January 15, 2010

Ms. Kathryn DuBose, Staff Director
Joint Legislative Auditing Committee
Room 876
Claude Pepper Building
111 West Madison Street
Tallahassee, Florida 32399-1400

Dear Ms. DuBose:

Pursuant to Section 20.055(5)(h), Florida Statutes enclosed is the Department’s written explanation of the status of recommendations contained in the Auditor General Report, Information Technology Operational Audit- Department of Financial Services and Selected Participating State Agencies Payment Card Programs Report (Number # 2010-005). If you have any questions in this regard, please call Joseph Aita, Director of Auditing, at 245-3151.

Sincerely,

Richard E. Lober
Inspector General

Enclosure

REL/ ksr

cc: Joseph Aita, Director of Auditing
    Michael Bullock, Director of Division of Recreation and Parks
    Michael W. Sole, Secretary
    John Willmott, Chief of Information Systems
FINDING NUMBER 3: Agency Self-Assessments:
DCA, DEP, DMA, and DOS did not complete the appropriate Self-Assessment Questionnaire to self-evaluate their compliance with the Payment Card Industry (PCI) Data Security Standard.

RECOMMENDATION:
Agencies should ensure that appropriate versions of the Questionnaire are fully completed to evaluate the necessary controls to meet PCI Data Security Standard requirements and protect cardholder data.

DIVISION:
Recreation and Parks

CURRENT STATUS:
All State Parks have disconnected all internet payment applications which alleviates the need to perform quarterly scans or use an approved scanning vendor. Since all credit card, charge card and debit card transactions are processed through the Bank of America approved T7 terminals, that are stand-along dial-up card terminals and considered validation type 3, all state parks are PCI compliant.
FINDING NUMBER 4: Network Scans:
DEP and DMA had not engaged an approved scanning vendor to perform external network scans for applicable payment card applications. In addition, DCA had not successfully passed network scans performed by an approved scanning vendor prior to audit inquiry.

RECOMMENDATION:
Agencies should ensure that approved scanning vendors are engaged to conduct quarterly network scans for vulnerabilities and when detected, are remedied in a timely manner.

DIVISION:
Recreation and Parks

CURRENT STATUS:
At this time, no parks within the Division are subject to quarterly network scans.
FINDING NUMBER 6: Information Security Policies and Procedures:
DCA, DEP, and DMA lacked certain written information security policies and procedures required by the PCI Data Security Standard.

RECOMMENDATION:
DCA, DEP, and DMA should develop written information security policies and procedures to document management’s expectations for the protection of cardholder data and promote compliance with the PCI Data Security Standard.

DIVISION:
Recreation and Parks

CURRENT STATUS:
The Division of Recreation has procedures in place in the Operations Manual that are used by all parks and bureaus to include security policies and standards as required by the Payment Card Industry Data Security Standards, requirement 12 as follows:

- Build and maintain secure computer networks by installing and maintaining firewall configurations to protect card holder data.
- Maintain clearly defined information security responsibilities for all employees and contractors.
- Protect card holder data by restricting physical access to data.
- Use and regularly update anti-virus software in order to maintain secure systems and applications.
- Implement strong access control measures to restrict access to cardholder data.
- Regularly monitor and test networks and security systems by tracking and monitoring all access to network resources and cardholder data.
- Maintain policies that address information security by ensuring that all employees are made aware of the importance of protecting cardholder data and complying with the PCI DSS.
FINDING NUMBER 7: Protection of Cardholder Data:
DEP and DMA point-of-sale systems did not comply with some requirements included in the PCI Data Security Standard.

RECOMMENDATION:
DEP and DMA should continue to assess their compliance with the PCI Data Security Standard to ensure the proper protection of cardholder data.

DIVISION:
Recreation and Parks

CURRENT STATUS:
Installation of a firewall on both of the POS network servers at Homosassa Springs State Park was completed and enabled with an automatic update notification system that will perform said updates when notified. All payment applications have been disconnected from both the POS system and internet service. The Division continues to work with the Office of Technology and Information Systems (OTIS) and has ensured compliance with security policies and standards for stand alone, non-DEP networked computers. Compliance with the OTIS security policies and standards were reached as of March 27, 2009.