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 June 30, 2002 515/281-5515

Auditor of State David A. Vaudt today released a report on the Iowa Department of Transportation for the year ended June 30, 2002.

The Department is responsible for planning, developing, regulating and improving the State of Iowa's transportation system to provide and preserve adequate, safe and efficient transportation services.

Vaudt recommended that the Department:

(1) Improve controls over automated systems for supply inventory.

(2) Implement procedures to restrictively endorse checks immediately upon receipt.

(3) Deposit all cash receipts for the day at the end of the day.

(4) Develop and distribute an entity-wide information system security program.

(5) Strengthen controls over access to information systems.

(6) Strengthen controls for application software development and change control.

(7) Strengthen procedures for access to system software.

(8) Strengthen procedures related to information system service continuity.

A copy of the report is available for review in the office of the Auditor of State and the Iowa Department of Transportation.

# # #

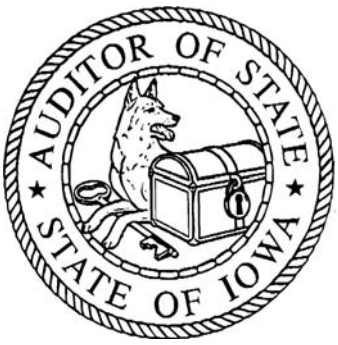
REPORT OF RECOMMENDATIONS TO THE IOWA DEPARTMENT OF TRANSPORTATION

JUNE 30, 2002

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 20, 2003

To Mark F. Wandro, Director of the Iowa
Department of Transportation:

The Iowa Department of Transportation is a part of the State of Iowa and, as such, has been included in our audits of the State's Comprehensive Annual Financial Report (CAFR) and the State's Single Audit Report for the year ended June 30, 2002.

In conducting our audits, we became aware of certain aspects concerning the Department's operations for which we believe corrective action is necessary. As a result, we have developed recommendations which are reported on the following pages. The recommendations include those which have been reported in the State's Single Audit Report as well as other recommendations pertaining to the Department's internal control and information system controls. 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 Department, citizens of the State of Iowa and other parties to whom the Department 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 Department during the course of our audits. Should you have any questions concerning any of the above matters, we shall be pleased to discuss them with you at your convenience. Individuals who participated in our audits of the Department 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

Findings Reported in the State's Single Audit Report:

CFDA Number 20.205 – Highway Planning and Construction
Agency Number: None
Federal Award Year: 2002

State of Iowa Single Audit Report Comment: 02-III-DOT-645-1

Davis-Bacon Act – Farm to Market Projects – The Department pays contractors directly for Farm to Market (FM) projects and, therefore, is responsible for compliance with federal requirements. The responsibility for compliance with federal requirements related to the Davis-Bacon Act has been delegated to the County Engineer, who is the contracting authority for these projects.

The Department relies on the final audit procedures performed by Transportation District personnel at the completion of a project to ensure that the Davis-Bacon requirements are being met. Documentation of final audit procedures performed by Transportation District personnel is not always specific enough to indicate if compliance with Davis-Bacon requirements had been determined.

The Department began developing written procedures for determining and documenting compliance with Davis-Bacon requirements for federally participating FM projects during fiscal year 2002 and fiscal 2003.

Recommendation – The Department should prioritize development and implementation of written procedures for determining and documenting compliance with Davis-Bacon requirements on federally participating FM projects. The written procedures should require that oversight activities be performed during the course of the project to ensure that federal requirements are being met and corrective action taken when non-compliance is noted.

Response and Corrective Action Planned – The Department has targeted the end of fiscal year 2003 to implement the written procedures on documenting compliance with Davis-Bacon on federal–aid Farm to Market (FM) projects. The committee that was formed to develop the written procedures is nearing completion of their assignment. The procedures will outline the documentation process by the Districts as part of their system review of federal-aid FM projects. The process by which the Office of Local Systems Field Review Technician documents the Davis-Bacon review on sampled federal-aid FM projects during the course of their construction will also be outlined. The Department will continue to work with the State Auditors and provide copies of the implementation procedures.

Conclusion – Response accepted.

