Payment Card Industry Data Security Standards Statewide Compliance

FY2012 Request: **$2,000,000**
Reference No: **51568**

AP/AL: Appropriation

Project Type: Information Technology / Systems / Communication

Category: General Government

Location: Statewide

House District: Statewide (HD 1-40)

Impact House District: Statewide (HD 1-40)

Contact: Ginger Blaisdell

Estimated Project Dates: 07/01/2011 - 06/30/2016

Contact Phone: (907)465-2312

Brief Summary and Statement of Need:
Payment Card Industry Data Security Standard (PCI DSS) Compliance is a mandatory requirement for all transactions involving credit card vendors, online merchants and service providers. The State of Alaska is considered a single merchant and the compliance of any single department reflects the state as a whole. This project reflects the costs to bring all State of Alaska departments that are currently accepting credit card payments into compliance.

Funding:	FY2012	FY2013	FY2014	FY2015	FY2016	FY2017	Total
Gen Fund	$2,000,000						$2,000,000
Total:	$2,000,000	$0	$0	$0	$0	$0	$2,000,000

☐ State Match Required ☑ One-Time Project ☐ Phased - new ☐ Phased - underway ☐ On-Going
0% = Minimum State Match % Required ☐ Amendment ☐ Mental Health Bill

Operating & Maintenance Costs:

	Amount	Staff
Project Development:	0	0
Ongoing Operating:	0	0
One-Time Startup:	0	
Totals:	0	0

Additional Information / Prior Funding History:

Project Description/Justification:
Payment Card Industry Data Security Standard (PCI DSS) Compliance is a mandatory requirement for all transactions involving credit card vendors, online merchants and service providers. The State of Alaska is considered a single merchant and the compliance of any single department reflects the state as a whole.

A PCI compliance review was conducted by Coalfire Systems, Inc., through a contract managed by Enterprise Technology Services (ETS). This review was conducted to identify non-compliant issues regarding credit card payment acceptance, focusing on the security of that sensitive data. Concluding this review all agencies were supplied a remediation roadmap detailing PCI requirements, testing procedures, gaps, and remediation needs.

This project charter reflects the costs to bring all State of Alaska departments that are currently accepting credit card payments in compliance as identified in the Coalfire audit with PCI DSS standards within one year. The cost of this project is based on a compilation of estimates from nine departments (Department of Public Safety, Department of Transportation & Public Facilities, Department of Environmental Conservation, Department of Commerce, Community & Economic

Development, Department of Natural Resources, Department of Fish & Game, Department of Administration, Department of Health & Social Services, and Lt. Governor) that were determined by Coalfire to be PCI non-compliant. These estimates were determined without central direction to standard solutions and policies.

The project cost compiled from the departments is estimated to be $4.0 million in the first year of the project, however this amount may be low based on the wide variance of estimates from departments and lack of experience with compliance costs. Ongoing cost to remain compliant will be approximately $450,000 for the next four years.

The PCI DSS, a set of comprehensive requirements for enhancing payment account data security, was developed by the founding payment brands of the PCI Security Standards Council, including American Express, Discover Financial Services, JCB International, MasterCard Worldwide and Visa Inc., to help facilitate the broad adoption of consistent data security measures on a global basis.

The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures. This comprehensive standard is intended to help organizations proactively protect customer account data.

The core of the PCI DSS is a group of principles and accompanying requirements, around which the specific elements of the DSS are organized:

Build and Maintain a Secure Network

Requirement 1: Install and maintain a firewall configuration to protect cardholder data
Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect Cardholder Data

Requirement 3: Protect stored cardholder data
Requirement 4: Encrypt transmission of cardholder data across open, public networks

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software
Requirement 6: Develop and maintain secure systems and applications

Implement Strong Access Control Measures

Requirement 7: Restrict access to cardholder data by business need-to-know
Requirement 8: Assign a unique ID to each person with computer access
Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

Requirement 10: Track and monitor all access to network resources and cardholder data
Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

In Scope

1. All State of Alaska departments and agencies processing credit cards under the state credit card contract.
2. Payment Card Industry compliance is mandated in order to process credit cards.
3. The government of the State of Alaska is considered a single merchant and the compliance of any single department reflects as the government of the State of Alaska as a whole.
4. Cost involved for departments who accept credit cards or plan to accept credit cards or departments with access to PCI data to become PCI DSS compliant
5. Security and risk training for all state employees involved in credit card processing
6. Cost involved for departments to modify program and services based on a new Credit card servicer.

Out of Scope

1. All State of Alaska departments that do not accept or do not plan to accept credit cards under the state credit card contract or departments without access to credit card data are out of scope.
2. Security policies and procedures not mandated by PCI DSS.
3. Changes to programs, policy or procedures not mandate by PCI DSS.
4. Changes to programs, policy or procedures not mandate by changes in the credit card servicer.

Project Goals and Objectives

1. An initial contract to determine centrally managed policies, procedures and processes that could be implemented in order to provide cost saving and consistency across State of Alaska departments in order to be PCI DSS compliant.
2. All departments of the State of Alaska that accept credit cards or plan to accept credit cards or have access to PCI data to become PCI DSS compliant in an economical and efficient manner.
3. All departments of the State of Alaska that process credit cards to modify programs and processes to work with a new credit card servicer without disruption to credit card processing.