REPORT NO. 2010-005
JULY 2009

DEPARTMENT OF FINANCIAL SERVICES AND SELECTED PARTICIPATING STATE AGENCIES

PAYMENT CARD PROGRAMS

Information Technology Operational Audit

For the Period
October 2008 Through January 2009
and Selected Actions Through March 2, 2009

STATE OF FLORIDA
AUDITOR GENERAL
DAVID W. MARTIN, CPA

CHIEF FINANCIAL OFFICER

Pursuant to Article IV, Sections 4.(c) and 5.(a) of the State Constitution, the Chief Financial Officer is an elected member of the Cabinet and serves as the chief fiscal officer of the State. Pursuant to Section 20.121(1), Florida Statutes, the Chief Financial Officer is the head of the Department of Financial Services. The Honorable Alex Sink served as Chief Financial Officer during the audit period.

EXECUTIVE DIRECTOR OF THE AGENCY FOR ENTERPRISE INFORMATION TECHNOLOGY

Pursuant to Section 14.204, Florida Statutes, the Agency for Enterprise Information Technology (AEIT) is created within the Executive Office of the Governor (EOG) and is a separate budget entity, not subject to control, supervision, or direction by EOG in any manner. The head of AEIT is the Governor and Cabinet. The Executive Director of AEIT is appointed by the Governor, confirmed by the Cabinet, and subject to confirmation by the Senate. David W. Taylor served as Executive Director during the audit period.

SECRETARY OF THE DEPARTMENT OF COMMUNITY AFFAIRS

Pursuant to Section 20.18(1), Florida Statutes, the Secretary of the Department of Community Affairs is appointed by the Governor and subject to confirmation by the Senate. Thomas G. Pelham served as Secretary during the audit period.

SECRETARY OF THE DEPARTMENT OF ENVIRONMENTAL PROTECTION

Pursuant to Section 20.255(1), Florida Statutes, the Secretary of the Department of Environmental Protection is appointed by the Governor with the concurrence of three or more members of the Cabinet and is confirmed by the Senate. Michael W. Sole served as Secretary during the audit period.

ADJUTANT GENERAL OF THE DEPARTMENT OF MILITARY AFFAIRS

Pursuant to Section 250.05(3), Florida Statutes, the head of the Department of Military Affairs is the Adjutant General. Pursuant to Section 250.10(1), Florida Statutes, the Adjutant General is appointed by the Governor and subject to confirmation by the Senate. Major General Douglas Burnett served as Adjutant General during the audit period.

SECRETARY OF STATE

Pursuant to Section 20.10(1), Florida Statutes, the head of the Department of State is the Secretary of State, who is appointed by the Governor and subject to confirmation by the Senate. Kurt S. Browning served as Secretary of State during the audit period.

SECRETARY OF THE DEPARTMENT OF TRANSPORTATION

Pursuant to Section 20.23(1)(a), Florida Statutes, the Secretary of the Department of Transportation is appointed by the Governor and subject to confirmation by the Senate. Stephanie C. Kopelousos served as Secretary during the audit period.

The audit team leader was Shawn McCormick, CISA, and the audit was supervised by Shelly Posey, CISA. Please address inquiries regarding this report to Jon Ingram, CPA, CISA, Audit Manager, by e-mail at joningram@aud.state.fl.us or by telephone at (850) 488-0840.

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

DEPARTMENT OF FINANCIAL SERVICES AND SELECTED PARTICIPATING STATE AGENCIES

Payment Card Programs

SUMMARY

Section 215.322(1), Florida Statutes, provides that it is the intent of the Legislature to encourage State agencies, the judicial branch, and units of local government to make their goods, services, and information more convenient to the public through the acceptance of payments by credit cards, charge cards, and debit cards (collectively referred to in this report as payment cards) to the maximum extent practicable when the benefits to the participating agency and the public substantiate the cost of accepting these types of payments. State agencies and the judicial branch may, pursuant to Section 215.322(2), Florida Statutes, accept payment cards in payment for goods and services with the prior approval of the Chief Financial Officer (CFO). The major payment card brands (i.e., Visa, MasterCard, etc.) require entities that accept payment cards in payment for goods and services to comply with Payment Card Industry (PCI) security standards set by the PCI Security Standards Council (Council) to protect cardholder data.

Our audit, for the period October 2008 through January 2009, and selected actions through March 2, 2009, focused on evaluating selected internal controls at the Agency for Enterprise Information Technology (AEIT), Department of Community Affairs (DCA), Department of Environmental Protection (DEP), Department of Financial Services (DFS), Department of Military Affairs (DMA), Department of State (DOS), and Department of Transportation (DOT) relating to compliance with the provisions of Section 215.322, Florida Statutes, pertaining to the acceptance of payment cards by State agencies and other relevant State laws. (See Exhibit A.) Our audit also focused on evaluating selected information technology (IT) controls relating to compliance with the PCI Data Security Standard at DCA, DEP, DMA, and DOS. In addition, we determined the status of corrective actions regarding selected deficiencies disclosed in our report No. 2004-053 that were applicable to the scope of this audit. Our audit was not a PCI Data Security Standard compliance validation assessment pursuant to the requirements of the Council, and we did not validate agencies' compliance with the PCI Data Security Standard.

The results of our audit are summarized below:

Finding No. 1: State agencies need improved guidance for ensuring an appropriate level of security of cardholder data and complying with the PCI Data Security Standard. In addition, DFS and AEIT should seek clarification in State law regarding their responsibilities in providing guidance for securing cardholder data.

Finding No. 2: Guidance and information within DFS rules and the DFS Web site relating to the acceptance of payment cards were out of date.

Finding No. 3: DCA, DEP, DMA, and DOS did not complete the appropriate Self-Assessment Questionnaire to self-evaluate their compliance with the PCI Data Security Standard.

Finding No. 4: 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.

Finding No. 5: Because DOT had engaged a qualified security assessor to perform PCI Data Security Standard assessments of SunPass, we did not similarly evaluate applicable SunPass IT controls. However, the qualified security assessor's initial assessment of SunPass identified 98 instances where security controls required by the PCI Data Security Standard were not in place. Under these conditions, the risk was increased that cardholder data could be breached and that sanctions could be applied by the major payment card brands.

