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

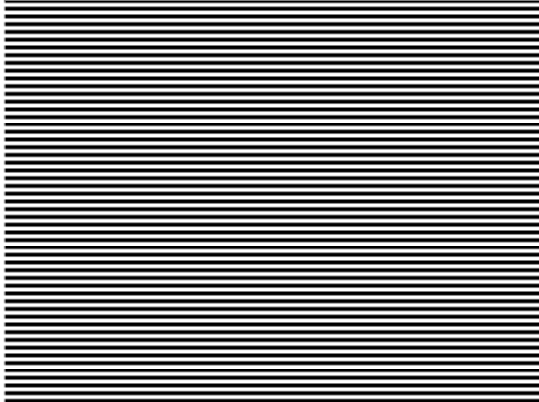FOR RELEASE   February 23, 2005   515/281-5834

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 April 5, 2004 through May 21, 2004.

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, improve controls for the FieldManager program and develop written procedures for the Contractor Pay System.

A copy of the report is available for review at the Iowa Department of Transportation or in the Office of Auditor of State.
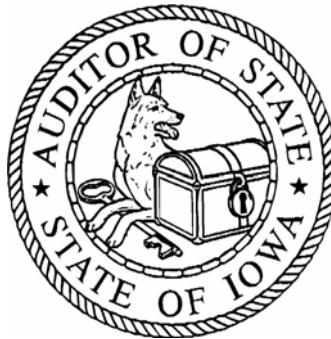
# # #

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

APRIL 5, 2004 TO MAY 21, 2004

═══ 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

State Capitol Building
Des Moines, Iowa 50319-0004

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

David A. Vaudt, CPA
Auditor of State

October 14, 2004

To Mark F. Wandro, 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, 2004, we conducted an information technology review of selected general and application controls of the Iowa Department of Transportation for the period April 5, 2004 through May 21, 2004. Our review focused on the general and application controls of the Iowa Department of Transportation's Contractor Pay 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 Contractor Pay System. These recommendations have been discussed with Department personnel and their responses to these recommendations are included in this report. We also reviewed and updated the status of previously issued recommendations for the Human Resource Information System (HRIS) included in our report dated July 3, 2003.

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 Contractor Pay System are listed on page 12 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
      Cynthia P. Eisenhauer, Director, Department of Management
      Dennis C. Prouty, Director, Legislative Services Agency

Contractor Pay System General and Application Controls

A. <u>Background</u>

The Iowa Department of Transportation's Contractor Pay System records construction progress through electronic updates by field inspectors and prepares a progress voucher for payment to the contractor.

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 Contractor Pay System for the period April 5 through May 21, 2004. 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. <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>Employee Password Reset</u> – 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 procedures for resetting passwords could be easily strengthened.

<u>Recommendation</u> – The Information Technology Division (IT Division) should strengthen procedures for the verification of the authenticity of the user prior to resetting the password.

Response – The IDOT purchased a software product called Proginet which addresses the issue of user verification for password changes. The software uses a web browser where the user would enter their userid and answer several questions that could be used to verify their identity should they need their password reset. When the user calls the Call Center for a password reset, the operator at the Call Center would access the system and ask the user to answer one or more of the specified questions prior to resetting the password. The IDOT will install the software this fiscal year and implement a revised policy/procedure for password reset.

Conclusion – Response accepted.

(2) 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 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 is in the process of implementing a new source code repository for all mainframe and client/server source code. This implementation is in part a result of previous audit recommendations. We will keep this and other recommendations in mind as we implement this source code repository.

Conclusion – Response accepted.

(3) Temporary Program Copies – To make changes, a programmer has the authority to take a copy of a production program or to take a second "temporary" copy. 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 IT Division should establish procedures to ensure logs document the distribution of all copies taken of a program.

Response – The IT Division is in the process of implementing a new source code repository for all mainframe and client/server source code. This implementation is in part a result of previous audit recommendations. We will keep this and other recommendations in mind as we implement this source code repository.

Conclusion – Response accepted.

(4) 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.

While a process has been implemented, including a change request form and management approval documentation, formal written policies and procedures for system software changes do not exist.

