OFFICE OF AUDITOR OF STATE
STATE OF IOWA

David A. Vaudt, CPA
Auditor of State

State Capitol Building
Des Moines, Iowa 50319-0004

Telephone (515) 281-5834 Facsimile (515) 242-6134

NEWS RELEASE

FOR RELEASE July 27, 2010

Contact: Andy Nielsen
515/281-5834

Auditor of State David A. Vaudt today released a report on a review of selected general and application controls over the Iowa Department of Transportation's Internal Billing System for the period April 6, 2009 through July 31, 2009.

Vaudt recommended the Department establish additional security policies and implement change control procedures to ensure activity is monitored and program changes are approved before they are placed into production.

A copy of the report is available for review at the Iowa Department of Transportation, in the Office of Auditor of State and on the Auditor of State's web site at http://auditor.iowa.gov/reports/1060-6450-BT01.pdf

# # #

REPORT OF RECOMMENDATIONS TO THE IOWA DEPARTMENT OF TRANSPORTATION ON A REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE INTERNAL BILLING SYSTEM

April 6, 2009 THROUGH JULY 31, 2009

Office of

AUDITOR OF STATE

State Capitol Building • Des Moines, Iowa

David A. Vaudt, CPA
Auditor of State

OFFICE OF AUDITOR OF STATE
STATE OF IOWA

David A. Vaudt, CPA
Auditor of State

State Capitol Building
Des Moines, Iowa 50319-0004

Telephone (515) 281-5834 Facsimile (515) 242-6134

June 18, 2010

To Nancy J. Richardson, Director of the
Iowa Department of Transportation:

In conjunction with our audit of the financial statements of the State of Iowa for the year ended June 30, 2009, we conducted an information technology review of selected general and application controls of the Iowa Department of Transportation for the period April 6, 2009 through July 31, 2009. Our review focused on the general and application controls of the Iowa Department of Transportation's Internal Billing System as they relate to our audit of the financial statements. The review was more limited than would be necessary to give an opinion on internal controls. Accordingly, we do not express an opinion on internal controls or ensure all deficiencies in internal controls are disclosed.

In conducting our review, we became aware of certain aspects concerning information technology controls for which we believe corrective action is necessary. As a result, we have developed recommendations which are reported on the following pages. We believe you should be aware of these recommendations which pertain to the Department's general and application controls over the Internal Billing System. These recommendations have been discussed with Department personnel and their responses to these recommendations are included in this report. While we have expressed our conclusions on the Department's responses, we did not audit the Department's responses and, accordingly, we express no opinion on them.

This report, a public record by law, is intended solely for the information and use of the officials and employees of the Iowa Department of Transportation, citizens of the State of Iowa and other parties to whom the Iowa Department of Transportation may report. This report is not intended to be and should not be used by anyone other than these specified parties.

We would like to acknowledge the many courtesies and assistance extended to us by personnel of the Iowa Department of Transportation during the course of our review. Should you have questions concerning any of the above matters, we shall be pleased to discuss them with you at your convenience. Individuals who participated in our review of the Internal Billing System are listed on page 8 and they are available to discuss these matters with you.

David A. Vaudt

DAVID A. VAUDT, CPA
Auditor of State

Warren Jenkins

WARREN G. JENKINS, CPA
Chief Deputy Auditor of State

cc: Honorable Chester J. Culver, Governor
Richard C. Oshlo, Jr., Director, Department of Management
Glen P. Dickinson, Director, Legislative Services Agency

Internal Billing System General and Application Controls

A. Background

The Iowa Department of Transportation's Internal Billing System is used to record equipment, equipment labor, material and supplies, job billings and surcharge expenses between various cost centers within the Department.

B. Scope and Methodology

In conjunction with our audit of the financial statements of the State of Iowa, we reviewed selected aspects of the general and application controls in place over the Iowa Department of Transportation's Internal Billing System for the period April 6, 2009 through July 31, 2009. Specifically, we reviewed the general controls: security program planning and management, access controls, change controls, segregation of duties, service continuity, system software and the application controls: input, processing and output controls. We interviewed staff of the Department and we reviewed Department policies and procedures. To assess the level of compliance with identified controls, we performed selected tests.

We planned and performed our review to adequately assess those Department operations within the scope of our review. We developed an understanding of the Department's internal controls relevant to the operations included in the scope of our review. We believe our review provides a reasonable basis for our recommendations.