Finding No. 6: **DCA, DEP, and DMA lacked certain written information security policies and procedures required by the PCI Data Security Standard.**

Finding No. 7: **DEP and DMA point-of-sale systems did not comply with some requirements included in the PCI Data Security Standard.**

Finding No. 8: **Certain user identifications (IDs) and passwords to the Sunbiz database were being shared by DOS employees.**

Finding No. 9: **DMA and DOS did not follow certain approval and reporting requirements set forth in Section 215.322, Florida Statutes, and the related DFS rules.**

Finding No. 10: **The DOS Letter of Understanding for payment card services lacked certain provisions required by Sections 287.058(1) and (2), Florida Statutes, and contained outdated provisions.**

Finding No. 11: **DCA lacked appropriate procedures for the reconciliation of income and expenses related to the acceptance of payment cards.**

BACKGROUND

PCI security standards are technical and operational requirements set by the Council to protect cardholder data. The standards globally govern all entities that store, process, or transmit cardholder data. Compliance with PCI security standards is mandatory and is enforced by the major payment card brands, which include American Express, Discover Financial Services (Discover), JCB International (JCB), MasterCard Worldwide (MasterCard), and Visa, Inc. (Visa). The major payment card brands enforce PCI compliance by providing sanctions for entity noncompliance. Sanctions vary by payment card brand but generally include higher processing fees, fines, and denial of the authority to accept payment cards.

The PCI security standards include the Data Security Standard that applies to any entity that stores, processes, or transmits cardholder data and specifies 6 goals and 12 requirements, listed in Exhibit B, that reflect best practices for securing sensitive information. For purposes of the PCI Data Security Standard, payment cards are defined as any payment card or device that bears the logo of the major payment card brands that established the Council. For the purposes of the PCI Data Security Standard, a merchant is defined as any entity (such as a State agency) that accepts payment cards bearing the logos of any of the five members of the Council as payment for goods and services. Service providers are business entities (such as BA Merchant Services LLC) that are not one of the major payment card brands but are directly involved in the processing, storage, or transmission of cardholder data.

Pursuant to Section 215.322(4), Florida Statutes, the CFO may establish contracts with financial institutions, credit card companies, or other entities for processing payment card collections by State agencies and the judicial branch for deposit into the State Treasury or another qualified public depository. The CFO established a contract with Bank of America, N.A., and BA Merchant Services LLC (Bank of America contract), effective January 1, 2007, for services governing the acceptance and processing of Visa and MasterCard transactions and the processing of American Express and Discover transactions for the State. On March 2, 2009, DFS staff indicated that they were aware of 80 agency payment card programs that utilized the State's Bank of America contract and 25 agency payment card programs that utilized other contracts for payment card processing. See Exhibit A for the agency payment card programs within the scope of our audit.

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.

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.

Finding No. 3: Agency Self-Assessments

The PCI Data Security Standard Self Assessment Questionnaire (Questionnaire) is a validation tool intended to assist entities in self-evaluating their compliance with the PCI Data Security Standard. There are four versions of the Questionnaire to meet five validation types established by the Council. The validation types correlate to the methods used by merchants to accept payment cards. The validation requirements vary with each type of payment method. For example, payment methods involving the storage of cardholder data are subject to more stringent security requirements. Therefore, the associated Questionnaire includes more validation steps for the merchant to complete.

Our audit disclosed instances where DCA, DEP, DMA, and DOS did not complete the appropriate Questionnaire to self-evaluate their compliance with the PCI Data Security Standard, increasing the risk that controls protecting cardholder data were not sufficiently assessed and tested. Specifically:

- DCA completed an abbreviated version of the Questionnaire that applied to merchants with payment application systems connected to the Internet that did not store electronic cardholder data. Merchants must certify their eligibility to complete the abbreviated version of the Questionnaire by meeting five specific requirements related to the payment application and surrounding IT infrastructure. However, DCA did not certify its eligibility for four of the five requirements. As a result, DCA could not demonstrate that it had completed the appropriate Questionnaire and self-evaluated its compliance with the PCI Data Security Standard in a complete manner.
- For all park locations, DEP completed one comprehensive Questionnaire for stand-alone dial-up terminal merchants because most park locations processed payment card transactions via stand-alone dial-up card terminals. However, DEP was not eligible to complete the stand-alone dial-up terminal merchant

Questionnaire for the Homosassa Springs State Park because the Park processed payment card transactions via a payment application connected to the Internet. Such payment applications are subject to more stringent security requirements that are incorporated into a different version of the Questionnaire.

- DMA Camp Blanding Exchange staff did not fully complete a Questionnaire to ensure that all necessary controls to protect cardholder data were evaluated.
- DOS inadvertently stored 8,332 payment card account numbers in electronic format in the Sunbiz database obtained from transactions that occurred between March 31, 2000, and December 28, 2001. In response to audit inquiry, DOS staff stated that, in late 2001, DOS discovered that it was receiving a summary file from its service provider that contained payment card account numbers of cardholders. DOS staff determined that the payment card account numbers were not needed and instructed the service provider to discontinue including payment card account numbers on the summary file. DOS staff further indicated that they were not aware that payment card account numbers collected prior to late 2001 were still stored and did not have a business reason to record and retain the stored payment card account numbers. On May 13, 2008, DOS staff completed a Questionnaire intended for merchants that had outsourced card-not-present cardholder data functions for e-commerce, mail, or telephone orders with no card present. However, because DOS had been inadvertently storing cardholder data in the database, the version of the Questionnaire applicable to merchants who store electronic cardholder data should have been completed instead.

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.

Finding No. 4: Network Scans

The PCI Data Security Standard requires all merchants conducting payment card transactions via payment applications connected to the Internet to engage an approved scanning vendor, certified by the Council, to conduct quarterly network scans for vulnerabilities. To demonstrate compliance, a scan must not detect any vulnerabilities indicating features or configurations that are in violation of the PCI Data Security Standard. Our audit disclosed instances where required network scans had not been performed or had detected vulnerabilities that violated the PCI Data Security Standard, jeopardizing the security over cardholder data. Specifically:

- Network scans had not been performed at the DEP Homosassa Springs State Park or at the DMA Camp Blanding Exchange, both of which processed payment card transactions via payment applications connected to the Internet.
- DCA had quarterly network scans performed by an approved scanning vendor on July 1, 2008, August 29, 2008, and December 2, 2008, noting vulnerabilities that violated the PCI Data Security Standard. As a result, DCA, in conjunction with the contractor responsible for the development of the Business Code Information System, were in the process of remediating the vulnerabilities identified in the scans. Subsequent to audit inquiry, DCA staff provided evidence demonstrating that DCA had passed a network scan on February 19, 2009.