Recommendation – The IT Division should implement written policies and procedures for system software modifications.

Response – The mainframe technical staff in the IT Division has scheduled the implementation of written policies and procedures for system software modifications in their FY05 work plan.

Conclusion – Response accepted.

(5) 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 IT Division should develop policies and procedures regarding access to system software and utilities that strictly limits system software and sensitive utility access. Additionally, a complete listing of available utilities should be maintained and access logs should be periodically reviewed.

Response – The mainframe technical staff in the IT Division are scheduled in FY05 to develop written policies and procedures for access to systems software and sensitive utilities. Security to the systems software is incorporated into RACF and access to sensitive databases and datasets is also protected thru RACF. Because the access to the data has been restricted, access to the data through the use of all but a select group of utilities is also restricted. However since certain utilities bypass normal security checking, access to these specific utilities has been restricted. The technical staff will develop a complete listing of available utilities and post in a shared folder on the LAN. Periodic reviews of RACF access reports will be assigned to the RACF administrator.

Conclusion – Response accepted.

(6) 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. In 1997, the Department developed a contingency plan for data processing center recovery in the event of a disaster. This plan has not been formally adopted.

Recommendation – The Department should update, adopt and distribute a contingency plan. Copies of the plan should be stored at an off-site location and the plan should be periodically tested.

Response – The IDOT is participating in a statewide project sponsored by Iowa Homeland Security and Emergency Management Division for continuity planning which addresses Continuity of Operations and Continuity of Government (COOP/COG). The State is working with a consultant, Systems Planning Corp., who is coordinating the statewide effort. The consultant will develop a standardized plan which will be used by each agency as they develop their departmental COOP/COG plan. These department plans will be incorporated into a Comprehensive State of Iowa COOP/COG with Agency Addendums/Annexes. This statewide comprehensive plan is scheduled to be delivered at the end of June 2005. The IDOT has assigned staff from various offices in the IDOT (including the IT Division) to participate in this continuity planning project. The IDOT will develop a COOP/COG plan during the F05 fiscal year to be compliant with the statewide initiative.

Conclusion – Response accepted.

Application Controls

(7) FieldManager Controls – The FieldManager program provides an interface for the resident engineer's offices to convert information into a progress voucher that is uploaded to the Contractor Pay System. The FieldManager program is primarily utilized by the engineer offices located around the state.

We performed a review of the FieldManager input process and noted:

   (a) Field level approval of a progress voucher may be performed by the same employee who generated the progress voucher.

   (b) Contract modifications, while requiring signature approval, do not require separate electronic approvals before being accepted by FieldManager.

   (c) FieldManager does not force a user to periodically change the access password.

   (d) An automatic log-off feature is not utilized after a period of inactivity.

   (e) An automated system log does not identify the system user generating a progress voucher or transferring the progress voucher to the Contractor Pay System.

Recommendation – The Department should strengthen controls over user access, progress voucher approvals and automated logging. Additionally, the FieldManager program should require the electronic approval of contract modifications.

Response –

   (a) An employee may generate and approve the same voucher. However, an additional accounting level approval is required for every progress voucher and is applied to the progress voucher after the voucher is loaded from the Contractor Payment System (CPS) to Accounts Payable. Accounting approval is restricted, only allowing the staff in the Office of Finance to apply this approval after the voucher has gone through a pre-audit. All voucher payments require two levels of approval. Office approval is "level 1 approval" and Accounting approval is "level 2 approval."

(b) Before a contract modification can be applied, the contract modification must be approved in FieldManager. The individual who initials the contract modification can also approve the modification. The FieldManager software is "purchased" software and the IDOT cannot modify the functionality of the program. Compensating controls are relied upon to properly manage project activity. For instance.....

Projects cannot be randomly added to FieldManager or CPS. Projects are added to these systems via electronic data pass from the contract letting conducted by the Office of Contracts. Project quantities are only added by staff with authorized access to FieldManager using individualized passwords.