CFDA Number 20.205 – Highway Planning and Construction
Agency Number: None
Federal Award Year: 2002

State of Iowa Single Audit Report Comment: 02-III-DOT-645-2

Subrecipient Monitoring – OMB Circular A-133 requires the pass-through entity to be responsible for monitoring the activities of the subrecipients, as necessary, to ensure that federal awards are used for authorized purposes in compliance with laws, regulations, and provisions of the contract or grant. A total of $46,474,031 was passed on to cities and counties in fiscal year 2002.

The Department monitors subrecipients through final audits performed by Transportation District personnel at the completion of a project. The final audits are not consistently documented and do not include several of the applicable federal compliance requirements.

The Department began developing written procedures for monitoring subrecipients' compliance with applicable federal requirements during fiscal year 2002 and fiscal year 2003.

Recommendation – The Department should complete the development of written procedures for monitoring subrecipients' compliance with applicable federal requirements so that Transportation District personnel clearly and consistently document the procedures performed. The monitoring process should cover all federal compliance requirements. The procedures should be implemented as soon as possible.

Response and Corrective Action Planned – The Department is currently in the process of completing the written procedures for monitoring and documenting the subrecipients' compliance with applicable federal requirements. The Office of Local Systems is currently working with the Districts to implement the documentation of the monitoring procedures they are responsible for. The Department is also completing the written procedures that will be utilized by the Office of Local Systems Field Review Technician during construction reviews of sampled federal aid projects. The Department will continue to work with the State Auditors and will have the written procedures available before the end of fiscal year 2003.

Conclusion – Response accepted.

CFDA Number 20.205 – Highway Planning and Construction
Agency Number: None
Federal Award Year: 2002

State of Iowa Single Audit Report Comment: 02-III-DOT-645-3

Cash Management – As stated in the Cash Management Improvement Act (CMIA) Agreement, the Department is to draw federal funds consistent with pre-issuance requirements. Federal funds should be deposited in a State account not more than two days prior to the day the State makes a disbursement.

A review of the cash management system for payments to subrecipients for the period July 1, 2001 through June 30, 2002 identified five instances in which federal funds were deposited from four to six days before they were disbursed.

Recommendation – The Department should develop and implement written procedures to ensure that federal funds are deposited and disbursed in accordance with the terms of the CMIA Agreement.

Response and Corrective Action Planned – In the five instances identified, federal funds were disbursed within 4 days of receipts and one item was disbursed within six days. Written procedures have been developed and implemented to ensure that federal funds are deposited and disbursed in accordance with the terms of the CMIA Agreement. The Department also worked with the Iowa Department of Revenue and Finance to modify the wording in the CMIA Agreement so that the time frame for disbursing federal funds will be consistent with the CMIA requirements.

Conclusion – Response accepted.

Findings Related to Internal Control:

(1) Segregation of Duties – An important aspect of an internal control system that safeguards assets and reasonably ensures the reliability of the accounting records is the concept of segregation of duties. When duties are properly segregated, the activities of one employee act as a check on those of another.

The Department uses a computerized on-line inventory system. At least eight employees have access to all areas of the inventory system and, therefore, can initiate and approve transactions without a separate review.

Recommendation – The Department should establish control procedures in the automated system for supply inventory that would prevent one individual from initiating and approving the same transaction or establish procedures to provide for an independent review of those transactions initiated and approved by the same individual.

Response – Beginning in February 2003, the Procurement and Distribution Office Director reviews a monthly report of all transactions processed by a single user if that user has authority throughout the inventory system.

Conclusion – Response accepted.

(2) Receipts Control – All mail receipts at the Department's Park Fair Mall offices (Motor Vehicle Enforcement, Vehicle Services, Drivers Services and Motor Carrier Services) are opened in the centralized mail room, sent to the individual offices for processing and then delivered to a central location for deposit. Checks are not restrictively endorsed until just prior to being deposited.

Recommendation – The Department should implement procedures to ensure that restrictive endorsements are placed on checks immediately upon receipt.

Response – The Office of Finance will work with these offices to implement the appropriate procedures.

Conclusion – Response accepted.