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

Finding No. 5: Validation of Data Security Standard Compliance

The major payment card brands require merchants to validate and report PCI Data Security Standard compliance according to their merchant PCI level, which is based on payment card transaction volume over a 12-month period. In 2007, Bank of America notified DOT that the transaction volume in SunPass had reached a threshold upon which

DOT was required to validate its compliance with the PCI Data Security Standard to Bank of America by September 30, 2008. As a part of these requirements, Visa established sanctions, including potential fines, for merchants who were not validated as PCI compliant by the deadline.

In response to the Bank of America notification, DOT engaged a qualified security assessor to perform a PCI Data Security Standard security assessment. Qualified security assessors are certified by the Council to validate an entity's adherence to the PCI Data Security Standard. Because DOT had engaged the qualified security assessor to validate compliance, we did not similarly evaluate applicable SunPass IT controls.

The qualified security assessor's initial assessment, dated July 30, 2008, identified 98 instances where controls required by the PCI Data Security Standard were not in place. For example, routers were not included in the firewall configuration standard, full payment card account numbers of cardholders were stored unencrypted, a formal system development life cycle based on industry best practices and secure coding was not in place, physical access to cardholder data was not appropriately restricted, and some policies and procedures required by the PCI Data Security Standard for the security of cardholder data did not exist. Under these conditions, the risk was increased that cardholder data could be breached and that sanctions could be applied by the major payment card brands.

On September 19, 2008, DOT requested an extension of the September 30, 2008, deadline to December 31, 2008. According to DOT management, Bank of America approved the extension request. SunPass was subsequently reported to have achieved PCI compliance prior to the December 31, 2008, deadline and no sanctions were assessed. Specifically, the qualified security assessor's final assessment, dated December 26, 2008, identified no areas of noncompliance. The qualified security assessor's Report on Compliance and Confirmation of Report Accuracy were reviewed by Bank of America and reported to Visa as validated for compliance with the PCI Data Security Standard.

Recommendation: Because of the volume of cardholder data retained in SunPass, DOT should closely monitor the ongoing effectiveness of SunPass security controls in complying with the PCI Data Security Standard and protecting cardholder data.

Finding No. 6: Information Security Policies and Procedures

Effective information security policies and procedures set the security tone for an agency and inform employees of what is expected of them regarding the protection of sensitive entity data. The PCI Data Security Standard requires merchants to establish, publish, maintain, and disseminate information security policies and procedures.

As previously discussed in Finding No. 3, the PCI Data Security Standard Self Assessment Questionnaire is a validation tool intended to assist entities in self-evaluating their compliance with the PCI Data Security Standard. Our review of Questionnaires completed by DCA on December 2, 2008; DEP Division of Recreation and Parks on June 30, 2008; and DMA on November 18, 2008, disclosed that certain written information security policies and procedures required by the PCI Data Security Standard for the security of cardholder data did not exist. As of March 2, 2009, pursuant to audit inquiry, the three agencies still lacked the applicable written information security policies and procedures. Without information security policies and procedures governing the protection of cardholder data, the risk is increased that appropriate security controls will not be followed consistently and in a manner pursuant to management's expectations and PCI requirements.

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.

Finding No. 7: Protection of Cardholder Data

DEP and DMA operated point-of-sale systems that were subject to various PCI compliance requirements for the protection of cardholder data. Our audit disclosed instances where DEP and DMA point-of-sale systems did not comply with the PCI Data Security Standard. Specifically:

- PCI Data Security Standard Requirement 1 requires that a firewall configuration be installed and maintained to protect cardholder data. Firewalls were not utilized on Internet-facing connections at the DEP Homosassa Springs State Park and DMA Camp Blanding Exchange point-of-sale systems. In response to audit inquiry, DEP disconnected its point-of-sale system. Additionally, DMA subsequently installed a firewall.
- PCI Data Security Standard Requirement 3 requires merchants to protect stored cardholder data. However, the full payment card account numbers of cardholders were stored unencrypted in The General Store point-of-sale system at DMA and displayed on reports generated by The General Store point-of-sale system without an established business purpose for retaining the cardholder data. DMA subsequently replaced The General Store point-of-sale system with a QuickBooks point-of-sale system that did not store full payment card account numbers in electronic form or display the numbers on reports.
- PCI Data Security Standard Requirement 5 requires that antivirus software be used and regularly updated. Antivirus software on systems running the payment application at the DMA Camp Blanding Exchange was not updated to current versions with current virus definitions to protect the system from malicious programs. Upon implementation of the QuickBooks point-of-sale system, DMA updated the antivirus software.
- PCI Data Security Standard Requirement 6 includes a requirement that all system components and software have the latest vendor-supplied security patches installed. At the DEP Homosassa Springs State Park, automatic updating of operating systems under which the payment applications reside was disabled, resulting in security patches not being applied to the operating systems. In response to audit inquiry, DEP enabled automatic updating of operating systems on February 20, 2009.
- PCI Data Security Standard Requirement 10 requires tracking and monitoring of accesses to cardholder data, such as cardholder payment card account numbers. However, at DMA, The General Store point-of-sale system did not have the capability to track and monitor accesses of cardholder data. The replacement QuickBooks point-of-sale system stored only partial payment card account numbers and no other cardholder data.
- The Council provides a list of payment applications that have been validated for compliance with the PCI Data Security Standard. The General Store point-of-sale system utilized in processing payment card transactions by the DMA Camp Blanding Exchange was not validated to assure that the system properly processed payment card transactions and enforced proper security controls over cardholder data. The replacement QuickBooks point-of-sale system has been validated by the Council.

Without continued compliance with the PCI Data Security Standard, the risk is increased that cardholder data will be inappropriately disclosed and exploited.

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

Finding No. 8: User Identification and Authentication

Effective access controls include a process for the unique identification and authentication of system users. The unique identification of system users allows management to affix responsibility for system activity to an individual person. DOS Access Controls Policy requires each user's identification to be unique and assigned to only one person.

Our audit disclosed that eight DOS employees shared four user IDs and passwords to support the DOS Sunbiz database. The absence of unique user IDs increases the risk that management will be unable to timely determine the persons responsible for system actions.

Recommendation: DOS should cease the practice of sharing user IDs and passwords and assign individual user IDs to all system users as provided for in its Access Controls Policy.

