



OFFICE OF INSPECTOR GENERAL

FLORIDA DEPARTMENT OF TRANSPORTATION

605 Suwannee Street • Tallahassee, FL 32399-0450
(850) 410-5800 • www.dot.state.fl.us/inspectorgeneral

Robert E. Clift,
Inspector General

September 18, 2013

Payment Card Industry Standards Audit Report No. 13P-5001

EXECUTIVE SUMMARY

The purpose of this audit was to conduct an analysis of the department's compliance with the Payment Card Industry (PCI) Data Security Standards (DSS). PCI security standards are technical and operational requirements established by the PCI Security Standards Council to protect payment cardholder data. Department offices that process, store or transmit payment card information are required as a condition of each brand's payment card acceptance agreement to report PCI compliance to the PCI Security Standards Council. During FY 2011-2012, the department processed 33,316,146 payment card transactions for a total of \$735,030,822 in revenue of which toll revenue represents 99.9 percent of the total dollar volume.

In order to evaluate the department's compliance with the PCI DSS, we reviewed the assessments submitted to the PCI Security Standards Council on behalf of the department. Additionally, we reviewed external guidance related to PCI DSS, reviewed prior year audit findings, interviewed employees and managers who handle cardholder data, conducted site visits to evaluate PCI-related operations within the department and evaluated the department's payment card security awareness program.

Based on the work performed, we determined department offices that accept payment by credit card (other than the Office of Toll Operations whose program met PCI DSS expectations) needed improvement in the following areas: selection of Self-Assessment Questionnaires (SAQs), electronic processing of cardholder data, protection of stored cardholder data, physical access controls and the payment card security awareness program.

We recommend management within the Maps and Publications Office, the Permits Office, the Contracts Administration Office, the Cashier's Office and the Office of Information Systems (OIS) ensure their compliance with PCI DSS based on each office's payment card data processing, storage or transmission.

Affected areas of the department have concurred with the findings and initiated corrective actions to mitigate risks associated with the engagement findings. Several of the corrective actions have been completed and the Office of Inspector General will continue to follow-up on those initiated for Findings 2 and Findings 5.

TABLE OF CONTENTS

<u>BACKGROUND AND INTRODUCTION</u>	3
<u>RESULTS OF REVIEW</u>	4
<u>FINDINGS AND RECOMMENDATIONS</u>	
Finding 1 – SAQ Selection	6
Finding 2 – Electronic Processing of Cardholder Data	6
Finding 3 – Protection of Physically Stored Cardholder Data	8
Finding 4 – Physical Access Controls	8
Finding 5 – Payment Card Security Awareness Program	10
<u>APPENDIX</u>	
A. Purpose, Scope and Methodology	12
B. Department Compliance with PCI Standards (2012)	13
C. PCI Compliance Levels	14
D. Management Response	17
<u>DISTRIBUTION, PROJECT TEAM AND STATEMENT OF ACCORDANCE</u>	22

BACKGROUND AND INTRODUCTION

In 2004, five global payment card brands (American Express, Discover, MasterCard, Visa, and JCB International) collaborated to form the PCI Security Standards Council. The payment card brands require all entities that store, process or transmit cardholder data, including merchants and service providers, to comply with PCI DSS. As an organization that accepts payment cards, the department is required by the payment card brands to be PCI compliant.

During FY 2011-2012, the department had five offices required to report PCI compliance: the Cashier's Office (Office of Comptroller), the Maps and Publications Office (Support Services), the Permits Office¹ (Office of Maintenance), the Contracts Administration Office (CAO) and the Florida Turnpike Enterprise, Division of Toll Operations (Toll Office). Each of these offices were required to report PCI compliance to the PCI Security Standards Council (PCI SSC) based on their merchant and service provider levels² and the PCI compliance requirements for these levels. The levels range from 1 to 4 for most of the payment card brands, with level 1 merchants and service providers being required to comply with each of the twelve PCI DSS requirements. The Toll Office, which operates the SunPass system, is a Level 1 merchant, and must validate PCI compliance by performing quarterly network scans and using a qualified third-party to perform the annual assessment. The remaining offices are Level 3 and Level 4 merchants, and are responsible for validating compliance with select PCI requirements using Self-Assessment Questionnaires (SAQs). The requirements³ are:

- install and maintain a firewall configuration to protect cardholder data;
- do not use vendor-supplied defaults for system passwords and other security parameters;
- protect stored cardholder data;
- encrypt transmission of cardholder data across open, public networks;
- use and regularly update anti-virus software or programs;
- develop and maintain secure systems and applications;
- restrict logical access to cardholder data by business need-to-know;
- assign unique ID to each person with computer access;
- restrict physical access to cardholder data;
- track and monitor all access to network resources and cardholder data;
- regularly test security systems and processes; and
- maintain a policy that addresses information security for all personnel.

The Cashier's Office provides PCI guidance for and facilitates the reporting of PCI compliance for the department. The office has created Procedure No. 350-080-300, Securing, Transmitting, Depositing, Recording, and Refunding Receipts to outline processes to ensure department compliance with the PCI DSS.

