LEGISLATIVE AUDIT DIVISION

Angus Maciver, Legislative Auditor
Deborah F. Butler, Legal Counsel

Deputy Legislative Auditors:
Cindy Jorgenson
Joe Murray

MEMORANDUM

TO:	Legislative Audit Committee Members
FROM:	Alyssa Sorenson, Performance Auditor
CC:	Sheila Hogan, Director, Department of Administration Mike Manion, Deputy Director, Department of Administration Ron Baldwin, Chief Information Officer
DATE:	September 2016
RE:	Performance Audit Follow-Up (17SP-03): Bankcard Transaction Fees and Contract Management (orig. 14P-04)
ATTACHMENTS:	Original Performance Audit Summary

Introduction

The Bankcard Transaction Fees and Contract Management report was issued to the Legislative Audit Committee in June 2015. The audit included three recommendations to the Department of Administration (DOA). In August 2016, we conducted follow-up work to assess implementation of the report recommendations. This memorandum summarizes the results of our follow-up work.

Overview

Audit work determined DOA could improve contract monitoring to better ensure the accuracy and security of point-of-sale and online bankcard transactions. Our performance audit included three recommendations to DOA regarding the review of independent security compliance audits, developing processes to assist agencies to resolve contractor disputes and monitor statewide fee data, and developing follow-up processes for addressing contractor security weaknesses. DOA concurred with all three recommendations. Based on our follow-up work, DOA has implemented two recommendations and is in the process of implementing one

Background

Citizens are increasingly using credit and debit cards to purchase goods and services from state agencies. The DOA manages two term contracts to facilitate the processing of payments made through online and point-of-sale systems. These state-wide contracts are in place for a fixed period of time to allow agencies to develop payment processing programs with the contractors without issuing individual requests for proposals. One contract processes point-of-sale payments that are completed by customers at state agencies and universities. The other contract is required for payments that are processed online and is used by state agencies and the University of Montana. Montana State University uses a different contract to process online payments.

In fiscal year 2013 there were nearly 1.1 million transactions totaling over $115 million processed using point-of-sale systems. Transaction fees for this contract totaled nearly $2.2 million. There were approximately 6 million online transactions totaling $209 million processed during calendar year 2013. Audit work estimates online transactions fees totaled over $11.5 million.

Audit Follow-up Results

Our performance audit report recommended three improvements DOA could make to manage the two term contracts. As part of our follow-up work, we interviewed DOA staff and agency staff using the contract, examined documentation regarding updated monitoring processes, and viewed updated contract policy.

RECOMMENDATION #1

We recommend the Department of Administration enforce contract provisions by receiving and reviewing the service organization review and documentation of Payment Card Industry Data Security Standards compliance annually to verify the contractor's compliance with security requirements.

Implementation Status – Implemented

The audit found that contract provisions requiring the contractor to provide reports on compliance to security standards to the department were not enforced by the contract manager. DOA should receive and review these reports to ensure contractors meet established security requirements. Follow-up work found that the department now annually requests and receives copies of the Pay Card Industry Data Security Standards (PCI DSS) compliance report and sends them to specialized staff for review. PCI DSS compliance reports for fiscal year 2015 were received from both contractors in September of 2015. A copy of the audit is kept by the contract manager with a record of the date of receipt. Currently, DOA does not document the results of the review. At the time of the follow-up, they indicated that they plan to do so in the future, which would further strengthen the review process. The previous year's reports indicate that both contractors were in compliance with industry security standards. The contract manager will request fiscal year 2016 PCI DSS compliance reports this September.

RECOMMENDATION #2

We recommend the Department of Administration improve its management of the contract for online transactions by:

A. **Developing a process to identify payment application issues on an ongoing basis and assist agencies with resolving problems.**

B. **Developing a process for receiving and analyzing statewide transaction fee and convenience fee data.**

Implementation Status – Being Implemented

The audit discovered that agency issues after payment application implementation were not identified or resolved by DOA, and that neither the online transaction contractor nor DOA could identify the amount of online bankcard fees charged statewide. Since the audit's completion, DOA has established a process to help agencies resolve contractor payment application issues and is developing a process to receive and analyze statewide bankcard fee data.

The issue resolution process appears to be making progress on solving long-standing problems between agencies and the contractor. In order to identify issues, the contract manager participates in an eGovernment Managers' Group with state-wide department representatives, meets weekly with the

contractor, and reviews documentation of project status updates at least monthly. The contract manager depends on agency eGovernment Mangers to disseminate information about the dispute resolution process to their department. Once an issue is identified, the contract manager directs the involved agency to a write formal letter detailing their dispute, which the contract manager uses to set up a meeting with the appropriate contractor representative. Any commitments made in the meeting must be documented by each side and followed up with a written status report for each item. Follow-up work examined written documentation of one of the two issues that have been addressed in this way in 2016, and interviewed agency staff involved in the dispute. The agency staff indicated that the process helped bring longstanding issues to the attention of senior contractor management and progress has been made on some issues. Prevailing issues, however, were recently submitted to the contract manager in a new formal letter to restart the complaint resolution process. In particular, the agency, DOA, and the contractor are currently trying to resolve issues regarding reconciliation of reimbursements with the contractor. Overall, progress has been made by DOA in addressing agency-contractor issues, though their process could be supplemented by establishing policy or written guidance to assist agencies in filing complaints.

To analyze statewide bankcard fee data, DOA staff is currently working with the contractor to create a new annual report that includes the number of transactions conducted by category. The information currently provided in the annual financial report, such as revenue collected, revenue remitted to the state, and transaction costs, will be used by staff to calculate average convenience fees statewide. The categories to be included in the report are still under negotiation, but may include by agency or type. Staff plans to use this information to analyze high level information to spot trends and identify potential agency level concerns. The report should be complete by the end of the year.

RECOMMENDATION #3

We recommend the Department of Administration develop a follow-up process on actions to be taken when contractor weaknesses or deficiencies are identified during the assessment of security controls.

Implementation Status –Implemented

Following up on security vulnerabilities of contractor servers and applications on the state network was identified in the audit as necessary to maintain citizens' data security. To address this concern, DOA conducts and reviews network scans annually, before application launch, and when notified of system updates. Identified security issues are detailed in a Security Audit Form. The contractor would be notified immediately of any problems discovered, and a date by which they must fix the issue. The form is used to determine if the issue is a security incident or a gap. If it is a security incident, such as a network vulnerability, an incident case is created in the bureau's Point of Business System to track, delegate, and record the incident to resolution. If it is a gap in the system or in the process, it is entered into the Gap Analysis/Plan of Action and Milestones Spreadsheet to track, delegate, and record. Once the contractor indicates the problem has been fixed, DOA conducts a follow up scan to ensure the actions taken solved the problem without creating new vulnerabilities. Though DOA does not require the contractor provide a corrective action plan as to how they will solve the problem, they do have their own internal process in place to ensure the issue is ultimately resolved.

In addition to these processes, DOA has also increased its ability to monitor security issues by allowing the contractor to conduct their own security scans. In concurrence, they approved a contract amendment that requires the contractor to notify DOA twenty-four hours in advance of conducting scans and require a copy of the scan results be supplied to DOA. If issues are noted in these scans, they will be tracked to resolution the same way DOA identified issues would be tracked.