Finding No. 9: Approval and Reporting Requirements

As previously discussed, Section 215.322, Florida Statutes, and related DFS Rule 69C-4, Florida Administrative Code, govern the establishment and acceptance of payment cards by State agencies and the judicial branch. Our audit disclosed instances where DMA and DOS did not follow certain approval and reporting requirements set forth in Section 215.322, Florida Statutes, and the related DFS rules. Specifically:

- Section 215.322(4), Florida Statutes, provides that State agencies shall use at least one of the contractors established by the CFO for the acceptance of payment cards, unless the State agency obtains authorization from the CFO to use another contractor that is more advantageous to such State agency. The DMA Camp Blanding Exchange did not use the standard Bank of America contract established by the CFO and, contrary to State law, had not obtained authorization from the CFO to use an alternative service provider. On June 29, 2005, DMA entered into an agreement with Capital City Bank, an alternative service provider for processing payment cards, without prior authorization from the CFO. On December 26, 2008, DMA began utilizing another service provider, Innovative Merchant Solutions LLC, without obtaining the prior approval of the CFO.
- DFS Rule 69C-4.009, Florida Administrative Code, provides that State agencies with an established payment card operation shall file an annual report with the CFO containing information for each type of transaction related to the fiscal year just ended. DMA and DOS had not filed the required annual reports with the CFO, limiting the CFO's ability to monitor the agencies payment card operations.

Recommendation: DMA should seek the prior approval of the CFO before entering into future contracts with service providers not established by the CFO for the acceptance of payment cards. In addition, DMA and DOS should file annual reports with the CFO as required by DFS rules.

Finding No. 10: Payment Card Services Letter of Understanding

Sections 287.058(1) and (2), Florida Statutes, provide that every procurement of contractual services in excess of the threshold amount provided in Section 287.017, Florida Statutes, for Category Two (currently $25,000) shall be evidenced by a written agreement that includes certain required provisions. DOS entered into a Letter of Understanding with Link2Gov dated June 15, 2000, regarding payment card services for accepting corporate filing fee payments. For the 2008 calendar year, Link2Gov retained $5,312,482 of the $155,743,288 in fees collected for the DOS Division of Corporations.

Our audit disclosed aspects of the DOS payment card services Letter of Understanding that lacked provisions required in Section 287.058(1), Florida Statutes. Specifically, the Letter of Understanding lacked provisions:

- Allowing unilateral cancellation by DOS for refusal by the contactor to allow public access to all documents, papers, letters, or other materials made or received by the contractor in conjunction with the contract.
- Dividing the contract into units of deliverables.
- Specifying the criteria and the final date by which such criteria must be met for completion of the contract.

- Specifying that the contract may be renewed for a period that may not exceed three years or the term of the original contract, whichever period is longer.
- Specifying that renewals shall be contingent upon satisfactory performance evaluations by DOS and subject to the availability of funds.

Section 287.058(2), Florida Statutes, provides that written agreements in excess of the threshold for Category Two shall be signed by the agency head. The DOS Letter of Understanding with Link2Gov was signed by the Director of the Division of Corporations.

In addition, our audit disclosed that the Letter of Understanding contained outdated provisions addressing electronic check payments that are no longer processed by Link2Gov. The Letter of Understanding also did not provide for fee adjustments or reflect the current fees that were being charged by Link2Gov. Furthermore, since the Letter of Understanding did not provide for a contract term or renewal options, DOS continued to utilize the services of Link2Gov without competitive resolicitation. Without appropriate contract provisions as required by State law, the risk is increased that the DOS payment card Letter of Understanding will not serve the best interests of the State.

Recommendation: In consultation with DFS, DOS should consider utilizing the DFS-established payment card services contract that is competitively resolicited on a periodic basis. If DOS determines that, in its specific circumstances, the established DFS contract is not in the best interest of the State, DOS should ensure that alternative contracts include provisions required by State law and that the provisions reflect current business practices.

Finding No. 11: Income and Expense Reconciliation

Effective management of payment card operations includes the performance of timely reconciliations of income and expenses related to the acceptance of payment cards. Reconciliation procedures within a payment card process would typically identify differences between sales transactions that occur on an agency's Web site and amounts collected and remitted to the State and would be expected to account for any associated service charges.

Our audit disclosed that DCA lacked appropriate procedures for the reconciliation of income and expenses related to the acceptance of payment cards, limiting the ability of DCA to ensure the appropriateness of amounts remitted to the State by service providers. Specifically:

- DCA did not perform reconciliations between DCA Building Code Information System data and reports provided by Bank of America, American Express, and Discover.
- Service charges being assessed by Bank of America, American Express, and Discover were not being evaluated by DCA to ensure that the service charges were in accordance with the rates outlined in the respective contracts.
- Fees for product approvals that were collected by payment card on behalf of the State by Bank of America, American Express, and Discover were remitted directly to a company that had been contracted by DCA to perform the product approval function. The company paid the service charges to Bank of America, American Express, and Discover and remitted a portion of the collections to DCA. DCA did not take steps to ensure that the amounts being remitted to DCA by the company were in accordance with the fee structure established in the contract.

Recommendation: DCA should perform appropriate reconciliations of income and expenses related to the acceptance of payment cards and promptly investigate and resolve any reconciling items in a timely manner to ensure that the State is receiving and expensing appropriate funds.

PRIOR AUDIT FINDINGS

DEP and DFS had corrected the deficiencies disclosed in our report No. 2004-053 that were applicable to the scope of this audit.

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 IT operational audit in accordance with applicable 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.

The objectives of this IT operational audit were to determine:

- The effectiveness of selected internal controls at AEIT, DCA, DEP, DFS, DMA, DOS, and DOT in achieving compliance with the provisions of Section 215.322, Florida Statutes, pertaining to the acceptance of payment cards by State agencies and other relevant State laws.
- The effectiveness of selected IT controls at DCA, DEP, DMA, and DOS in achieving compliance with the PCI Data Security Standard.
- Whether DFS and DEP had corrected, or were in the process of correcting, selected deficiencies disclosed in our report No. 2004-053 that were applicable to the scope of this audit.
- Statutory and fiscal changes that may be recommended to the Legislature pursuant to Section 11.45(7)(h), Florida Statutes.

Our audit, for the period October 2008 through January 2009, and selected actions through March 2, 2009, focused on selected IT controls relating to compliance with the PCI Data Security Standard. The audit included selected general IT controls at DCA (Building Code Information System), DEP (Florida State Parks and Centralized Payment System), DMA (The General Store and QuickBooks), DOS (Sunbiz), and DOT (SunPass) over systems software and database management, logical access to programs and data, and physical safeguards. In addition, the audit included selected controls relating to DFS and AEIT responsibilities regarding State agency payment card acceptance pursuant to 215.322, Florida Statutes. Our audit was not a PCI Data Security Standard compliance validation assessment pursuant to the requirements of the Council, and we did not validate agencies' compliance with the PCI Data Security Standard.

