NEWS RELEASE

Contact: Andy Nielsen

FOR RELEASE   March 31, 2009   515/281-5834
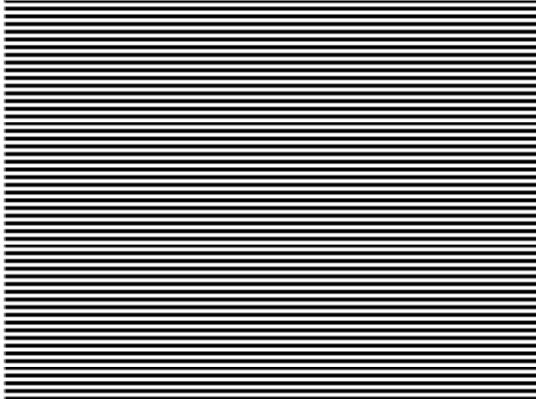
Auditor of State David A. Vaudt today released a report on a review of selected general and application controls over the Iowa Department of Transportation's Contractor Pay System for the period May 5, 2008 through July 31, 2008.

Vaudt recommended the Department establish procedures to ensure activity is monitored and program changes are approved before they are placed into production and restrict and monitor access to system software and system software utilities.

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/reports.htm.

# # #

**REPORT OF RECOMMENDATIONS TO THE
IOWA DEPARTMENT OF TRANSPORTATION
ON A REVIEW OF SELECTED GENERAL AND
APPLICATION CONTROLS OVER THE
CONTRACTOR PAY SYSTEM**

May 5, 2008 THROUGH JULY 31, 2008

$=$ Office of $=$

AUDITOR
OF STATE

State Capitol Building • Des Moines, Iowa

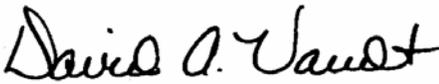## David A. Vaudt, CPA
Auditor of State

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, 2008, we conducted an information technology review of selected general and application controls of the Iowa Department of Transportation for the period May 5, 2008 through July 31, 2008. Our review focused on the general and application controls of the Iowa Department of Transportation's Contractor Pay System (CPS) 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 CPS. These recommendations have been discussed with Department personnel and their responses to these recommendations are included in this report.

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 CPS are listed on page 7 and they are available to discuss these matters with you.

DAVID A. VAUDT, CPA
Auditor of State
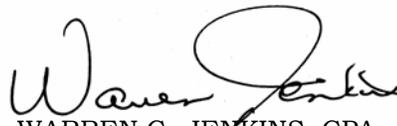
WARREN G. JENKINS, CPA
Chief Deputy Auditor of State

February 24, 2009

cc: Honorable Chester J. Culver, Governor
      Charles J. Krogmeier, Director, Department of Management
      Glen Dickinson, Director, Legislative Services Agency

Contractor Pay System General and Application Controls

A. <u>Background</u>

    The Iowa Department of Transportation's Contractor Pay System (CPS) is used to record construction progress reported by field inspectors and to prepare a progress voucher for payment to the contractor. The system is also used to manage contract change orders for the construction project.

B. <u>Scope and Methodology</u>

    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 CPS for the period May 5, 2008 through July 31, 2008. Specifically, we reviewed the general controls: access controls, application software development and change controls, system software controls and segregation of duties, 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. <u>Results of the Review</u>

    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.

<div align="center"><u>**General Controls**</u></div>

(1) <u>Change Control</u> – Change control procedures do not ensure modifications to application programs are approved before they are placed into production. 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. Final approval for DSR 25129 was dated 8 days after the modifications were placed into production.

    b. Supervisors do not necessarily check the DSR when an automated email is received to ensure the modification has been approved.

    c. Logs are not periodically reviewed for inappropriate activity.

Recommendation – The Department should establish procedures to ensure activity is monitored and program changes are approved before they are placed into production.

Response –

    a. Developers will be attaching each e-mail authorizing production implementation to the Development Service Request (DSR).

    b. The DSR number will be placed in the transaction comment for review by the Supervisor or the Supervisor's designee(s). The Supervisor or the Supervisor's designee(s) will spot check transaction comments to ensure requested modification work has been approved.

    c. Reviewing the Vault logs is not necessary because the information contained in the logs is the same information as is contained in the Vaults e-mails, which are reviewed, above.

Conclusion – Response accepted.

(2) System Software Access – Application programmers and system analysts are not prohibited from accessing system software. Access to system software is controlled by obscurity or the user's lack of knowledge about the program and not through security software restrictions.

Recommendation – The Department should establish procedures to restrict access to system software to only those individuals who need access to perform their job responsibilities.

Response – DOT will develop procedures to restrict access to currently unrestricted system libraries. DOT will review access to system software and restrict access to only those individuals who need access to perform their job responsibilities.

Conclusion – Response accepted.

(3) System Software and System Software Utilities Monitoring – Access to system software and system software utilities is logged but procedures have not been established to monitor access or periodically review activity.

Recommendation – The Department should establish procedures to monitor access to and usage of system software and system software utilities.

Response – In fiscal year 2009, the DOT IT Division will purchase a log management, or SIEM (Security Incident Event Management) solution. Products will be reviewed and tested to determine which will best meet the requirements of DOT's current infrastructure environment and necessary business requirements.

In fiscal year 2010, the DOT will develop procedures for log management after the product has been purchased and implemented.

Conclusion – Response accepted.

Application Controls

No recommendations were noted in our review of application controls for the Department's Contractor Pay 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:

    Michael P. Piehl, Senior Auditor
    Adam D. Steffensmeier, Staff Auditor
    Keith C. Kistenmacher, Staff Auditor
    Kelly L. Hilton, Assistant Auditor