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

NEWS RELEASE

Contact: Andy Nielsen
515/281-5834

FOR RELEASE November 30, 2004

Auditor of State David A. Vaudt today released a report on the review of selected general and application controls over the State University of Iowa (University of Iowa) accounts receivable system (MARS) for the period of June 7, 2004 through July 23, 2004.

Vaudt recommended the University of Iowa develop and implement procedures to improve information system controls related to system access, documentation of authorized access requests and migration of programs to production.

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

# # #

REPORT OF RECOMMENDATIONS TO THE STATE UNIVERSITY OF IOWA ON THE REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE UNIVERSITY'S ACCOUNTS RECEIVABLE SYSTEM

JUNE 7, 2004 TO JULY 23, 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

David A. Vaudt, CPA
Auditor of State

State Capitol Building
Des Moines, Iowa 50319-0004

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

October 8, 2004

To the Members of the
Board of Regents, State of Iowa:

In conjunction with our audit of the financial statements of the State University of Iowa (University of Iowa) for the year ended June 30, 2004, we conducted an information technology review of selected general and application controls for the period June 7, 2004 through July 23, 2004. Our review focused on the general and application controls of the University's accounts receivable system (MARS) 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 University's general and application controls over the MARS system. These recommendations have been discussed with University 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 University of Iowa, citizens of the State of Iowa, and other parties to whom the University of Iowa 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 University 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 MARS system are listed on page 7, 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 Thomas J. Vilsack, Governor
Cynthia P. Eisenhauer, Director, Department of Management
Dennis C. Prouty, Director, Legislative Services Agency

Accounts Receivable System (MARS) General and Application Controls

A. Background

The accounts receivable system (MARS) at the University of Iowa (University) is used to process customer charges, credits and payments; generate billings; and maintain reporting information.

B. Scope and Methodology

In conjunction with our audit of the financial statements of the University, we reviewed selected aspects of the general and application controls in place over the MARS system for the period June 7 through July 23, 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 University and we reviewed University 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 University operations within the scope of our review. We developed an understanding of the University's internal control 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 use our finite review resources to identify where and how improvements can be made. Thus, we devote 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 University's responses, are detailed in the remainder of this report.

General Controls

(1) Password Controls – User ID's and passwords are used to identify and authenticate users in controlling access to system resources. Passwords, however, are not conclusive identities of specific individuals since they may be guessed, copied, overheard or recorded and played back. Typical controls for protecting the confidentiality of passwords include the requirements they be changed every 60 to 90 days and locked out after a limited number of consecutive unsuccessful attempts to log on within a 24 hour time period. Hawk ID passwords are not currently changed every 90 days and access is not denied after a limited number of unsuccessful attempts to log on within a 24 hour time period.

Recommendation – The University should implement security features to require Hawk ID passwords be changed every 60 to 90 days and reduce the number of unsuccessful log on attempts allowed within a 24 hour time period before the account is locked.

Response – The Enterprise Password Policy is enforced for the Hawk ID system, which services all students, faculty and staff, including those working in the health care areas. Bi-annual password changes which align with primary semester boundaries were chosen for several reasons. There is significant industry debate whether frequent password expiration strengthens or weakens security, given that users tend to write down passwords that change too often. We've coupled several password complexity measures along with maintaining password history, to further strengthen passwords. Ninety days is too short an interval to cover the period when many students are absent, which could result in significant support problems at our busiest time of year. Finally, we partnered on the policy with health care officials and with our Internal Audit Department, who agreed that the policy was acceptable given our academic environment.

The lockout settings provide sufficient protection against brute force password cracking attempts, but still provide necessary access to the system for legitimate users in lieu of having 24 hour help desk staff available to assist with login problems.

Conclusion – Response acknowledged. Technology advances continue to drive changes in best practices.

(2) Documentation of Access Requests – A formal process for requesting, authorizing, documenting and transmitting authorizations for access to system resources reduces the risk of mishandling, alterations and misunderstandings. The University has established an email process for the MARS system to request and authorize system access rights for individual users. Authorized email access requests are not maintained on file.

Recommendation – The University should develop procedures to retain documentation of system access requests authorized.

Response – A new utility within the MARS security system has been designed and is in process of being developed that accepts, tracks and maintains all MARS authorization requests and changes. It is expected that this module will be in place by November 1st, 2004, and that this electronic process will replace the existing email based system.

Conclusion – Response accepted.

(3) Migration of Programs to Production – 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, procedures and techniques to ensure all programs and program modifications are properly authorized, tested and approved and access to programs is carefully controlled. Access to the MARS program is controlled, but programmers have access to other mainframe programs after they are submitted for review but before the program is placed into production.

Recommendation – The University should establish controls to ensure programmers do not have access to a program after submitting it for review and before promotion to production.

Response – The concern is once a developer submits their program for promotion, they still have the ability to modify the code. Our security architecture prohibits their access to production code and modification of production data. Our change management system prevents staff from promoting their own code but does not have the capability to freeze the code and lock/prevent access to it once it has been submitted for promotion and prior to being promoted from test to another region. Managers who promote programs between regions use a manual utility to determine if code has been modified between when it was submitted and when it was actually promoted. Source code management systems are available that would resolve this problem but would require a significant investment in both capital and staff training. With the trend towards web-based and client/server applications and away from the main frame platform, it seems like the manual solution is the most prudent at this time.

Conclusion – Response acknowledged. Procedures to detect unauthorized changes after the fact are not as effective as controls to prevent unauthorized changes from occurring.

Application Controls

No recommendations were noted in our review of application controls for the University's MARS system.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Ted M. Wiegand, CPA, Senior Auditor
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Steven O. Fuqua, CPA, Senior Auditor
Beth A. Wichtendahl, CPA, Staff Auditor
Brad T. Holtan, Assistant Auditor