In conducting our audit, we:

- Interviewed AEIT, DCA, DEP, DFS, DMA, DOS, and DOT staff.
- Obtained an understanding of selected State agencies' roles in the payment flow; the extent to which the agencies store, process, and transmit cardholder data; and the provisions of agency contracts with service providers that process payment card collections.
- Obtained an understanding of DFS and AEIT legal authority, purpose, and responsibilities pursuant to 215.322, Florida Statutes, pertaining to the acceptance of payment cards by State agencies.
- Obtained an understanding of the provisions of the DFS contract with Bank of America for processing payment card collections for deposit into the State Treasury.

- Observed, documented, and tested the effectiveness of selected internal controls at AEIT, DCA, DEP, DFS, DMA, DOS, and DOT in achieving compliance with the provisions of Section 215.322, Florida Statutes, pertaining to the acceptance of payment cards by State agencies and other relevant State laws.
- Observed, documented, and tested the effectiveness of selected IT controls at selected State agencies relevant to the PCI Data Security Standard.

AUTHORITY

Pursuant to the provisions of Section 11.45, Florida Statutes, I have directed that this report be prepared to present the results of our IT operational audit.

David W. Martin, CPA
Auditor General

MANAGEMENTS' RESPONSES

In letters dated July 10, 2009, through July 21, 2009, respectively, the heads of the applicable agencies provided responses to our preliminary and tentative findings. The letters are included at the end of this report as Exhibit C.

EXHIBIT A
SELECTED PARTICIPATING STATE AGENCIES
PAYMENT CARD PROGRAMS

Agency Payment Card Program	Payment Card Service Provider/ Processor	2008 Annual Number of Transactions (Unaudited)	2008 Total Annual Fees and Costs to Agency (Unaudited)
DCA Division of Housing and Community Development - Building Code Information System	BA Merchant Services LLC	4,960	$3,030
DEP Division of Recreation and Parks – Florida State Parks	BA Merchant Services LLC	194,618	$173,193
DEP Division of Waste Management - Centralized Payment System	BA Merchant Services LLC	972	$3,569
DMA Camp Blanding Exchange – The General Store and QuickBooks	Capital City Bank and Innovative Merchant Solutions LLC	24,000 (combined)	$27,855 (combined)
DOS Division of Corporations – Sunbiz	Link2Gov	1,148,390	$5,312,482
DOT Florida's Turnpike Enterprise -SunPass	BA Merchant Services LLC	19,901,154	$11,398,212

EXHIBIT B
PCI DATA SECURITY STANDARD
GOALS AND REQUIREMENTS FOR MERCHANTS AND SERVICE PROVIDERS

Goals	PCI Data Security Standard Requirements
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update antivirus software 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security

EXHIBIT C
MANAGEMENTS' RESPONSES

STATE OF FLORIDA

DEPARTMENT OF COMMUNITY AFFAIRS

"Dedicated to making Florida a better place to call home"

CHARLIE CRIST
Governor

THOMAS G. PELHAM
Secretary

July 10, 2009

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

Re: Information Technology Audit of the Department of Financial Services and Selected Participating State Agencies Payment Card Programs

Dear Mr. Martin:

This letter is to provide the Department's responses to the preliminary and tentative findings dated June 12, 2009, regarding the Department of Financial Services and Selected Participating State Agencies, Payment Card Programs, Information Technology Operational Audit.

Finding No. 3: DCA, DEP, DMA, and DOS did not complete the appropriate Self-Assessment Questionnaire to self-evaluate their compliance with the PCI Data Security Standard.

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

Department Response: DCA completed a self assessment provided by SecurityMetrics, our PCI-approved scanning contractor. We concur that we should have also completed the latest version of the official PCI Self-Assessment Questionnaire provided by the PCI Security Standards Council.

Finding No. 4: 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.

2555 SHUMARD OAK BOULEVARD ♦ TALLAHASSEE, FL 32399-2100
850-488-8466 (p) ♦ 850-921-0781 (f) ♦ Website: www.dca.state.fl.us
♦ COMMUNITY PLANNING 850-488-2356 (p) 850-488-3309 (f) ♦ FLORIDA COMMUNITIES TRUST 850-922-2207 (p) 850-921-1747 (f) ♦
♦ HOUSING AND COMMUNITY DEVELOPMENT 850-488-7956 (p) 850-922-5623 (f) ♦

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

David W. Martin, Auditor General
July 10, 2009
Page 2

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

Department Response: The Department concurs with this preliminary finding. DCA had been working on a variety of network infrastructure changes and, as noted in the detailed audit finding, did pass a network scan dated February 19, 2009, subsequent to the audit inquiry. DCA has also passed a later quarterly scan dated May 19, 2009.

Finding No. 6: DCA, DEP, and DMA lacked certain written information security policies and procedures required by the PCI Date Security Standard.

Auditor General 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.

Department Response: DCA has completed a comprehensive set of Department Security Policies and Procedures. These documents are in the final stages of Department review.

Finding No. 11: DCA lacked appropriate procedures for the reconciliation of income and expenses related to the acceptance of payment cards.

Auditor General Recommendation: DCA should perform appropriate reconciliations of income and expenses related to the acceptance of payment cards and promptly investigate and resolve any reconciling items in a timely manner to ensure that the State is receiving and expensing appropriate funds.

Department Response: DCA agrees with this preliminary finding. Effective January 1, 2009, DCA revised its procedures to perform reconciliations between the DCA Building Code Information System data and reports provided by Bank of America, American Express, and Discover to ensure the service charges are in accordance with the rates outlined in the respective contracts. These revised procedures also enable statements to be pulled directly from the Bank of America and DCA Building Code Information System to insure the amounts being remitted are in accordance with the fee structure established in the contract.

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

David W. Martin, Auditor General
July 10, 2009
Page 3

On behalf of the Department, we look forward to your final audit findings and recommendations and will implement corrective actions, as appropriate.

Sincerely yours,

Tom Pelham

Thomas G. Pelham
Secretary

TGP/cmf

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

STATE OF FLORIDA
Department of Military Affairs
Office of the Adjutant General
St. Francis Barracks, P.O. Box 1008
St. Augustine, Florida 32085-1008

July 10, 2009

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

Dear Mr. Martin:

In accordance with Section 11.45(4)(d), *Florida Statutes*, enclosed is the Florida Department of Military Affairs' (DMA) explanation of actual or proposed corrective actions related to preliminary audit findings which may be included in a report to be prepared by your office. This review concerned 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. Our response is directed to Finding Nos. 3, 4, 6, 7, and 9 which your audit determined related to the DMA.

