automated procedures. These procedures will be completed by August 31, 2009.

***OIG Position:* We will continue to monitor this recommendation until the user access procedures are completed.**

Revenue and Cash Receipts

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

Recommendation 7: 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.

- 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.

Original Response to Recommendation 7:

Bureau of Financial Management Services

- 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

- 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.

- 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.

- 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 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.

- 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.

- 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

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

Current Status of Recommendation 7:

Bureau of Financial Management Services

- On December 18, 2008, 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

- The division is in the process of updating the procedure SOP 500-51 to incorporate all management and control of cash receipts. These procedures will be completed by August 30, 2009.

- In February 2009, the division updated SOP 500-51 to specify endorsements of checks received for DSGI. The procedures also explain what to do with checks incorrectly delivered to DSGI. All checks are logged and reconciled at the end of the month.

- SOP 500-40 – Disbursement – Post Tax Premium Refund and SOP-41 University and Non-Warrant Agency Premium Refunds are in draft to include the separation of duties regarding preparing vouchers, reviewing batches, and receiving checks.

- DSGI has contacted the University of South Florida and is continuing to work with the University to process the premiums through an eservices account. The Division of Retirement has successfully received wire transfers from the University of South Florida for February, March, and April for the retirement contributions.

- In February 2009, the division updated Standard Office Procedure (SOP) 500-51 to include the timeframe for the deposit of all checks.

Division of Retirement

- The Division of Retirement revised its policies and procedures on April 20, 2009 to require restrictive endorsement upon receipt of checks in the division's mail center.

OIG Position: ***We will continue to monitor this recommendation until DSGI procedures regarding settlement checks and premium refunds are completed.***

If further information is needed, please contact John Davis, Auditor Director, or myself at 488-5285.

JSR/crm

cc: Kathy Dubose, Director of Joint Legislative Auditing Committee
David W. Martin, Auditor General
Ken Granger, Chief of Staff
David Faulkenberry, Deputy Secretary
Sarabeth Snuggs, Director, Division of Retirement
Debra Forbess, Director of Administration
Charles Covington, Director of State Purchasing
Michelle Robleto, Director of Division of State Group Insurance
John Brenneis, General Counsel
Joe Wright, Chief Information Office