We used a risk-based approach when selecting activities to be reviewed. We focused our review efforts on those activities we identified through a preliminary survey as having the greatest probability for needing improvement. Consequently, by design, we used our finite review resources to identify where and how improvements can be made. Thus, we devoted little effort to reviewing operations that may be relatively efficient or effective. As a result, we prepare our review reports on an "exception basis." This report, therefore, highlights those areas needing improvement and does not address activities that may be functioning properly.

C. Results of the Review

As a result of our review, we found certain controls can be strengthened to further ensure the reliability of financial information. Our recommendations, along with the Department's responses, are detailed in the remainder of this report.

General Controls

(1) Security Program Planning and Management – Security Program Planning and Management is the foundation of an entity's security control structure and a reflection of senior management's commitment to addressing security risks. It should be a written and formally adopted framework and should be a continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well designed program, security controls may be inadequate, responsibilities may be unclear, misunderstood, and improperly implemented and controls may be

inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

The Department's security framework utilizes components of well established security controls. To name a few, these components include the adoption of specific IT policies, such as laptop encryption and removable media encryption, the establishment of security management structure, informal security awareness, training and implementation of physical controls, such as firewalls, routers and software to monitor network traffic. However, written policies have not been formally adopted in the following areas:

a. Annual risk assessment and penetration testing policy – A Department policy establishing annual risk assessments and penetration testing is important to help ensure all threats and vulnerabilities are identified and adequately planned for on a timely basis.

b. Entity-wide security plan policy - A Department policy establishing and describing the Department's security program and the policies and procedures supporting it.

c. Background check policy – A Department policy identifying and addressing all IT related positions with access to critical or confidential data where background checks are necessary. Background checks would be conducted as part of the hiring process.

d. Incident response policy – A Department policy outlining potential security risks and procedures for employees to follow in response to those risks.

Recommendation – The Department should establish policies and procedures to include the above items to ensure the security framework is formally adopted, comprehensive and disseminated to all Department employees.

Response–

a. The Department conducts annual IT security risk assessments and penetration tests for vulnerabilities through IT Division procedures. The Department will review and convert these IT Division procedures into departmental policy during FY11. (DOT policy 030.11 Information Resources Security)

b. The Department currently has an Entity-wide Information Resources Security Policy (DOT policy 030.11 Information Resources Security). This policy will be revised in FY11 to include a description of the Department's security program and the policies and procedures that support it.

c. The Department published a policy in January 2010 (DOT policy 210.02 Recruitment/Selection/Hiring Process) which addresses employee background checks.

d. The Department will develop incident response policies for the potential security risks with procedures for employees to follow in responding to those risks.

Conclusion–Response accepted.

(2) Change Control – The establishment of controls over the modification of application programs helps to ensure only authorized programs and authorized modifications are implemented. This can be accomplished by instituting policies and procedures to ensure all programs and program modifications are properly authorized, tested and approved and access to programs is carefully controlled.

Development Service Requests (DSR) are prepared by users whenever a new application, enhancement or modification is needed. The DSR tracks progress and documents user approvals. Additionally, Vault software is used for version control. Activity is logged and supervisors are automatically notified via email when programs are checked back in. The following situations were noted where procedures did not appear to be effectively controlling program modifications:

a. Not all approvals are documented on the DSR's before changes are placed into production. For example, user approval is done verbally, the change is placed into production, then the user formally approves the change.

b. Some applications or programs do not have a person assigned to receive an automated email any time code is changed and placed into production. Two of seven team leaders have not been set up to receive the automated messages.

c. There is currently no review to remove VPN access to the Vault software upon expiration of the business contract for 3rd party programmers.

Recommendation – The Department should establish procedures to ensure program changes are approved before they are placed into production, activity is monitored through email notifications and only authorized individuals have access to the Vault software.

Response–

a. Support team policies have been established, as documented in the IT Division procedures for Software Development Lifecycle, (IT00.201 Information Processing Software Development Procedures), to require all production implementations shall be authorized by the user in writing, and a record of that authorization will be retained.

b. All Team Leaders or Managers responsible, as documented in the IT Division procedures for Software Development Lifecycle, (IT00.201 Information Processing Software Development Procedures, for reviewing work assignments have been set up to receive automated messages when code is changed and placed in production.

c. Non-DOT user access (including VPN access) lists are sent to the appropriate DOT offices where they are reviewed and expired users are removed. This process occurs every six months. DOT will establish and implement a process to expire external users after a specified timeframe with a written process to extend access beyond the specified duration.

Conclusion - Response accepted.

Application Controls

No recommendations were noted in our review of application controls for the Department's Internal Billing System.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Scott P. Boisen, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Adam D. Steffensmeier, Staff Auditor
Jenny R. Lawrence, Staff Auditor