We are pleased to note that corrective actions have been completed or are being aggressively pursued.

Finding No. 3: Agency Self-Assessments

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

On, or about, April 21, 2009, the DMA Camp Blanding Joint Training Center Post Exchange completed the appropriate questionnaire. The questionnaire will be completed on an annual basis to ensure compliance with the PCI Data Security Standard.

Finding No. 4: Network Scans

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

An approved scanning vendor (ASV) has been selected and an appropriate scan will be performed prior to July 15, 2009. Additionally, ASV will perform external network scans for applicable payment card applications on a quarterly basis.

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Finding No. 6: Information Security Policies and Procedures

Recommendation: 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.

Management of the Post Exchange is in the process of developing appropriate policies and procedures to ensure compliance with PCI Data Security Standards. This matter will be completed in a timely manner.

Finding No. 7: Protection of Cardholder Data

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

The implementation of the QuickBooks point-of-sale system will continue to ensure that the DMA is in compliance with the PCI Data Security Standard and provide proper protection of cardholder data.

Finding No. 9: Approval and Reporting Requirements

Recommendation: DMA should seek the prior approval of the CFO before entering into future contracts with service providers not established by the CFO for the acceptance of payment cards. In addition, DMA should file annual reports with the CFO as required by DFA rules.

The DMA is in the process of preparing appropriate requests to the CFO for approval of the use of service providers not established by the CFO for the acceptance of payment cards. Additionally, through improved coordination with the DMA's reporting activity, the filing of annual reports with the CFO will be improved to comply with DFA rules.

We appreciate the courtesies and professionalism of your staff throughout the audit process. If you have any questions, or if you require any additional information, please do not hesitate to contact Ms. Leslye Stevenson, Post Exchange Manager, at (904) 682-3513 or Mr. Edward C. Mosca, CPA, State Inspector General, at (904) 823-0220.

Sincerely,

DOUGLAS BURNETT
Major General, FLANG
The Adjutant General

Copy Furnished:
Mr. Jon Ingram, Audit Manager
Mr. Shawn McCormick, IT Auditor

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Florida Department of Transportation

CHARLIE CRIST
GOVERNOR

605 Suwannee Street
Tallahassee, FL 32399-0450

STEPHANIE C. KOPELOUSOS
SECRETARY

July 10, 2009

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

Dear Mr. Martin:

I am pleased to respond to the preliminary and tentative audit findings and recommendations concerning the operational audit of:

Department of Financial Services and Selected Participating State Agencies
Payment Card Programs
for the period October 2008 through January 2009

As required by Section 11.45(4)(d), Florida Statutes, our response to the finding is enclosed.

I appreciate the efforts of you and your staff in assisting to improve our operations. If you have any questions, please contact our Inspector General, Ron Russo, at 410-5800.

Sincerely,

SCKopel

Stephanie C. Kopelousos
Secretary

SCK:hmt

Enclosure

cc: Ron Russo, Inspector General

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

FLORIDA DEPARTMENT OF TRANSPORTATION

Response to the Auditor General's Preliminary and Tentative Audit Findings and Recommendations

Information Technology Operational Audit Payment Card Program October 2008 through January 2009

Finding No. 5: Validation of Data Security Standard Compliance

The major payment card brands require merchants to validate and report PCI Data Security Standard compliance according to their merchant PCI level, which is based on payment card transaction volume over a 12-month period. In 2007, Bank of America notified DOT that the transaction volume in SunPass had reached a threshold upon which DOT was required to validate its compliance with the PCI Data Security Standard to Bank of America by September 30, 2008. As a part of these requirements, Visa established sanctions, including potential fines, for merchants who were not validated as PCI compliant by the deadline.

In response to the Bank of America notification, DOT engaged a qualified security assessor to perform a PCI Data Security Standard security assessment. Qualified security assessors are certified by the Council to validate an entity's adherence to the PCI Data Security Standard. Because DOT had engaged the qualified security assessor to validate compliance, we did not similarly evaluate applicable SunPass IT controls.

The qualified security assessor's initial assessment, dated July 30, 2008, identified 98 instances where controls required by the PCI Data Security Standard were not in place. For example, routers were not included in the firewall configuration standard, full payment card account numbers of cardholders were stored unencrypted, a formal system development life cycle based on industry best practices and secure coding was not in place, physical access to cardholder data was not appropriately restricted, and some policies and procedures required by the PCI Data Security Standard for the security of cardholder data did not exist. Under these conditions, the risk was increased that cardholder data could be breached and that sanctions could be applied by the major payment card brands.

On September 19, 2008, DOT requested an extension of the September 30, 2008, deadline to December 31, 2008. According to DOT management, Bank of America approved the extension request. SunPass was subsequently reported to have achieved PCI compliance prior to the December 31, 2008, deadline and no sanctions were assessed. Specifically, the qualified security assessor's final assessment, dated December 26, 2008, identified no areas of noncompliance. The qualified security assessor's Report on Compliance and Confirmation of Report Accuracy were reviewed by Bank of America and reported to Visa as validated for compliance with the PCI Data Security Standard.

Recommendation: Because of the volume of cardholder data retained in SunPass, DOT should closely monitor the ongoing effectiveness of SunPass security controls in complying with the PCI Data Security Standard and protecting cardholder data.

Management Response: Florida's Turnpike Enterprise concurs and acknowledges the finding and recommendation. Due to the volume of credit card and customer information processed and managed by the SunPass program, we have and will continue to focus our efforts on protecting the confidentiality, integrity and availability of customer data.

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Florida Department of Environmental Protection
Marjory Stoneman Douglas Building
3900 Commonwealth Boulevard
Tallahassee, Florida 32399-3000

Charlie Crist
Governor

Jeff Kottkamp
Lt. Governor

Michael W. Sole
Secretary

July 13, 2009

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

Dear Mr. Martin:

Enclosed is the Division of Recreation and Parks' response pertaining to the Preliminary and Tentative Audit Findings from the Information Technology Operational Audit of the Department of Financial Services and Selected Participating State Agencies Payment Card Programs for the period October 2008 through January 2009. As noted in the enclosure, the Division of Recreation and Parks has taken the appropriate actions and revised policies to ensure that appropriate Payment Card Industry (PCI) Standards are followed.

If you have questions in this regard, please call Joseph Aita, Director of Auditing, at 850-245-3151. Thank you for the opportunity to respond.