¹ The Permits Office audited is responsible for the Overweight and Over-Dimensional Vehicle Program, not One-Stop Permitting.

² See Appendix C - PCI Compliance Levels

³ The requirements were obtained from PCI SSC Quick Reference Guide published by the PCI Security Standards Council (www.pcisecuritystandards.org).

RESULTS OF REVIEW

PCI Compliance Level 1 - Toll/SunPass

During FY 2011-2012, the Toll Office processed 33,286,222 transactions via the electronic SunPass tolling system. These transactions yielded \$730,567,242 in department revenue.

To comply with PCI standards, the Toll Office has implemented a comprehensive information security and risk management program in order to prevent and detect the exposure of cardholder data via the SunPass system. This program includes well-defined governance using Toll Office policies and procedures, extensive training and certification of the Information Security and Privacy Office staff, funding of third-party quality assurance and testing of the information technology functions related to PCI-related operations and the implementation of physical and logical controls to systems that interact with cardholder data.

According to the PCI Security Standards Council, the transaction volume and the methods used to process, transmit, and store cardholder data, require the Toll Office to perform quarterly network scans and use a qualified third-party to perform the annual PCI DSS assessment.

We reviewed the annual third-party assessment of Toll PCI compliance for FY 2011-2012. This assessment determined the quarterly scans were performed and no network vulnerabilities were identified. Based on our review of the third-party assessment, we determined that no corrective action or monitoring was required for Turnpike/Toll for the 2012 PCI assessment and risk for prior audits findings had been sufficiently mitigated.

PCI Compliance Level 3 & 4 - Other Department Offices

The Cashier's Office, the Maps and Publications Office, the Permits Office and the Contracts Administration Office accept credit card payments for a variety of items (as shown in the table below). During FY 2011-2012, these department offices, along with their third party payment card processors, processed 29,924 payment card transactions for a total of \$4,463,580 in revenue.

Summary of Payment Card Activity (Excluding Tolls Office)			
Office	No. of Transactions	Receipts	Goods/Services
Cashier's FY 11/12	172	\$2,486	NSF payments; signs
Maps & Publications FY 11/12	707	\$26,414	public docs; maps; publications
Permits FY 11/12	28,836	\$4,431,935	oversize/overweight permits
Contracts Administration FY 11/12	209	\$2,745	public docs; bid packages; contracts
Total	29,924	\$4,463,580	

According to the PCI Security Standards Council, the transaction volume and the methods used to process, transmit and store cardholder data require the Cashier's Office, the Maps and Publications Office, the Permits Office and the Contracts Administration Office to complete Self-Assessment Questionnaires (SAQs) to report PCI compliance.

Based on our evaluation of PCI processes within these department offices, we determined improvements were needed in the selection of Self-Assessment Questionnaires (SAQs), electronic processing of cardholder data, protection of stored cardholder data, physical access controls and the payment card security awareness program. These findings and recommendations are described on the following pages and in Appendix C.

FINDINGS AND RECOMMENDATIONS

Audit Finding 1 – Self-Assessment Questionnaire (SAQ) Selection

Though four out of five offices completed the correct SAQ based on their payment card processing, storage and transmission practices, the Permits Office did not submit correct SAQs. The Permits Office practices for handling cardholder data were more risky (refer to Finding 2) and required adherence to additional criteria not included in SAQs A and B; therefore the office did not self-assess their PCI compliance properly. Selecting the correct SAQ each year is necessary to maintain the department's compliance with PCI DSS. Non-compliance with PCI DSS standards could result in financial penalties up to and including revocation of the ability to accept payment cards. Additionally, credit card data could be at risk of exposure if systems are not properly secured.

Moreover, the Office of Maintenance management responsible for reporting PCI compliance for the Permits Office was not aware of this business practice implemented by their service provider (who has been contracted to administer the Permits program for the department).

We recommend the State Structures Maintenance Engineer⁴ continue to work with the Cashier's Office to determine the appropriate SAQ based on the office's payment card processing, storage or transmission. Additionally, we recommend the State Structures Maintenance Engineer implement additional procedures to verify the PCI compliance of their outsourced vendor.

Audit Finding 2 – Electronic Processing of Cardholder Data

Primary Account Numbers (PANs) were processed, transmitted and stored electronically by Permits Office staff by means prohibited in the PCI DSS and department procedure. The processing, transmission and storage of full PANs on computer screens, payment card receipts, faxes or paper reports can result in this data being obtained by unauthorized individuals and used fraudulently.

Since 2008, Permits Office staff used department computers and systems to transmit full PANs over the department's network via electronic fax. This practice resulted in cardholder data also being stored unencrypted on the department's email inbox and email journal. Also, two contractors in the Permits Office were able to view full PANs on the auxiliary website provided by Bank of America. The Office of Maintenance management responsible for reporting PCI compliance for the Permits Office was not aware that unmasked PANs were being transmitted electronically and/or viewed on department computer systems.

