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

Contact: Andy Nielsen
515/281-5834

FOR RELEASE June 30, 2006

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 Accounts Payable System for the period July 11, 2005 through August 3, 2005.

Vaudt recommended the Department implement procedures to strengthen employee password reset policies, improve controls over the migration of programs into production, develop written policies for access to and modification of system software, update and test the contingency plan, conduct periodic vulnerability assessments, review the listing of individuals with elevated privileges and strengthen procedures for handling output.

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 ACCOUNTS PAYABLE SYSTEM

JULY 11, 2005 TO AUGUST 3, 2005

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

February 28, 2006

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, 2005, we conducted an information technology review of selected general and application controls of the Iowa Department of Transportation for the period July 11, 2005 through August 3, 2005. Our review focused on the general and application controls of the Iowa Department of Transportation's Accounts Payable 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 Accounts Payable System. 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 Accounts Payable System are listed on page 10 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

cc: Honorable Thomas J. Vilsack, Governor
Michael L. Tramontina, Director, Department of Management
Dennis C. Prouty, Director, Legislative Services Agency

Accounts Payable System General and Application Controls

A. Background

The Iowa Department of Transportation's Accounts Payable System is used to process payments to vendors for goods and services delivered.

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 Accounts Payable System for the period July 11, 2005 through August 3, 2005. Specifically, we reviewed the general controls: security program, access controls, application software development and change controls, system software controls, segregation of duties and service continuity; 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) System Software Modifications – Formal policies and procedures should exist for requesting and authorizing new or modified system software. At a minimum, policies should include the use of a change request system, acceptance testing, documentation of management review and approval, a chronological record of changes and a problem log for tracking and troubleshooting system software.

Formal written policies and procedures for system software changes have not been developed.

Recommendation – The Department's IT Division should develop written policies and procedures to control system software modifications.

Response – The IT Division will expand existing procedures into an Applications Technology Services team work directive. The IT Division is working to implement the HP OpenView Service Desk product around July 2006. A Change Control module within this application will be customized to meet our needs in tracking system software modification.

Conclusion – Response accepted.

(2) Vulnerability Assessments – Internet–borne attacks targeting security vulnerabilities occur on a daily basis and can threaten assets and mission critical systems. A proven way to reduce risks from attack is to proactively test systems and implement appropriate counter measures. Vulnerability assessments are a valuable tool in this process and help in gauging the effectiveness of security measures.

Vulnerability assessments have not been performed.

Recommendation – The Department's IT Division should establish procedures to ensure vulnerability assessments are conducted periodically for critical systems.

Response – The Department will either engage the State of Iowa Information Security Office (ISO) to use their vulnerability assessment tool named Core Impactor or the Department will work with the ISO to contract with a vendor to perform the assessment.

Conclusion – Response accepted.

(3) System Software Access – Controls over access to and modification of system software and system software utilities are essential in providing reasonable assurance operating system-based security controls are not compromised. Access to system software and sensitive software utilities should be restricted to a very limited number of personnel whose job responsibilities require they have access. Application programmers and computer operators should not have access to system software, as this would be incompatible with their assigned responsibilities.

Policies and procedures do not provide guidance on restricting access to system software and utilities and access logs are not periodically reviewed. Additionally, a complete listing of available system utilities has not been maintained.

Recommendation – The Department's IT Division should develop policies and procedures to strictly limit access to system software and sensitive utilities. Additionally, a complete listing of available utilities should be maintained and access logs should be periodically reviewed.

Response – The Department will develop work directives which limit access to system software and utilities. The work directives will reflect existing procedures which utilize a dual control method for protection of data. The primary method restricts access to data through IBM's Resource Access Control Facility (RACF) security. The secondary method restricts access to sensitive utilities through RACF.

A list of utilities has been compiled. Those utilities controlled through RACF will be indicated on the list. A work directive will be established requiring periodic review of utilities controlled through RACF, who has accessed them, and utility usage rates. An IT Division work directive will be written requiring all requests, with accompanying justification, for access to RACF-controlled utilities to be approved by the Application Technology Services manager prior to access being granted.