Project costs are reconciled at the end of the project before the retainage is released. As part of the project audit, all paper contract modifications are accounted for by both the project engineer and the pre-audit staff in the Office of Finance. The paper contract modifications must contain the proper signatures in order for the retainage to be released to the contractor.

(c) The new release of FieldManager allows the IDOT to set these parameters in the agency configuration program. The new configuration will have to be developed and imported into the FieldManager programs at all offices. In addition, all contracts will have to be "re-passed" to each office. The IDOT will analyze the impact of incorporating these changes.

(d) The new release of FieldManager allows the IDOT to set these parameters in the agency configuration program. The new configuration will have to be developed and imported into the FieldManager programs at all offices. In addition, all contracts will have to be "re-passed" to each office. The IDOT will analyze the impact of incorporating these changes.

(e) FieldManager documents who inputs pay quantities by posting the initials of the user who "signed onto the system" in the inspector daily work log. The FieldManager software is purchased software thereby limiting the IDOT's abilities to add additional controls over the input of data. The identity of who entered the pay data into FieldManager is not in a field which can be passed to the log in the Contractor Pay System (CPS).

While CPS may not identify who entered the data into FieldManager, the documentation does exist, it is in the FieldManager system. In addition, access to FieldManager is restricted to those with passwords. Procedures in the field are set as to who is authorized to transfer the pay data to CPS.

Conclusion – Response acknowledged.

(8) <u>Written Policies and Procedures</u> – The Department does not have formal written procedures covering the reconciliation, verification and handling of Contractor Pay System output.

    <u>Recommendation</u> – The Department should develop and implement formal written procedures over the Contractor Pay System. Procedures should include delivery of output, as well as reconciliation and verification of output.

    <u>Response</u> – Procedures for processing Contractor Pay are documented in staff desk manuals. The program produces a record or message which identifies that the number of records read (input) equals the number of records written (output). If the records read does not equal the records written the program will abend and will not complete. In this case the problem will be identified, resolved and re-submitted. In addition, the on-line programs in both the Contractor Pay and Accounts Payable systems have proofreaders and error checkers to correct data before it is submitted for processing.

    <u>Conclusion</u> – Response accepted.

D. <u>**Status of Prior Year's Recommendations**</u>

(1) <u>Iowa Department of Personnel Approvals</u> – Five separate system approvals are required to add a new permanent full time position. One of the five approvals is the Iowa Department of Personnel (IDOP). One Iowa Department of Transportation (IDOT) employee has the ability to apply approvals for IDOP. Additionally, the System Administrator for employee services of IDOT provides the logical access to employees to apply IDOP approval. Effective July 1, 2003, IDOP became the Iowa Department of Administrative Services, Human Resource Enterprise (DAS–HRE).

    <u>Prior Recommendation</u> – The ability of the IDOT employee to provide Iowa Department of Personnel authorization should be removed immediately. Additionally, written authorization should be obtained from IDOP for any user given authorization to apply IDOP approval.

    <u>Prior Response</u> – At the time of this audit, no employee in the Office of Employee Services (OES) had this authority. In the past, this authority was given to the employee in response to a specific request for assistance from the IDOP and later removed. OES will develop a procedure requiring written documentation of any possible future similar requests from IDOP, the personal approval of the Office Director before implementation of the request and written verification that the authority was subsequently removed.

    <u>Current Status</u> – Two Department employees could apply both P-1 approval and DAS-HRE (formerly IDOP) approval as of May 14, 2004. Written authorization had not been obtained from DAS-HRE.

    <u>Current Recommendation</u> – The ability of Department employees to provide Iowa Department of Personnel authorization should be removed and procedures should be established to ensure written authorization is obtained from IDOP/DAS-HRE for any user given authorization to apply IDOP approval.

    <u>Current Response</u> – The two employees have had their ability to apply DAS/HRE approval removed. Additionally, the ability to grant DAS/HRE approval within the Security System has been blocked. In order to grant DAS/HRE approval the P-1 System Administrator will need to have IT staff temporarily unblock DAS/HRE approval. Procedures will be established to ensure that written authorization is obtained from DAS/HRE before any user is given authorization to apply DAS/HRE approval.