(3) Controls Over Cash Receipts – Cash receipts at the Park Fair Mall Drivers License Station in Des Moines are reconciled to the register and accounting records at the end of each business day. The receipts are placed in a safe for deposit at a local bank the afternoon of the next business day.

Approximately $12,000 was stolen from the Park Fair Mall office both in November 2002 and March 2003.

Recommendation – The Department should review and monitor its procedures for securing and depositing cash receipts to minimize the risk of loss. The Department should deposit all proceeds, other than the change fund balances, at the end of the day.

Response – The Department reviewed its procedures at the Park Fair Mall Drivers License Station and is now depositing all proceeds at the end of the day.

Conclusion – Response accepted.

Findings Related to Information System Controls:

Entity-Wide Security Program Planning and Management

(1) Security Plan – A written security plan should clearly describe the Department's security program and the policies and procedures that support it. The plan and related policies should cover all major systems and facilities and outline the duties of those who are responsible for overseeing security, as well as those who manage, use, or rely on the Department's computer resources. The security plan should be available to all affected employees.

Our review indicated policies and procedures are not always in writing and a comprehensive written security plan has not been approved.

Recommendation – The Department should complete the development and approval of a written security program that covers all major systems and facilities and outlines duties of those responsible for overseeing security as well as those who manage, use, or rely on the Department's computer resources. The plan should also be distributed to all affected employees.

Response – The IT Division and the Office of Facilities Support will develop/update security policies and procedures and work on a written security plan.

Conclusion – Response accepted.

Access Controls

(1) Password Control – Logical access controls involve the use of software, user ID's and passwords to control access to system resources. The Department's password policies do not appropriately protect resources.

Recommendation – The Department should implement security features that strengthen password controls.

Response – On October 1, 2002, the DOT adopted policy 030.11 addressing Information Resources Security.

Conclusion – Response acknowledged. Lockout features should also be strengthened.

(2) Employee Password Reset – Occasionally users forget passwords used to gain access to system resources. User verification procedures should be in place to help ensure the authenticity of the user asking for a password reset.

Recommendation – The Department should strengthen policies for user verification prior to resetting a password.

Response – The DOT is researching software to strengthen controls over password resets.

Conclusion – Response acknowledged. Until adequate software is implemented, policies over password reset should be strengthened.

Application Software Development and Change Control

(1) Access to Programs Turned in for Review – After a programmer completes a change to a program and management has approved the change, operations is notified by a "blue card" that 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 should implement controls to ensure that programmers do not have access to a program after management approval and before migration to the production library by operations.

Response – Because of our Support Team configuration and the process we use for development, we do not consider this a major threat to the security of our applications. Each analyst is assigned total responsibility for several systems. They have full responsibility for all changes to the systems and are the ones that initiate the "Blue Card" process. The possibility of them making last minute changes to the application is minimal because they would be the one responsible for correcting any errors generated.

Operations migrate the programs to the production library on a daily basis. We do agree that for a short period of time there is a possibility that someone else could possibly access the applications and make changes to it.

We are researching solutions that would provide better security for this process. Implementing a new source code repository tool may be the answer for this concern as well as "Temporary Program Copies".

Conclusion – Response acknowledged. To help minimize the risk that unauthorized changes are made, programmers access should be restricted after the program has been turned in to department management.

(2) Temporary Program Copies – In order 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. 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 – A log should document the distribution of all copies taken of a program.

Response – We recognize your concerns with this issue and plan to explore alternatives, such as implementing a source code repository tool which handles versioning, to the current process being followed. The support team structure has proven successful in preventing temporary copies from being placed into production by closely monitoring the work assignments within each team. Each program is assigned to one team member who responsible for pulling a copy from production, making modifications and placing it back into production.

Although there is the ability to obtain a temporary copy, this does not interfere with the proper version of a program being placed back into production. Programmers use the temporary copy option to obtain source code for use as a template for new development that contains similar logic.

Conclusion – Response acknowledged. To help minimize the risk of unauthorized changes to programs, the log should identify all copies of programs that have been made.

System Software

(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 policies and procedures for system software changes do not exist.

Recommendation – The Department should implement written policies and procedures for changes to system software.