⁴ The State Structures Maintenance Engineer oversees the Permits Office management and staff.

PCI DSS requires merchants to mask PANs when displayed, render PANs unreadable anywhere they are and to never transmit unprotected PANs by end user messaging technologies (for example: email, instant messaging, chat, etc.). Additionally, department Procedure No. 350-080-300, Securing, Transmitting, Depositing, Recording, and Refunding Receipts prohibits the following: faxes containing cardholder data being sent or received by the use of an email system, cardholder data being transmitted in an insecure manner; and cardholder data (PAN, payment card type, expiration date, etc.) being stored in any manner on computers or networks.

We recommend the State Structures Maintenance Engineer:

- continue efforts to cease the business practice in the Permits Office in which full PANs were being transmitted within electronic fax; and
- continue efforts to modify contractual language with the third party vendor to require customer PANs on websites be masked according to PCI DSS Requirement 3.3.

We also recommend the Chief Information Officer continue efforts to assess the presence of unmasked cardholder data on the department network email system and email journal and remove this data to prevent it from becoming breached.

Corrective Action Initiated

In response to audit inquiry, the Permits Administrator⁵ contacted Bank of America and requested that Permit Office PANs be truncated. This system modification became effective February 27, 2013.

Additionally, the Permits Office management informed its customers that applications and documents containing cardholder data will be rejected. To protect cardholder data transmitted on the department network, the Permits Office and the Cashier's Office coordinated with the Office of Information Systems to disable the archiving feature in the Permits inbox and limit access to the inbox's previously archived records to two employees responsible for the information.

To provide more consistent oversight of Permits Office staff, the Permits Administrator will conduct quarterly audits similar to the annual PCI audits conducted by the Office of Inspector General.

Additionally, the Office of Information Systems will deploy Microsoft Office 365 department wide by December 2013, which will encrypt email data during transmission and within storage media.

⁵ The Permits Administrator oversees the Permits Office staff and reports to the State Structures Maintenance Engineer.

Audit Finding 3 – Protection of Physically Stored Cardholder Data

Records with unmasked PANs were being physically stored without a business need in the Contracts Administration and Cashier's Offices. Extended storage of PANs which exceeds business needs increases the risk of unauthorized access to cardholder data.

The Contracts Administration Office had original fax order forms and sales receipts containing unmasked PANs. While the original forms and receipts were stored in a locked file cabinet in the Contracts Administration Office, there is no business need to retain full PANs. While the Cashier's Office has not maintained a standard business practice of storing PANs since 2008, the office did store payment records (dated prior to 2008) with unmasked PANs. The records were stored in a file cabinet; however, the Cashier's Office does not have a business need to retain unmasked PANs. Management in both offices believed keeping unmasked PANs in locked file cabinets was sufficient to protect cardholder data.

PCI DSS requires merchants to limit cardholder data storage and retention time unless it is required for business, legal and/or regulatory purposes. Furthermore, department Procedure No. 350-080-300, Securing, Transmitting, Depositing, Recording, and Refunding Receipts requires the following: cardholder data be eradicated once it is no longer needed for business use; cardholder data be cross-cut shredded (not discarded in the trash) once it has met the retention period for the department; and the retention period for payment card information be five fiscal years, provided all applicable audits, if any, have been released.

We recommend the Contracts Administration Manager and the Comptroller ensure PANs are masked on original order forms and receipts and/or securely dispose records that have met the retention period.

Corrective Action Initiated

In response to audit inquiry, the Deputy Comptroller ensured the Cashier's Office disposed of the payment records with the full PANs.

Audit Finding 4 – Physical Access Controls

Physical access controls in some offices were present but not always applied properly in the Permits, Cashier's and Maps and Publications Offices to ensure protection of cardholder data. The more people who have access to cardholder data, the more risk there is that a user's account will be used maliciously. Limiting access to those with a strong business reason for the access helps an organization prevent mishandling of cardholder data through inexperience or malice.

We noted the following during our observation of PCI-related operations:

- Within the Permits Office, employees in the fax room and the accounting room maintained a standard business practice of viewing unmasked payment card data on their computer screens and/or on forms. The doors to the fax room and the accounting room both contained pin codes and signs stating the areas were for authorized personnel; however, the doors to both remained open during the team's site visit. Unauthorized staff were observed entering and leaving the fax room, but not the accounting room.
- Within the temporary location of the Maps and Publications Office, employees occasionally processed or handled cardholder data. The Maps and Publications door, intended to be accessible via a security card, was left open several times while the team was performing the site visit.
- Employees with access to cardholder data from the Permits Office and Maps and Publications were observed not logging off or locking their computers when leaving them unattended.
- The Permits Office maintained a standard business process of storing cardholder data (including the full unmasked primary account number) on authorization forms in an unlocked lateral file cabinet in the unsecured Accounting Office during office hours.
- The access report for the Cashier's Office listed 14 Comptroller employees and 13 additional employees (primarily Support Services employees) with access to this area containing cardholder data.

