REPRESENTING
ALEX SINK
CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

January 12, 2010

The Honorable Alex Sink
Chief Financial Officer
The Capitol, PL-11
Tallahassee, Florida 32399-0301

Dear CFO Sink:

Pursuant to Section 20.055 (5)(h), Florida Statutes, the enclosed response provides a six-month follow-up on the status of corrective actions taken by the Department regarding the findings and recommendations included in the Auditor General's Report No. 2010-005, Information Technology Audit of the Department of Financial Services and Selected Participating State Agencies Payment Card Programs, for the Period October 2008 through January 2009 and selected actions through March 2, 2009.

If you have any questions or would like to discuss the matter further, please contact me at (850) 413-4960.

Sincerely,

Robert E. Clift

REC:sc

Enclosure

cc: Jon Ingram, CPA, CISA, Audit Manager, Office of the Auditor General
✓Kathy DuBose, Staff Director, Joint Legislative Auditing Committee

RECEIVED
JAN 12 2010

FLORIDA DEPARTMENT OF FINANCIAL SERVICES
Robert E. Clift • Inspector General
200 E. Gaines St. • Tallahassee, FL 32399-0312 • Tel. 850-413-3112 • Fax 850-413-4973
Email • Bob.Clift@myfloridacfo.com

Florida Department of Financial Services and Selected Participating State Agencies
Six-Month Audit Response
Payment Card Programs
Information Technology Audit
For the Period October 2008 through January 2009 and Selected Actions through March 2, 2009

Finding No. 1: DFS and AEIT Guidance for Agency Payment Card Programs

Section 215.322(2), Florida Statutes, provides that a State agency may accept payment cards for goods and services with the prior approval of the CFO. If the Internet or other related electronic methods are to be used as the collection medium, AEIT shall review and recommend to the CFO whether to approve the request with regard to the process or procedure to be used. Pursuant to Section 282.318(2)(a), Florida Statutes, AEIT, in consultation with each agency head, is responsible for assessing and recommending minimum operating procedures for ensuring an adequate level of security for all data and IT resources for executive branch agencies.

Our audit disclosed that, although written rules and guidelines existed for maintaining an adequate level of security for data and IT resources in general, no written DFS or AEIT guidance existed that specifically addressed protecting cardholder data or complying with the PCI Data Security Standard. In addition, neither DFS nor AEIT had established written policies or procedures addressing the AEIT review of applicable State agency processes or procedures associated with payment card program requests. No agency payment card program approval requests that planned to use the Internet or other related electronic methods as the collection medium had been submitted to DFS or AEIT during the audit period. However, the process for guiding the agencies in the technical aspects of agency payment card acceptance, including the division of responsibilities between DFS and AEIT, was not clearly described in State law, rule, or other policies and procedures. The need for clearer agency guidance is demonstrated in subsequent findings in this report that describe improvements needed in various agency measures to comply with the PCI Data Security Standard or to assess their progress toward compliance.

In response to audit inquiry, management of both DFS and AEIT stated that, instead of reviewing individual agency payment card program requests, the appropriate level of AEIT involvement would be to review the DFS process for evaluating the technical aspects of agency requests, make recommendations to DFS as applicable, and provide other technical advice to DFS as required. However, as stated above, current law provides for AEIT review of agency requests involving the use of the Internet or other related electronic methods as the collection medium.

Recommendation: DFS and AEIT are well positioned to review and guide agency efforts to implement appropriate safeguards over cardholder data in their payment card programs. DFS and AEIT should work together to establish and document a process for guiding State agencies in establishing an adequate level of security over cardholder data within agency payment card programs. As a part of this effort, DFS and AEIT should establish written guidance for the

Florida Department of Financial Services and Selected Participating State Agencies
Six-Month Audit Response
Payment Card Programs
Information Technology Audit
For the Period October 2008 through January 2009 and Selected Actions through March 2, 2009

Finding No. 1: DFS and AEIT Guidance for Agency Payment Card Programs

Section 215.322(2), Florida Statutes, provides that a State agency may accept payment cards for goods and services with the prior approval of the CFO. If the Internet or other related electronic methods are to be used as the collection medium, AEIT shall review and recommend to the CFO whether to approve the request with regard to the process or procedure to be used. Pursuant to Section 282.318(2)(a), Florida Statutes, AEIT, in consultation with each agency head, is responsible for assessing and recommending minimum operating procedures for ensuring an adequate level of security for all data and IT resources for executive branch agencies.

Our audit disclosed that, although written rules and guidelines existed for maintaining an adequate level of security for data and IT resources in general, no written DFS or AEIT guidance existed that specifically addressed protecting cardholder data or complying with the PCI Data Security Standard. In addition, neither DFS nor AEIT had established written policies or procedures addressing the AEIT review of applicable State agency processes or procedures associated with payment card program requests. No agency payment card program approval requests that planned to use the Internet or other related electronic methods as the collection medium had been submitted to DFS or AEIT during the audit period. However, the process for guiding the agencies in the technical aspects of agency payment card acceptance, including the division of responsibilities between DFS and AEIT, was not clearly described in State law, rule, or other policies and procedures. The need for clearer agency guidance is demonstrated in subsequent findings in this report that describe improvements needed in various agency measures to comply with the PCI Data Security Standard or to assess their progress toward compliance.