Response – Effective February 21, 2003, the DOT implemented a written process for change control for system software modifications. A change control form is stored in a shared folder on a server with write permissions limited to technical staff. Each time a system software change is made, the technician creates a new form and enters the appropriate information. All domain users can read the documents.

Conclusion – Response accepted.

(2) System Software Access – Controls over access to and modification of system software and system software utilities are essential in providing reasonable assurance that 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 that they have access. Application

programmers and computer operators should not have access to system software, as this would be incompatible with their assigned responsibilities.

A review of access rights to system software indicated that computer operators, application programmers and others have system software and utilities access capabilities. Policies and procedures do not provide guidance and restrictions on system software or utility access. Access logs should be periodically reviewed. Additionally, a complete listing of available system utilities has not been maintained.

Recommendation – The Department 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 DOT will develop a procedure to protect datasets that contain system software and system utilities. Some system datasets have already been incorporated into RACF security. Currently, we use System Management Facility (SMF) to record certain events while the operating system is running. SMF has the capability of capturing failed attempts, which can be imported into RACF for report generation. The DOT will develop a procedure for capturing failed attempts from SMF and develop RACF reports to be run and reviewed on a periodic basis.

Conclusion – Response accepted.

(3) Master Console Access – Access to the master console should be restricted to a very limited number of individuals, primarily computer operations personnel, as critical system commands can be issued from the master console.

A review of master console access indicated that thirty-one user ID's have access to the master console. Of these thirty-one, two user ID's are for vendors, and eighteen are employees of another state department.

Recommendation – The Department should review access to the master console and strictly limit access to appropriate personnel.

Response – The DOT has reviewed the access to the master console. We have removed access for vendors and have removed access for all other state departments with the exception of one user from ITD technical staff who occasionally assists the DOT with storage management. There are 11 DOT employees with access to the master console.

Conclusion – Response accepted.

Service Continuity

(1) Off-site Data Set Inventory – Routinely copying data files and software and securely storing these files at a remote location are usually the most cost effective actions that an entity can take to mitigate service interruptions. The Department maintains backup of data sets at a separate off-site location. A review of procedures revealed that a current inventory listing of data sets is maintained at the data center, but a copy is not kept at the off-site storage location with the tapes.

Recommendation – The Department should develop procedures to maintain a copy of the current inventory of backup data sets at both the data center and the off-site storage location.

Response – The DOT utilizes software called CAI for its tape management system. CAI contains a listing of all data sets at the data center. The Computer Operations Manager maintains an electronic listing of all tapes that are at the off-site storage location at Park Fair Mall. He provides the computer operator at Park Fair with a hardcopy of that listing when changes are made to the tape inventory.

Conclusion – Response accepted.

(2) Contingency Plan – Losing the capability to process, retrieve, and protect information maintained electronically can significantly affect an entity's ability to accomplish its mission. For this reason, an entity should have (1) procedures in place to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. In 1997, the Department developed an 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.

Response – The DOT is in process of relocating the data center at the Ames Complex. The relocation will take place in September 2003. The design of the new data center has taken into consideration the placement of water pipes and shutoff valves to minimize risks along with the moisture detection system. The design also includes a fire suppression system for data center. The data center, the telecommunications closets and key technical staff are covered by an uninterruptible power supply (UPS), which will also be incorporated into the new data center as well. The DOT is in the process of reviewing the 1997 contingency plan and will make any appropriate adjustments in conjunction with mandates and recommendations from the Emergency Operations Center and ITD. The DOT will formally adopt and distribute the revised contingency plan.

Conclusion – Response accepted.

Staff:

Questions or requests for further assistance should be directed to:

Kay F. Dunn, CPA, Manager
Ruth H. Hill, CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this audit include:

Ernest R. Ruben, Jr., CPA, Senior Auditor II
Steven O. Fuqua, CPA, Senior Auditor
Daniel L. Durbin, CPA, Staff Auditor
Shawn P. Limback, CPA, Staff Auditor
Julie J. Lyon, CPA, Staff Auditor
Kelly V. Rea, CPA, Staff Auditor
Sarah M. Wright, Staff Auditor
Elvir Alicic, Assistant Auditor
Heather L. Templeton, Assistant Auditor