Management has not set clear parameters for and/or monitored persons who have access to areas containing cardholder data. Additionally, some employees are not properly utilizing the physical controls which are already in place.

PCI DSS require the following: merchants to limit access to system components and cardholder data to only those individuals whose job requires such access; merchants use appropriate facility entry controls to limit and monitor physical access to systems in the cardholder data environment; and merchants physically secure all media, i.e., all paper and electronic media containing cardholder data. Furthermore, department Policy No. 001-325-060, Security and Use of Information Technology Resources requires users to logoff or lock their workstations prior to leaving the work area.

We recommend the following:

- The Document Control Manager and the State Structures Maintenance Engineer continue their efforts to require employees to use the facility entry controls that are currently in place to limit and monitor physical access to systems in the cardholder data environment;
- The Document Control Manager and the State Structures Maintenance Engineer require employees to adhere to Section 7.7 of department Policy No. 001-325-060, Security and Use of Information Technology Resources, which requires employees to lock their computers when unattended; and
- The Deputy Comptroller coordinate with the Office of Support Services to reduce the number of maintenance employees who have access to the Cashier's Office.

Corrective Action Initiated

In response to audit inquiry, the Permits Office management stated the lower leaf of the security door to the accounting room will be locked. In the absence of any authorized personnel, both accounting room door leaves will be locked. The Permits Office management stated all Permits Office computers will be set to automatically lock after a 15 minute period of inactivity, and employees will be instructed to lock their computers when they leave their work stations.

Lastly, the Permits Office management stated payment card data will be stored in a separate locked cabinet marked uniquely to delineate confidentiality for a period of time not to exceed 14 business days or until the information becomes obsolete, whichever comes first.

In response to audit inquiry, the Document Control Manager reminded Maps and Publications employees that all doors are to remain locked and areas should be secured.

In response to audit inquiry, the Deputy Comptroller ensured the Cashier's Office disposed of the payment records with the full PANs which were previously stored in a locked cabinet. Since no cardholder data is being stored in the Cashier's Office, the risk of unauthorized access of this data has been eliminated.

Audit Finding 5 – Payment Card Security Awareness Program

The department's payment card security awareness program did not educate personnel upon hire and at least annually about the PCI DSS and did not require personnel to acknowledge annually that they have read and understood the PCI related policies and procedures. Furthermore, the program did not require communication with the Computer Security Incident Response Team (CSIRT) in the event of a breach. If personnel are not educated about their security responsibilities as well as implemented security safeguards and processes, these controls may become ineffective through errors or intentional actions.

We noted the following during the engagement:

- When interviewed, three employees in the Maps and Publications Office and five contract employees in the Permits Office confirmed they were responsible for cardholder data. However, two of the Maps and Publications employees and three of the Permits contract employees were not aware of or had not read the Comptroller's credit card security awareness bulletins or Procedure No. 350-080-300, Securing, Transmitting, Depositing, Recording, and Refunding Receipts.
- When interviewed, two department employees in the Contracts Administration Office indicated they were responsible for cardholder data; however, one

employee had not read the Comptroller's credit card security awareness bulletins.

- While Section 6.1.1 of the Comptroller's Procedure No. 350-080-300, Securing, Transmitting, Depositing, Recording, and Refunding Receipts addressed the reporting of credit/debit card security incidents, it did not require the department's CSIRT be notified if a cardholder data breach were to occur.
- Department Policy No. 001-325-060, Security and Use of Information Technology Resources, and Procedure No. 325-060-015, Computer Security Incident Response Team (CSIRT), did not address cardholder data security.

Management relied on past distributions and posting of security awareness bulletins to address cardholder data security for department employees and contractors.

PCI DSS requires the following: merchants to establish, publish, maintain and disseminate a security policy that addresses all PCI DSS requirements and includes a review at least once a year and when the environment changes; merchants to implement a formal security awareness program to make all employee and contractor personnel aware of the importance of cardholder data security; merchants to educate personnel upon hire and at least annually of PCI DSS; merchant's personnel to acknowledge at least annually that they have read and understood the cardholder data security policy and procedures; and merchants to implement an incident response plan and be prepared to respond immediately to a system breach.

Furthermore, department Procedure No. 350-080-300, Securing, Transmitting, Depositing, Recording, and Refunding Receipts requires all personnel with access to cardholder data to review the Credit Card Security Awareness Bulletins located on the Cashier's Office website.

We recommend the Comptroller continue efforts to improve the payment card security awareness program by:

- educating personnel upon hiring about the PCI DSS and having them acknowledge at least annually they have read and understood the PCI-related policies and procedures for the department; and
- coordinating with OIS to ensure department policies and procedures address cardholder data security.

Corrective Action Initiated

In response to audit inquiry, the State Structures Maintenance Engineer stated the new contract with the third party vendor will require PCI compliance and routine training.

APPENDIX A – Purpose, Scope and Methodology

The **purpose** of this engagement was to evaluate the department's compliance with PCI DSS to ensure the protection of cardholder data.