Conclusion – Response accepted.

(4) Employee Password Reset – Occasionally, users forget passwords needed to gain access to system resources and are required to call the help desk to have their password reset. User verification procedures help ensure the authenticity of the user asking for a password reset.

Current steps taken to authenticate users could be strengthened.

Recommendation – The Department's IT Division should strengthen procedures for the verification of the authenticity of the user prior to resetting their password.

Response – The Department purchased the Proginet software to aid password resets. This software allows the user to store answer questions of their choice. Users who forget their password can go to a web site and answer questions with their unique pre-recorded responses. If the questions are answered correctly they will be allowed to reset their own password. Users who have not answered the questions or who have forgotten the answers to the questions are asked to call the Call Center who then will contact the user's supervisor. The supervisor verifies the identity of the user needing a reset. The Call Center then resets the questions to "null" which requires the user to establish new answers. The user then can reset their own passwords.

Conclusion – Response accepted.

(5) Access to Programs Turned in for Review – After a programmer completes a change to a program and management approves the change, operations is notified by a "blue card" when the program is ready to be loaded to the production library. Until the program is migrated to the production library by operations, the programmer still has access to the program and could make unauthorized changes.

Recommendation – The Department's IT Division should implement controls to ensure programmers do not have access to a program after management approval and before migration to the production library by operations.

Response – The IT Division has implemented a new source code repository for all mainframe and client/server source code thus eliminating this concern. Versioning of the source code ensures management approved code is the only code which is placed into production.

Conclusion – Response accepted.

(6) Temporary Program Copies – A programmer has the authority to take a copy of a production program or to take a second "temporary" copy in order to make changes. A log is maintained to document the first copy taken. However, the log does not document who took a second "temporary" copy. Additionally, if the "temporary" copy is placed with operations to be put into production first, an unauthorized program may be implemented without management oversight.

Recommendation – The Department's IT Division should establish procedures to ensure logs document the distribution of all copies taken of a program.

Response – The IT Division has implemented a new source code repository for all mainframe and client/server source code thus eliminating this concern. The software records the userid of the programmer along with a date/time stamp each time the program is checked in, and also records incremental changes with each new version. This recording of incremental changes eliminates the possibility that a program change could be placed into production without management approval.

Conclusion – Response accepted.

(7) Contingency Plan – Losing the capability to process, retrieve and protect information maintained electronically can significantly affect the Department's ability to accomplish its mission. For this reason, the Department should have procedures in place to protect information resources and minimize the risk of unplanned interruptions and a plan to recover critical operations should interruptions occur. The Department participated in a State initiative to develop continuity of operations and continuity of government plans, but a contingency plan for recovery of the data processing center in the event of a disaster has not been formally adopted.

Recommendation – The Department's IT Division should update and formally adopt a contingency plan for the recovery of operations in the event of a disaster. Copies of the plan should be provided to responsible individuals and stored at an off-site location. The plan should also be tested periodically.

Response – The DOT has prepared an overall Continuity of Operations/Continuity of Government (COOP/COG) plan which was submitted to Homeland Security and incorporated as Annex Y in the statewide COOP/COG plan. Elaboration of this plan will take place in FY2007.

Conclusion – Response accepted.

(8) RACF Access – IBM's Resource Access Control Facility (RCAF) is used by the Department to control system access. Three attributes (special, audit and operations) provide users with extraordinary privileges. We noted 30 individuals with the special attribute which allows the modification of all profiles in the RACF database and lets the user perform all functions except those requiring the audit attribute. Also, three users' password intervals were set to "NoInterval", meaning the system would not force the user to change their password periodically.

Recommendation – The Department's IT Division should periodically review the special, audit and operations attributes to ensure they are granted only to those individuals requiring these levels of access to perform their job duties and passwords are required to be periodically changed.