In response to audit inquiry, management of both DFS and AEIT stated that, instead of reviewing individual agency payment card program requests, the appropriate level of AEIT involvement would be to review the DFS process for evaluating the technical aspects of agency requests, make recommendations to DFS as applicable, and provide other technical advice to DFS as required. However, as stated above, current law provides for AEIT review of agency requests involving the use of the Internet or other related electronic methods as the collection medium.

Recommendation: DFS and AEIT are well positioned to review and guide agency efforts to implement appropriate safeguards over cardholder data in their payment card programs. DFS and AEIT should work together to establish and document a process for guiding State agencies in establishing an adequate level of security over cardholder data within agency payment card programs. As a part of this effort, DFS and AEIT should establish written guidance for the

agencies in maintaining security over cardholder data and complying with applicable provisions of the PCI Data Security Standard. DFS and AEIT should also consider legally available options for responding to instances of agency noncompliance with established guidance or PCI standards. Furthermore, DFS and AEIT should seek clarification in State law, as appropriate, regarding their responsibilities in ensuring that payment card programs use an appropriate technical approach and provide adequate security over cardholder data.

Response: We concur. The Division of Treasury will work with the AEIT to draft legislation that clearly defines program responsibility. We believe legislation should assign oversight of Payment Card Industry (PCI) Data Security Standards to the Chief Financial Officer, providing the CFO authority to set compliance standards and to require annual reporting by agencies of their PCI compliance efforts.

Despite the current lack of statutory direction, the Division of Treasury has undertaken an aggressive approach to educating state agencies about the requirements of the PCI Data Security Standard. This effort has involved presentations to agency officials and serving as an information resource to agencies as needed.

Six-Month Status: DFS has submitted proposed changes to Section 215.322, Florida Statutes for legal review. The change clarifies the roles of the CFO and the AEIT for establishing safeguards over cardholder data within agency payment card programs. This change will be submitted during the 2009-2010 Legislative Session.

Finding No. 2: DFS Payment Card Program Rules and Other Guidance

Effective management includes, among other things, communication of business and IT objectives and direction throughout the enterprise. The information communicated should clearly articulate management's objectives and procedures and be periodically reviewed and, if appropriate, updated to reflect relevant changes in conditions.

DFS promulgated Rule 69C-4, Florida Administrative Code, governing the establishment and acceptance of payment cards by State agencies or the judicial branch. Our audit disclosed provisions of the rules that were out of date. Specifically, the rules:

- Made reference to the State Technology Office that was abolished effective July 1, 2007.
- Made reference to the Bureau of Banking that was renamed the Bureau of Funds Management effective July 1, 2000.
- Had not been updated to reflect certain DFS form changes.

The DFS Division of Treasury Web site provides agencies access to payment card program information and DFS-required forms. Our audit disclosed that certain Web site links provided out-of-date guidance and information or were no longer valid. Specifically:

- Contact information on the Participation Requirements link directed agencies to contact a DFS employee who was no longer the person responsible for payment card activities, including the contract administration function.

- The Web site linked to an outdated form for State agencies' Annual Report to the Chief Financial Officer.

- Certain Web site links provided various documents associated with an expired Bank of America contract, dated October 29, 2001. Additionally, the Information Profile for State of Florida Agencies was not the current form that agencies were required to submit to DFS.

- The MasterCard and Visa 2006 Interchange Programs or Fees Refund Programs links provided information related to outdated interchange rates effective April 2006 and fee refund rates effective October 2005.

- The American Express link provided an expired contract summary and State contract effective January 1, 2004, through December 31, 2006.

- The Procedures for Accepting Credit and Debit Cards – Florida Administrative Code link was no longer valid, returning a message stating that the page had been moved or the uniform resource locator (URL) was incorrect.

The lack of current rules and instructions for State agencies increases the risk that agencies will misunderstand and not consistently follow DFS requirements in administering their payment card programs.

Recommendation: DFS should update its rules to reflect current procedures for the establishment and acceptance of payment cards by State agencies or the judicial branch. In addition, DFS should update its Web site to provide agencies with access to current payment card information and required forms.

Response: We concur that information included in Rule 69C-4, Florida Administrative Code and on the Treasury Web site needed updating.

Treasury staff is in the process of making the recommended updates to Rule 69C-4, Florida Administrative Code. In addition, all Web site links noted in the finding have been updated with current information and materials.

Six-Month Status: DFS staff has submitted needed changes for Rule 69C-4 to management, and the proposed changes are being routed through our Legal Department for review.

The Treasury website has been updated with current documentation.