The **scope** of the audit included all department offices that handle or process cardholder data for fiscal years 2011-2012.

To meet the objectives, the **methodology** included:

- reviewing policies, procedures, statutes, rules and regulations;
- reviewing PCI DSS version 2.0 guidance and instructions;
- reviewing prior audits;
- reviewing the 2012 third-party assessment of the Toll Office's PCI compliance and monitoring their action plan progression;
- reviewing the SAQs submitted to the PCI Security Standards Council on behalf of the department offices;
- interviewing department employees and managers;
- conducting site visits to evaluate PCI-related operations within the department; and
- evaluating the department's payment card security awareness program.

APPENDIX B – Department Compliance with PCI Standards (2012)

Department Compliance with PCI Standards (2012)					
Criteria*	Toll	Permits	Maps	CAO	Cashier's
1. Install and maintain a firewall configuration to protect cardholder data	Compliant	Not required	Not required	Not required	Not required
2. Do not use vendor-supplied defaults for system passwords and other security parameters	Compliant	Not required	Not required	Not required	Not required
3. Protect stored cardholder data	Compliant	Finding #2	Not required	Finding #3	Finding #3
4. Encrypt transmission of cardholder data across open, public networks	Compliant	Finding #2 ⁶	Not required	Not required	Not required
5. Use and regularly update anti-virus software or programs	Compliant	Not required	Not required	Not required	Not required
6. Develop and maintain secure systems and applications	Compliant	Not required	Not required	Not required	Not required
7. Restrict access to cardholder data by business need to know	Compliant	Finding #4	Finding #4	Not required	Finding #4
8. Assign a unique ID to each person with computer access	Compliant	Not required	Not required	Not required	Not required
9. Restrict physical access to cardholder data	Compliant	Finding #4	Finding #4	Finding #3	Finding #4
10. Track and monitor all access to network resources and cardholder data	Compliant	Not required	Not required	Not required	Not required
11. Regularly test security systems and processes	Compliant	Not required	Not required	Not required	Not required
12. Maintain a policy that addresses information security for all personnel	Compliant	Finding #5	Finding #5	Finding #5	Finding #5

*- The requirements were obtained from PCI SSC Quick Reference Guide published by the PCI Security Standards Council (www.pcisecuritystandards.org).

⁶ The Permits Office had a practice of transmitting PANs over the department's network (not an open network) via electronic fax.

APPENDIX C – PCI Compliance Levels

Level	Payment Brand	Definition	Validation Requirement
1	American Express- Merchant/Service Provider	<ul style="list-style-type: none"> All merchants/service providers processing 2.5 million American Express Card transactions or more per year Any merchant that American Express otherwise deems a Level 1 merchant 	<ul style="list-style-type: none"> Annual Onsite Assessment performed by a Qualified Security Assessor (QSA) Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Discover- Service Provider	<ul style="list-style-type: none"> All service providers processing 300,000 Discover card transactions per year Any service provider that Discover, in its sole discretion, determines should meet the Level 1 compliance validation and reporting requirements 	<ul style="list-style-type: none"> Annual Onsite Assessment performed by a Qualified Security Assessor (QSA) Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Discover- Merchant	<ul style="list-style-type: none"> All merchants processing more than 6 million card transactions annually on the Discover network Any merchant that Discover, in its sole discretion, determines should meet the Level 1 compliance validation and reporting requirements All merchants required by another payment brand or acquirer to validate and report their compliance as a Level 1 merchant 	<ul style="list-style-type: none"> Annual Onsite Assessment performed by a Qualified Security Assessor (QSA) Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Mastercard- Merchant	<ul style="list-style-type: none"> Any merchant that has suffered a hack or an attack that resulted in an account data compromise Any merchant having more than 6 million total combined MasterCard and Maestro transactions annually Any merchant meeting the Level 1 criteria of Visa Any merchant that MasterCard, in its sole discretion, determines should meet the Level 1 merchant requirements to minimize risk to the system 	<ul style="list-style-type: none"> Annual Onsite Assessment performed by a Qualified Security Assessor (QSA) Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Mastercard- Service Provider	<ul style="list-style-type: none"> All Third Party Processors (TPPs) All Data Storage Entities (DSEs) with more than 300,000 total combined MasterCard and Maestro transactions annually 	<ul style="list-style-type: none"> Annual Onsite Assessment performed by a Qualified Security Assessor (QSA) Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Visa- Merchant	Merchants processing over 6 million Visa transactions annually	<ul style="list-style-type: none"> Annual Onsite Assessment performed by a Qualified Security Assessor (QSA) Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)