Response – The RACF access listing has been reviewed for individuals with the "s" (special) attribute and a determination made as to whether this access is required. An IT Division work directive will be written to require quarterly review of individuals possessing special, audit and operations attributes. Requests for the elevated attributes, along with the required justification, will be sent to the Application Technology Services team manager for approval.

The work directive will also require quarterly review to discover whether any "NoInterval" passwords exist. The work directive will state all passwords must be reset at specific intervals.

Conclusion – Response accepted.

Application Controls

(1) Written Policies and Procedures – Written procedures help ensure the consistency, accuracy and completeness of output produced as personnel change. The Department has not developed written procedures covering the reconciliation, verification and handling of system output.

Recommendation – The Department should develop written procedures for system output, including the reconciliation, verification and handling of output.

Response – We will comply with the auditor's recommendation.

Conclusion – Response accepted.

(2) Segregation of Duties – Work responsibilities are typically segregated so one individual does not control all critical stages of a process or perform incompatible duties. This helps diminish the likelihood errors or wrongful acts will go undetected because the activities of one group or individual will serve as a check on the activities of the other.

Four individuals have the ability to change a vendor address and approve the transaction at the accounting level.

Recommendation – The Department should modify responsibilities so individuals applying accounting level approval cannot change vendor addresses.

Response – The Department does not have the resources to completely segregate these functions and provide cross training amongst staff for critical functions. Due to the compensating controls implemented within the Accounts Payable System, the Department believes it has minimized the risk associated with this situation.

Compensating controls include: 1) While the address could be changed by these three individuals, the vendor name can not be changed on a voucher which has already been initiated. Therefore, the warrant would still be made out to the approved vendor and need to be endorsed by the approved vendor or designee to be considered a valid endorsement, 2) Two levels of approval are needed before a voucher can be paid and these approvals can not be applied by the same person,

3) The creation of voucher, Office approval and Accounting approval can not be applied by the same individual, 4) Vendor entry and update is restricted to designated individuals and 5) The address and vendor name is stamped in the voucher log when paid (newly added in FY2005), identifying where the payment was mailed and who the warrant was made out to.

Conclusion – Response accepted.

(3) Warrant Custody – Warrants to pay vouchers not paid by EFT are written in Des Moines by the Department of Administrative Services and delivered to Ames by shuttle. Warrants for contractor pay vouchers and multiple page accounts payable vouchers are separated from the warrants for simple, one or two page vouchers. Contractor pay vouchers and multiple page accounts payable vouchers are stuffed with the warrants and mailed from Ames. Simple one or two page vouchers are sent to Des Moines with the warrants for stuffing and mailing.

No record is kept of which warrants are mailed from Ames and which warrants are sent to Des Moines for mailing. Also, warrants prepared for delivery to Des Moines were not always stored in a secure location.

Recommendation – The Department should develop procedures to ensure the accountability and security of warrants is maintained.

Response – The warrant listing provides a record of the warrants that are mailed from Ames and those sent to Des Moines for mailing. We reconcile the dollar amount of the abstract to the warrant listing. We do not create a listing for those vouchers that are "pulled" for special mailing. Such a hand-prepared listing would only add time to the process and provide little real benefit should a warrant turn up missing, since the abstract/warrant listing gives us all the information necessary. Our procedures for lost checks are the same whether they were special mailing or not.

The warrants are received the previous day and are kept in a locked filing cabinet overnight for processing early the following morning. There have been a few instances when the courier returned late and has kept the warrants in mail room until the next morning. We will work with mail services to ensure that the warrants are secure under such conditions.

Conclusion – Response acknowledged. If the batch of warrants sent to Des Moines for mailing are lost or destroyed in transit, the identification and replacement of those warrants could be difficult.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Ernest H. Ruben, Jr., CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Patricia J. King, CPA, Senior Auditor II
Shawn R. Elsbury, Assistant Auditor
Carey L. Fraise, Assistant Auditor
Scott D. Trauger, Assistant Auditor
Donna R. Neubauer, Assistant Auditor