Sincerely,

Michael W. Sole
Secretary

REL/ja/ksr
Enclosure

cc: Mike Bullock, Director, Division of Recreation and Parks
Rufus Noble, Director, Division of Administrative Services
John Willmott, Chief of the Office of Information and Technology Services

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Memorandum **Florida Department of Environmental Protection**

DATE: June 24, 2009

TO: Joseph Aita, Director of Auditing
Office of Inspector General

FROM: Mike Bullock, Director
Division of Recreation and Parks

SUBJECT: Preliminary and Tentative Audit Findings from Information Technology Operational Audit of Payment Card Programs
Division of Recreation and Parks

This memorandum will serve as the Division's response to Preliminary and Tentative Audit Findings from the Information Technology Operational Audit of the Division's payment card programs for the period October 2008 through January 2009. Recommendations implemented have provided improved security policies and standards to protect cardholder information and DEP and non-DEP networks. Please see the summary of corrective actions taken by the Division and completion dates below.

Finding No. 3, Agency Self-Assessments:
The PCI Data Security Standard Self Assessment Questionnaire (Questionnaire) is a validation tool intended to assist entities in self-evaluating their compliance with the PCI Data Security Standard. There are four versions of the Questionnaire to meet five validation types established by the Council. The validation types correlate to the methods used by merchants to accept payment cards. The validation requirements vary with each type of payment method. For example, payment methods involving the storage of cardholder data are subject to more stringent security requirements. Therefore, the associated Questionnaire includes more validation steps for the merchant to complete. Our audit disclosed instances where DCA, DEP, DMA, and DOS did not complete the appropriate Questionnaire to self-evaluate their compliance with the PCI Data Security Standard, increasing the risk that controls protecting cardholder data were not sufficiently assessed and tested. Specifically:

- For all park locations, DEP completed one comprehensive Questionnaire for stand-alone dial-up terminal merchants because most park locations

processed payment card transactions via stand-alone dial-up card terminals. However, DEP was not eligible to complete the stand-alone dial-up terminal merchant Questionnaire for the Homosassa Springs State Park because the Park processed payment card transactions via a payment application connected to the Internet. Such payment applications are subject to more stringent security requirements that are incorporated into a different version of the Questionnaire.

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 Response:
Completed. Homosassa Springs State Park has disconnected all payment applications from both the Catapult POS system and the BrightHouse Internet service, which disqualifies them from completing a SAQ type C and from performing quarterly scans or using an Approved Scanning Vendor (ASV). Since all credit card, charge card and debit card transactions are processed through the Bank of America approved T7 terminals, which are stand-alone dial-up card terminals, Homosassa Springs State Park is considered validation type 3 allowing them to be included in the annual SAQ type B, completed as of March 27, 2009.

Finding No. 4, Network Scans:
The PCI Data Security Standard requires all merchants conducting payment card transactions via payment applications connected to the Internet to engage an approved scanning vendor, certified by the Council, to conduct quarterly network scans for vulnerabilities. To demonstrate compliance, a scan must not detect any vulnerability indicating features or configurations that are in violation of the PCI Data Security Standard. Our audit disclosed instances where required network scans had not been performed or had detected vulnerabilities that violated the PCI Data Security Standard, jeopardizing the security over cardholder data. Specifically:

- Network scans had not been performed at the DEP Homosassa Springs State Park or at the DMA Camp Blanding Exchange, both of which processed payment card transactions via payment applications connected to the Internet.

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

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

Division Response:
Completed. At this time, no parks within the Division are subject to quarterly network scans. (Please see Division Response to Finding No. 3.)

Finding No. 6, Information Security Policies and Procedures:
Effective information security policies and procedures set the security tone for an agency and inform employees of what is expected of them regarding the protection of sensitive entity data. The PCI Data Security Standard requires merchants to establish, publish, maintain, and disseminate information security policies and procedures. As previously discussed in Finding No. 3, the PCI Data Security Standard Self Assessment Questionnaire is a validation tool intended to assist entities in self-evaluating their compliance with the PCI Data Security Standard. Our review of Questionnaires completed by DCA on December 2, 2008; DEP Division of Recreation and Parks on June 30, 2008; and DMA on November 18, 2008, disclosed that certain written information security policies and procedures required by the PCI Data Security Standard for the security of cardholder data did not exist. As of March 2, 2009, pursuant to audit inquiry, the three agencies still lacked the applicable written information security policies and procedures. Without information security policies and procedures governing the protection of cardholder data, the risk is increased that appropriate security controls will not be followed consistently and in a manner pursuant to management's expectations and PCI requirements.

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 Response:
Completed. The Division of Recreation and Parks has updated the Operations Manual used by all parks and bureaus to include security policies and standards as required by the Payment Card Industry Data Security Standards, requirement 12. Specifically:

- Build and maintain secure computer networks by installing and maintaining firewall configurations to protect card holder data. Clearly defined information security responsibilities for all employees and contractors.

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

- 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 card holder 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 card holder data and complying with the PCI DSS.

Finding No. 7, Protection of Cardholder Data:
DEP and DMA operated point-of-sale systems that were subject to various PCI compliance requirements for the protection of cardholder data. Our audit disclosed instances where DEP and DMA point-of-sale systems did not comply with the PCI Data Security Standard. Specifically:

- PCI Data Security Standard Requirement 1 requires that a firewall configuration be installed and maintained to protect cardholder data. Firewalls were not utilized on Internet-facing connections at the DEP Homosassa Springs State Park and DMA Camp Blanding Exchange point-of-sale systems. In response to audit inquiry, DEP disconnected its point-of-sale system. Additionally, DMA subsequently installed a firewall.
- PCI Data Security Standard Requirement 6 includes a requirement that all system components and software have the latest vendor-supplied security patches installed. At the DEP Homosassa Springs State Park, automatic updating of operating systems under which the payment applications reside was disabled, resulting in security patches not being applied to the operating systems. In response to audit inquiry, DEP enabled automatic updating of operating systems on February 20, 2009.

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

Division Response:
Ongoing. After consultation with the Auditor General's office, the staff at Homosassa Springs State Park established, through its internet service provider BrightHouse Network, the installation of the available firewall (Sonic Firewall) on both of the POS network servers. Firewall installation was completed as of March 13, 2009. The Homosassa Springs State Park staff enabled the automatic updates notification and will continue to perform said updates when notified. The automatic updates notification was enabled on February 20, 2009. All

payment applications have been disconnected from both the Catapult POS system and the BrightHouse Internet service. The Division continues to work with 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 was reached as of March 27, 2009.