*Office of Inspector General
Florida Department of Transportation*

	Visa- Service Provider	VisaNet processors or any service provider that stores, processes and/or transmits over 300,000 Visa transactions annually	<ul style="list-style-type: none"> Annual Onsite Assessment performed by a Qualified Security Assessor (QSA) Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
Level	Payment Brand	Definition	Validation Requirement
2	American Express-Merchant/Service Provider	All merchants/service providers processing 50,000 to 2.5 million American Express Card transactions per year	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Discover-Service Provider	All service providers that store, process, and/or transmit less than 300,000 Discover card transactions per year	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Discover- Merchant	All merchants processing between 1 million and 6 million card transactions annually on the Discover network	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Mastercard- Merchant	<ul style="list-style-type: none"> All merchants/service providers with more than 1 million to 6 million total combined MasterCard and Maestro transactions annually Any merchant meeting the Level 2 criteria of Visa 	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Onsite Assessment performed by a Qualified Security Assessor (QSA) at Merchant Discretion Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Mastercard- Service Provider	All Data Storage Entities with 300,000 or less total combined MasterCard and Maestro annual transactions annually	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Visa- Merchant	All merchants processing 1 million to 6 million Visa transactions annually	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Visa- Service Provider	Any service provider that stores, processes and/or transmits less than 300,000 Visa transactions annually	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
Level	Payment Brand	Definition	Validation Requirement
3	American Express-Merchant/Service Provider	All merchants/service providers who process less than 50,000 American Express Card transactions per year	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Discover- Merchant	All merchants processing between 20,000 and 1 million card-not-present only transactions annually on the Discover network	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Discover- Service Provider	There is no level 3 for Discover Service Providers	There is no level 3 for Discover Service Providers
	Mastercard- Merchant	<ul style="list-style-type: none"> All merchants with more than 20,000 combined MasterCard and Maestro e-commerce transactions annually but less than or equal to one million total combined MasterCard and Maestro e-commerce transactions annually 	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)

*Office of Inspector General
Florida Department of Transportation*

		<ul style="list-style-type: none"> Any merchant meeting the Level 3 criteria of Visa 	
	Mastercard- Service Provider	There is no level 3 for Mastercard Service Providers	There is no level 3 for Mastercard Service Providers
	Visa- Merchant	All merchants processing 20,000 to 1 million Visa transactions annually	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Visa- Service Provider	There is no level 4 for Visa Service Providers	There is no level 4 for Visa Service Providers
Level	Payment Brand	Definition	Validation Requirement
4	American Express- Merchant/Service Provider	There is no level 4 for American Express Merchants/Service Providers	There is no level 4 for American Express Merchants/Service Providers
	Discover- Merchant	All other merchants who do not meet the criteria for Levels 1 through 3	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Discover- Service Provider	There is no level 4 for Discover Service Providers	There is no level 4 for Discover Service Providers
	Mastercard- Merchant	All other merchants who do not meet the criteria for Levels 1 through 3	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Vulnerability Scans performed by an Approved Scanning Vendor (ASV)
	Mastercard- Service Provider	There is no level 4 for Mastercard Service Providers	There is no level 4 for Mastercard Service Providers
	Visa- Merchant	All merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	<ul style="list-style-type: none"> Annual Self-Assessment Questionnaire Quarterly Network Scan by Approved Scan Vendor (ASV) if applicable Compliance validation requirements set by acquirer
	Visa- Service Provider	There is no level 4 for Visa Service Providers	There is no level 4 for Visa Service Providers

APPENDIX D – Management Response

In response to audit inquiry, Jeff Pouliotte, State Structures Maintenance Engineer, submitted the following response via email on behalf of the Permits Office on August 2, 2013:

Finding 1 – Self-Assessment Questionnaire (SAQ) Selection

Response and Corrective Action (to address finding): The findings indicated are accurate, corrective actions have been implemented, and are being monitored for compliance quarterly. The Permit Office has ceased its electronic payment card processing, storage and transmission practices.

Finding 2 – Electronic Processing of Cardholder Data

Response and Corrective Action (to address finding): The findings indicated are accurate, corrective actions have been implemented, and are being monitored for compliance quarterly. In response to audit inquiry, the Permits Administrator⁷ contacted Bank of America and requested that PANs be truncated. This system modification became effective February 27, 2013.

Additionally, the Permits Office management informed its customers that applications and documents containing cardholder data will be rejected. To protect cardholder data transmitted on the department network, the Permits Office and the Cashier's Office coordinated with the Office of Information Systems to disable the archiving feature in the Permits inbox and limit access to the inbox's previously archived records to two employees responsible for the information.

To provide more consistent oversight of Permits Office staff, the Permits Administrator will conduct quarterly audits similar to the annual PCI audits conducted by the Office of Inspector General.

Finding 4 – Physical Access Controls

Response and Corrective Action (to address finding): The findings indicated are accurate, corrective actions have been implemented, and are being monitored for compliance quarterly. In response to audit inquiry, the Permits Office management stated the lower leaf of the security door to the accounting room will be locked. In the absence of any authorized personnel, both accounting room door leaves will be locked. The Permits Office management stated all Permits Office computers will be set to automatically lock after a 15

⁷ The Permits Administrator oversees the Permits Office staff and reports to the State Structures Maintenance Engineer.

minute period of inactivity, and employees will be instructed to lock their computers when they leave their work stations.

