Telephone: (515) 281-5368
Fax: (515) 281-7562

Michael L. Fitzgerald
Treasurer of State
Capitol Building
Des Moines, Iowa 50319-0005

E-Mail: treasurer@max.state.ia.us
Web: www.treasurer.state.ia.us

RECEIVED
NOV 07 2007
DIRECTOR OF REVENUE

November 7, 2007

Mark R. Schuling, Director
Iowa Department of Revenue
Hoover State Office Building
LOCAL

Re: Iowa Technology Governance Board and Payment Card Industry Data Security Standards

Dear Mark:

I am responding to your letter dated October 16, 2007 regarding state agencies that accept credit cards and their compliance with the Payment Card Industry Data Security Standards.

This office was given authority in the Iowa Code to enter into a credit card contract on behalf of state agencies, and we are also given the authority to authorize agencies to accept credit cards. Due to the detailed nature of the PCI-DSS requirements, we do not believe we are able to independently verify that agencies accepting credit cards under our authority are complying with the standards. Each operates its own credit card program in a unique environment; while many agencies use ITE's e-Payment engine, others use different equipment, software, or internet applications to process credit card payments. Even agencies using the e-Payment engine differ in where their websites and related databases are hosted.

Given these complexities, we believe each agency must be responsible for its own compliance with PCI-DSS. Therefore, this office is developing an agreement that each agency accepting credit card payments will be required to sign. In this agreement, the agency must certify that it is PCI-compliant, and agree to assume responsibility for any penalties, fines, and costs that may arise as a result of non-compliance. Agencies that do not sign this agreement will not be authorized to accept credit card payments. We hope to have these agreements in place within a year.

The Treasurer's Office is trying to assist agencies in the compliance process. We sponsored a half-day seminar for agencies in which an expert explained PCI-DSS and why it is important. We have distributed information on websites and conferences where they can learn more about the security standards. In addition, we are hiring a compliance validation firm to assist agencies with the compliance process. This firm will host question and answer sessions with agencies via a series of conference calls. It will conduct monthly system vulnerability scans for those agencies that are required to have them. In addition, the

firm will provide agencies with an online version of the PCI self-assessment questionnaire. Each agency must successfully complete the questionnaire in order to validate compliance. While we hope that this firm will provide most agencies with the assistance they need to become compliant, there may be agencies that require additional help. In that case, it will be the agency's responsibility to seek additional assistance.

At this time, we do not believe any agency accepting credit cards under our authority has properly completed the self-assessment questionnaire, nor has any undergone system vulnerability scans. Unfortunately, we believe that many agencies erroneously assume that once ITE's e-Payment engine is compliant, they will automatically be compliant as well. Hopefully, once we begin working with the compliance validation firm, agencies will better understand their responsibilities in the compliance process.

I would ask that the Board encourage agencies to consolidate in one place the technology associated with accepting credit card payments over the internet. By standardizing where payment websites are hosted and payment data is stored, we can reduce the scope of state systems falling under PCI-DSS. It should then be easier and cheaper for state agencies to become, and stay, compliant.

Please let me know if my staff and I can provide you with any additional information.

Sincerely,

Michael L. Fitzgerald
Treasurer of State

MLF/rmt