MB/cl

CC: Valerie Peacock
Rufus Noble
Steve Dana
Rick Lober
John Willmott

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

CHIEF FINANCIAL OFFICER
STATE OF FLORIDA

ALEX SINK

July 13, 2009

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

Dear Mr. Martin:

Pursuant to Section 11.45(4)(d), Florida Statutes, the enclosed response is provided for the preliminary and tentative audit findings included in the Auditor General's Operational 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 Bob Clift, Inspector General, at (850) 413-4960.

Sincerely,

James R Cassady
Chief of Staff
for

Alex Sink

Enclosure

DEPARTMENT OF FINANCIAL SERVICES
THE CAPITOL, TALLAHASSEE, FLORIDA 32399-0301 • (850) 413-2850 • FAX (850) 413-2950

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Florida Department of Financial Services and Selected Participating State Agencies
Audit Response
Payment Card Programs
Information Technology Audit
Preliminary and Tentative Audit Findings
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.

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.

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

- 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.

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Governor Charlie Crist
Attorney General Bill McCollum
Chief Financial Officer Alex Sink
Commissioner Charles H. Bronson

Agency for Enterprise Information Technology
David W. Taylor
Executive Director
State Chief Information Officer

July 16, 2009

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

Dear Mr. Martin:

I have reviewed the preliminary and tentative audit findings and recommendations on your Information Technology Audit of the Department of Financial Services (DFS) and Selected Participating State Agencies Payment Card Programs.

In response to Finding No. 1:
State agencies need improved guidance for ensuring an appropriate level of security of cardholder data and for complying with the PCI Data Security Standard. In addition, DFS and AEIT should seek clarification in State law regarding their responsibilities in providing guidance for securing cardholder data. We agree.

We are available to work with DFS 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. We are also available to work with DFS in seeking clarification in State law, as appropriate, regarding our individual responsibilities regarding this matter.

If you have any questions, please contact me as below.

Sincerely,

David W. Taylor
Executive Director and State CIO
Agency for Enterprise Information Technology
4030 Esplanade Way, Suite 135
Tallahassee, FL 32399-0950
Phone: 850-922-7502

cc: Mike Russo

Agency for Enterprise Information Technology
4030 Esplanade Way, Ste 135
Tallahassee, Florida 32399-0950
850.922.7502: TEL, 850.487.9937: FAX

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

FLORIDA DEPARTMENT of STATE

CHARLIE CRIST
Governor

KURT S. BROWNING
Secretary of State

July 21, 2009

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

Re: Preliminary and Tentative Audit Findings - Department of Financial Services and Selected Participating State Agencies - Payment Card Programs

Dear Mr. Martin:

Attached is the Department of State's response to the preliminary and tentative audit findings.

If you have questions or require additional information, please contact Dawn K. Roberts, Assistant Secretary of State, at 245-6524. Thank you for the opportunity to respond to your report.

Sincerely,

Kurt S. Browning
Secretary of State

Attachment (1)

cc. Dawn K. Roberts, Assistant Secretary of State
Jennifer Kennedy, Deputy Secretary of State
Kirby J. Mole, Inspector General

R. A. Gray Building • 500 South Bronough Street • Tallahassee, Florida 32399-0250
Telephone: (850) 245-6500 • Facsimile: (850) 245-6125
www.dos.state.fl.us

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Preliminary and Tentative Audit Findings

DEPARTMENT OF FINANCIAL SERVICES
AND
SELECTED PARTICIPATING STATE AGENCIES
Payment Card Programs

Information Technology Operational Audit

July 17, 2009

The audit from October 2008 through January 2009, and selected actions through March 2, 2009, focused on evaluating selected internal controls at the Agency for Enterprise Information Technology (AEIT), Department of Community Affairs (DCA), Department of Environmental Protection (DEP), Department of Financial Services (DFS), Department of Military Affairs (DMA), Department of State (DOS), and Department of Transportation (DOT) relating to compliance with the provisions of Section 215.322, Florida Statutes, pertaining to the acceptance of payment cards by State agencies and other relevant State laws.

The audit also focused on evaluating selected information technology (IT) controls related to compliance with the PCI Data Security Standard at DCA, DEP, DMA, and DOS. In addition, we determined the status of corrective actions regarding selected deficiencies disclosed in our report No. 2004-053 that were applicable to the scope of this audit. Our audit was not a Payment Card Industry, (PCI) Data Security Standard compliance validation assessment pursuant to the requirements of the Council, and we did not validate agencies' compliance with the PCI Data Security Standard.

Auditor General's Finding No. 3: Agency Self-Assessments

Auditor General's 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.

Department's Response:
Conditions which necessitated this recommendation have changed. We are meeting with members of the Department of Financial Services on July 15, 2009, in order to determine which, if any, questionnaire we need to complete. The CIO will submit the appropriate questionnaire at the appropriate time.

Auditor General's Finding No. 8: User Identification and Authentication

Auditor General's Recommendation :
DOS should cease the practice of sharing user IDs and passwords and assign individual user IDs to all system users as provided for in its Access Controls Policy.

EXHIBIT C (CONTINUED)
MANAGEMENTS' RESPONSES

Department's Response:
This recommendation has already been implemented. Each user now has an individual user ID that is in accordance with the Department's security policy.

Auditor General's Finding No. 9Approval and Reporting Requirements

Auditor General's Recommendation:
DMA should seek the prior approval of the CFO before entering into future contracts with service providers not established by the CFO for the acceptance of payment cards. In addition, DMA and DOS should file annual reports with the CFO as required by DFS rules. **NOTE: DMA is the Department of Military Affairs.**

Department's Response:
The appropriate annual reports will be filed by the CIO on behalf of the Department of State.

Auditor General's Finding No. 10 Payment Card Services Letter of Understanding

Auditor General's Recommendation:
In consultation with DFS, DOS should consider utilizing the DFS-established payment card services contract that is competitively resolicited on a periodic basis. If DOS determines that, in its specific circumstances, the established DFS contract is not in the best interest of the State, DOS should ensure that alternative contracts include provisions required by State law and that the provisions reflect current business practices.

Department's Response:
The Department is currently, actively pursuing utilizing the DFS established payment card services contract. However, the current contract will need to be revised to accommodate the Department's needs. This is presently still in the negotiations phase. If negotiations are not successful, any alternative contract will include provisions required by State law and will be reflective of current business practices. The Department has already obtained approvals from DFS and the Council on Efficient Government (CEG) to outsource this function to an independent contractor. If we are not able to utilize the current DFS established payment card services contract, the Department will issue a Request for Proposal (RFP) for such services.