Lastly, the Permits Office management stated payment card data will be stored in a separate locked cabinet marked uniquely to delineate confidentiality for a period of time not to exceed 14 business days or until the information becomes obsolete, whichever comes first.

In response to audit inquiry, Joe Kowalski, Deputy Comptroller, submitted the following response via email on behalf of the Cashier's Office on August 26, 2013:

Finding 3 – Protection of Physically Stored Cardholder Data

Response and Corrective Action (to address finding): The pre-2009 records containing PANs have been securely disposed. In 2009, a process was put in place by the Cashier's Office to mask PANs. This process will continue. In response to audit inquiry, the Cashier's Office disposed of the payment records with the full PANs.

Finding 4 – Physical Access Controls

Response and Corrective Action (to address finding): The Cashier's Office has disposed of the payment records with the full PANs which were previously stored in a locked cabinet. Therefore, no cardholder data is being stored in a manner which can be accessed by employees without a need-to-know. The risk of unauthorized access has been eliminated. In response to audit inquiry, the Cashiers Office disposed of the payment records with the full PANs which were previously stored in a locked cabinet. Therefore, no cardholder data is being stored in a manner which can be accessed by employees without a need-to-know.

Finding 5 – Payment Card Security Awareness Program

Response and Corrective Action (to address finding): We concur. *We will continue efforts to improve* the payment card security awareness program by educating personnel upon hiring about the PCI DSS and having them acknowledge at least annually they have read and understood the PCI-related policies and procedures for the department. Also, we have added the requirement for notification of the CSIRT in the PCI-related procedure in the event of a breach.

In response to audit inquiry, Juanita Moore, Contracts Administration Manager, submitted the following response via email on behalf of the Contract Administration Office on August 8, 2013:

Finding 3 – Protection of Physically Stored Cardholder Data

Response and Corrective Action (to address finding): All original order forms that have met the retention period have now been destroyed. The Contracts Administration Office no longer requires payment for orders. Thus, this issue will not be applicable in the future.

In response to audit inquiry, Ron James, Document Control Manager, submitted the following response via email on behalf of the Maps and Publications Office on July 31, 2013:

Finding 4 – Physical Access Controls

Response (to finding): Below are the contents of the email message sent to the entire Document Control staff on 01/03/2013, regarding the audit findings.

From: James, Ron
Sent: Thursday, January 03, 2013 8:51 AM
To: DuBose, Destin
Cc: Whitehead, Huey; Crum, Katifani
Subject: RE: PCI potential findings - Maps and Publications Office

Good morning all,
I have met with the entire Document Control team which includes Maps and Publication as well as Records Retention, regarding results from last week's walk-through. The subject of our meeting was the importance of maintaining a secure environment when handling material of such a sensitive nature. I will also forward to you an earlier email message reminding the staff that all doors are to remain locked and the area secured.

Ron James
Document Control Manager
Printing/Reprographics Administrator
ph. (850) 414-4427
fax (850) 414-4948

Another topic of discussion at the above meeting was the importance of the Document Control staff locking computer screens while away from their respective workstations.

Below is an earlier email that was sent to the Document Control staff on 12/07/2012 addressing security risks created by open and unlocked doors.

From: James, Ron
Sent: Friday, December 07, 2012 3:26 PM
To: Whitehead, Huey; Ponds, Amelia; Davis, Steve; Richardson, Shakaël; Thompson, Charles; MacWhite, Lucille
Subject: Door adjacent to stairwell

Good afternoon all,
Friday afternoon a former Document Control employee re-entered the building (via the door adjacent to the stairwell)and entered the Document Control area without anyone noticing. This presents a potential security risk, that I do not want any of us to take for granted. Therefore I am issuing a directive that this door is to remain closed at all times. Anyone not authorized to be in the building will be required to ring the bell for entry, so remember to have your key card with you at all times. This way we can all help police the area and be able to recognize anything that is out of the ordinary. I'm open to input and suggestions so shoot me an email, stop me in the hallway or drop by my office with any questions or concerns.