    <u>Conclusion</u> – Response accepted.

(2) <u>Payroll Notifications</u> – A procedure has been put into place which requires the payroll department be notified whenever a payroll warrant is written exceeding $10,000. The notification is reported on the output to the payroll department. However, there is no documented evidence the payroll department reviews the notifications for propriety.

   <u>Prior Recommendation</u> – The payroll department should document the review of the notifications to help ensure warrants are proper and are authorized.

   <u>Prior Response</u> – Payroll will document the review of the notifications.

   <u>Current Status</u> – No documentation of reviews could be found.

   <u>Current Recommendation</u> – The payroll department should document the review of the notifications to help ensure warrants are proper and authorized.

   <u>Current Response</u> – Each pay period, staff review the processing documentation identifying and resolving error messages to ensure payroll has processed accurately. Effective immediately, staff will document their review of the payroll processing by initialing and dating the program documentation.

   <u>Conclusion</u> – Response accepted.

(3) <u>Proxy Access</u> –IDOT has a process where one employee can approve a new hire or an employee timesheet on behalf of a supervisor. System logs show the individual applying the approval as well as the supervisor for which they are a proxy. Procedures do not exist outlining how this access is to be granted. Additionally, the current process does not provide documentation for an employee's authority to act as a supervisor's proxy.

   <u>Prior Recommendation</u> – IDOT should establish written procedures identifying situations when proxy access should be granted as well as the process through which access is established. Additionally, documented approvals should be obtained anytime an employee is given proxy authority for a supervisor.

   <u>Prior Response</u> – The System Access System provides documented approval levels when a supervisor delegates proxy authority to an employee. IDOT has a policy (30.11) which states The user shall not use another's individual user ID and password without obtaining prior authorization, but does not identify situations when proxy access may be granted as well as the process through which access is established. The Office of Employee Services (OES) will work with the Information Technology Division (ITD) to review the policy and update it as needed. In addition, the OES and ITD will jointly prepare a memorandum to all managers and supervisors to remind them of the process and notify them of the change in the policy.

   <u>Current Status</u> – The policy has not been updated.

   <u>Current Recommendation</u> – The Department should establish written procedures identifying situations when proxy access could be granted as well as the process through which access is established. Additionally, authorization should be documented anytime an employee is given proxy authority for a supervisor.

   <u>Current Response</u> – The IDOT will move to update this proxy approval authority from the Security application to the System Access application. This will make the proxy approval authority more accessible to end users, formalize the request and approval process, and document the processing once the request are completed.

   <u>Conclusion</u> – Response accepted.

(4) <u>Emergency Recovery Procedures</u> – IDOT does not have written procedures to re-establish payroll in the event of a disaster. Essential department functions may still require human resources for which IDOT would have a responsibility to ensure employees are paid.

   <u>Prior Recommendation</u> – IDOT should establish written procedures to ensure employees will continue to be compensated for services rendered in the event of a disaster.

   <u>Prior Response</u> – IDOT is in the process of revising the 1997 disaster contingency plan. This plan will include all IDOT priority systems including payroll. The plan will provide for an efficient and timely resumption of business processes. The plan will be completed in fiscal year 2004.

   <u>Current Status</u> – The revision of the disaster contingency plan has not been completed.

   <u>Current Recommendation</u> –The Department should establish written procedures to ensure employees will be compensated for services rendered in the event of a disaster.

   <u>Current Response</u> – IDOT will establish written procedures to ensure employees will be compensated for services rendered in the event of a disaster as part of the COOP/COG plan to be developed by the IDOT in FY05. The IDOT plan will be incorporated into a statewide COOP/COG plan to be delivered in June, 2005.

   <u>Conclusion</u> – Response accepted.

(5) <u>Payroll Warrant Numbers</u> – Recommendation resolved.

Staff:

Questions or requests for further assistance should be directed to:

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

Other individuals who participated on this review include:

    Shawn P. Limback, CPA, Staff Auditor
    Curtis J. Schroeder, Assistant Auditor
    Trevor L. Theulen, Assistant Auditor