LEGISLATIVE AUDIT DIVISION

Tori Hunthausen, Legislative Auditor
Monica Huyg, Legal Counsel

Deputy Legislative Auditors:
James Gillett
Angie Grove

MEMORANDUM

TO: Legislative Audit Committee Members

FROM: Kent Rice, Information Systems Audit Manager

DATE: September 2010

CC: George Dennison, President, The University of Montana – Missoula
Waded Cruzado, President, Montana State University
Dr. Ronald Sexton, Chancellor, Montana State University – Billings
Jim Lynch, Director, Department of Transportation

RE: Follow-up IS Audit (10SP-28):
Payment Card Industry Data Security Standard and Related Controls (09DP-02)
The University of Montana – Missoula
Montana State University
Montana State University – Billings
Department of Transportation

INTRODUCTION

We presented our Information Systems audit on the Payment Card Industry Data Security Standard (PCI DSS) and Related Controls to the Legislative Audit Committee in June 2009. The report contains two recommendations relating to:

- Development and implementation of policies to define requirements and increase awareness.
- Ensuring existing devices meet requirements of the PCI DSS.

We requested and received information from The University of Montana – Missoula (UM), Montana State University (MSU), Montana State University – Billings (MSUB), and Department of Transportation (MDT) personnel regarding progress toward implementation of the report recommendations. This memorandum summarizes their responses and our follow-up work.

BACKGROUND

Cardholder data security has become a priority for the major payment card brands leading them to create their own association to establish and regulate security standards. The PCI DSS addresses security concerns by requiring agencies to develop policies and implement business processes to handle payment cardholder data in a secure manner. The State of Montana has entered into a term contract with a third party vendor to provide credit card approvals and provide equipment for card processing. Any agency using the state contract for credit card processing services is required by the contract to follow the provisions contained within the PCI DSS.

FOLLOW-UP DISCUSSION

The following sections summarize the report recommendations, and the progress towards implementing the recommendations.

Processing and Storage of Cardholder Data

Many of the requirements of the PCI DSS address processing and storage of cardholder data. Agencies must process payment card transactions in a secure manner. If a merchant requires any cardholder data be retained, it must be stored in a manner that allows access by authorized personnel only.

Our audit selected specific PCI DSS elements for review based on the business processes in place at UM, MSU, MSUB, and MDT (referred to collectively as agencies for the remainder of this memorandum). The audit determined agency policy and business processes did not conform to these specific elements of the PCI DSS related to the processing and storage of cardholder data for the following reasons:

- Policy regarding the handling of payment cardholder information either did not exist or did not completely address requirements.
- Sensitive authentication data was being stored after authorization.
- Access to cardholder data was not being limited effectively to those with a business need to know, and overall physical access to stored cardholder data was not properly restricted.
- Lists of all point of sale devices in use were either not kept or were incomplete.

Recommendation #1

We recommend the four agencies comply with the contract by:

A. Developing and implementing specific payment card data security policies which include:
- **Cardholder data retention**
- **Storage of sensitive authentication data**
- **Securing (masking) primary account numbers**
- **Restricting access to cardholder data**
- **Completing and tracking an inventory of all point of sale devices**

B. Formally communicating specific payment card data security policies to staff to increase awareness at the departmental level.

C. Formally monitoring the implementation of payment card data security policies.

A. Implementation Status: Being Implemented

Two of the four agencies have fully implemented this recommendation and two are currently in the process of implementing it. We reviewed the new policies for cardholder data in place at each of the four agencies for each of the elements above. Two agencies addressed each of the specific areas of concern as well as specifically incorporating the PCI DSS as the security standard for cardholder data. The other two agencies have developed new policies or modified existing policies. However, these policies did not fully address the areas of concern from our audit, so the agencies are in the process of addressing those concerns.

B. Implementation Status: Being Implemented

All four agencies have notified key credit card processing staff of changes to policies and procedures. Notification occurs via training and formal notices such as policy announcements to staff. Two of the four agencies have not trained all necessary staff at this time. However, both agencies plan to conduct annual training to ensure that all current and new staff are trained in properly handling credit cardholder information.

C. Implementation Status: Being Implemented

Each of the four agencies is developing procedures to formally monitor the implementation of new credit card handling procedures and policies. Some procedures are more developed than others. However, none of the agencies have completed monitoring to date.

Point of Sale (POS) Security

With the exception of transactions carried out through agency websites, the majority of payment card transactions are carried out using POS devices. Cardholder information is entered into the device either by swiping the card or by hand keying the card information. The data is transmitted to the card processor for authorization. At the time of our audit, we determined each of the four agencies were using POS devices which were not compliant with the PCI DSS due to not encrypting the data during transmission.

Recommendation #2

We recommend the four agencies ensure all point of sale devices encrypt cardholder data as required by the Payment Card Industry Data Security Standard.

Implementation Status: Implemented

Shortly after the completion of our audit the state term contract for payment card processing services was rebid and a new vendor was contracted. A result of the contract was a complete review of all POS devices in use at the four agencies. Any noncompliant POS devices were replaced by the vendor. To verify this, we obtained a list of all POS devices from the four agencies and determined all the noncompliant POS models we identified were replaced with PCI DSS compliant models.

S:\Admin_Restricted\IS\Follow-up\10SP-28-Univ-follow-up-orig-09DP-02.docx/eb