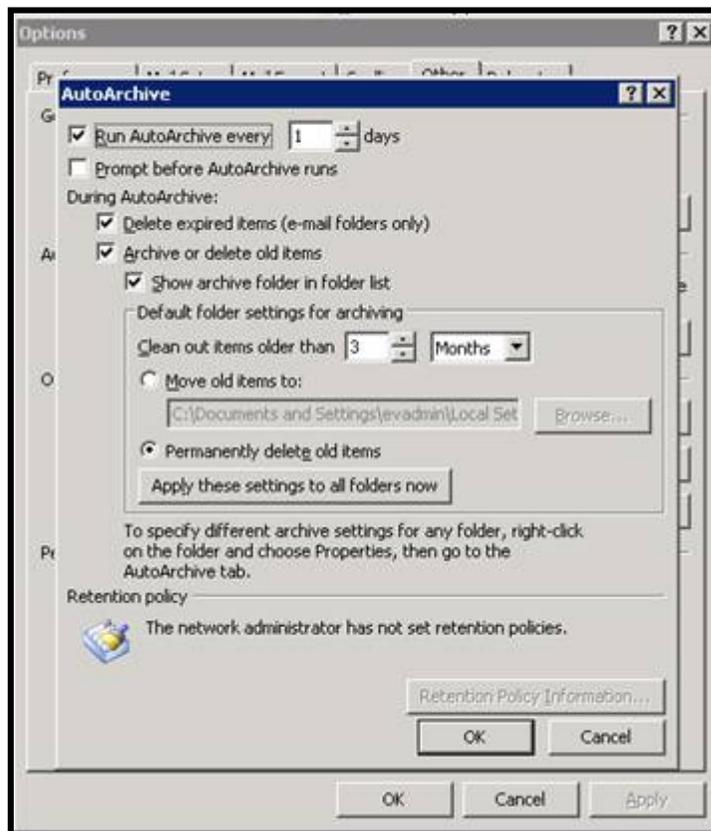
Ron James
Document Control Manager
Printing/Reprographics Administrator
ph. (850) 414-4427
fax (850) 414-4948

Corrective Action (to address finding): In response to audit inquiry, the Document Control Manager reminded Maps and Publications employees that all doors are to remain locked and areas should be secured.

In response to audit inquiry, Joseph Veretto, OIS Management Consultant Supervisor, submitted the following response via email on behalf of the Office of Information Systems on August 26, 2013:

Finding 2 – Electronic Processing of Cardholder Data

Response (to finding): To mitigate the risk of maintaining PAN information within the Department's e-mail system, the Office of Information Systems has set the Permit Office's mailbox archive options to delete archives over three months old from all folders. This process shall assure that any PAN information that may have been sent via e-mail is deleted from personal archives.



Access to the Department's Journal archive is limited to a small number of Central Office employees charged with supporting and maintaining the enterprise messaging archive environment. This archive is maintained for five years, upon which time archives are automatically deleted. During discussions with the Office of Inspector General and the Permits Office, it was determined that there are sufficient mitigating risk factors in place to prevent unauthorized disclosure of any PAN information that may be contained within the Department's Outlook Journal Archive. Mitigating controls include limited number of Central Office OIS personnel with access to the Journal, and documented processes for redacting confidential and exempt information when responding to public records requests. Additionally, with the upgrade to the Office 365, e-mail shall be encrypted during transmission and within storage media, effectively encrypting any PAN information that may reside within the Journal.

Corrective Action (to address finding): The Office of Information Systems will deploy Microsoft Office 365 department wide by December 2013, which will encrypt email data during transmission and within storage media.

DISTRIBUTION, PROJECT TEAM AND STATEMENT OF ACCORDANCE

Action Official Distribution:

Brian Peters, Assistant Secretary of Finance and Administration
Robin Naitove, Comptroller
Joe Kowalski, Deputy Comptroller
Wilson Dilmore, Manager of the Technology Services and Support Office
April Blackburn, Manager of the Business Systems Support Office
Howard Jemison, Manager of Support Services Office
Ron James, Document Control Manager
Diane Guittierez-Scaccetti, Director of Turnpike Enterprise
Reginald Hardee, Information Systems Manager for Turnpike Enterprise
Brian Blanchard P.E., Assistant Secretary Engineering and Operations
Tom Byron P.E., Chief Engineer
Tim Lattner P.E., Director of Office of Maintenance
Jeff Pouliotte P.E., State Structures Maintenance Engineer
Dave Sadler P.E., Director of the Office of Construction
Juanita Moore, Manager of Contracts Administration Office

Information Distribution:

Ananth Prasad, P.E., Secretary of Transportation
Jim Boxold, Chief of Staff

Project Team:

Engagement was conducted by:
Katifani Crum, Auditor in Charge; and
Destin DuBose, Auditor
Under the supervision of:
Joe Gilboy, Audit Manager; and
Kristofer B. Sullivan, Director of Audit
Approved by: Robert E. Clift, Inspector General

Statement of Accordance

The mission of the department is to provide a safe transportation system that ensures the mobility of people and goods, enhances economic prosperity, and preserves the quality of our environment and communities.

The mission of the Office of Inspector General is to promote integrity, accountability and process improvement in the Department of Transportation by providing objective fact-based assessments to the DOT team.

This work product was prepared pursuant to Section 20.055, Florida Statutes, in accordance with the applicable Principles and Standards for Offices of Inspectors General as published by the Association of Inspectors General; the International Standards for the Professional Practice of Internal Auditing as published by the Institute of Internal Auditors; and the American Institute of Certified Public Accountants and standards contained in Government Auditing Standards issued by the Comptroller General of the United States.

This report is intended for the use of the agency to which it was disseminated and may contain information that is exempt from disclosure under applicable law. Do not release without prior coordination with the Office of Inspector General.

Please address inquiries regarding this report to the department's Office of Inspector General at (850) 410-5800.