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 February 20, 2006

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) Human Resources Information System (HRIS) for the period June 6, 2005 through July 29, 2005.

Vaudt recommended the University of Iowa develop and implement procedures to improve information system controls related to system access, test procedures and security profile changes.

A copy of the report is available for review at the University of Iowa, 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 STATE UNIVERSITY OF IOWA ON THE REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE UNIVERSITY'S HUMAN RESOURCES INFORMATION SYSTEM

June 7, 2005 through July 29, 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

September 22, 2005

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, 2005, we conducted an information technology review of selected general and application controls for the period June 6, 2005 through July 29, 2005. Our review focused on the general and application controls of the University's Human Resources Information System (HRIS) 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 HRIS 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 HRIS system are listed on page 6, 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
Michael L. Tramontina, Director, Department of Management
Dennis C. Prouty, Director, Legislative Services Agency

Human Resources Information System (HRIS) General and Application Controls

A. Background

The Human Resources Information System (HRIS) at the University of Iowa (University) is used to process payroll and benefits 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 University's HRIS system for the period June 6 through July 29, 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 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 regularly, not allowed to be reused and locked out after a limited number of consecutive unsuccessful attempts. HRIS password policies include these controls, but they could be strengthened.

Recommendation – The University should implement security features to strengthen HRIS password controls.

Response – The University of Iowa will immediately take steps to strengthen password controls as suggested by this audit recommendation.

Conclusion – Response accepted.

2) Test Procedures – A disciplined process for testing and approving new and modified software prior to implementation is essential to make sure programs operate as intended and unauthorized changes are not introduced. Because testing is an interactive process generally performed at several levels, it is important to adhere to a formal set of procedures or standards for prioritizing, scheduling, testing and approving changes.

Program testing procedures defining responsibilities for each party have not been formalized or approved for all levels of testing for the HRIS system.

Recommendation – The University should develop and adopt written test procedures to identify the levels where testing is required.

Response – Fixes to the product are received from the vendor on a periodic basis. As these fixes are received, the changes are reviewed. Changes to the processes the University uses are thoroughly tested before being implemented. Before any change is moved to production a complete parallel payroll is run to document the results are the same. If other HR modules (e.g.: benefits) are affected by a fix, then these modules are thoroughly tested as well. Upgrades to the product are received every 24-36 months. All business processes are tested before an upgrade is put into production.

In response to this recommendation, the co-directors of Information Management Finance and Operations (IMFO) will develop a generic set of procedures that will be put into place before the next set of fixes or software modifications are moved into production. These new procedures will document the steps that will be taken to complete a review of the fixes. In addition, the procedures document will identify the tasks to be performed by technical and functional staff that will be required to perform a system test before approving the software updates that will be rolled into production.

Conclusion – Response accepted.

3) Security Profile Changes – Security profiles or authorized access rights help protect against tampering or unauthorized changes. Changes to security profiles by security managers granting administrative or system rights should be automatically logged and periodically reviewed by management independent of the security function.

Security profile changes are not logged or reviewed by management.

Recommendation – The University should enable or establish security features to ensure all security profile changes granting administrative or system rights are logged and periodically reviewed by management independent of the security function.

Response – We have turned on logging to track changes made to a persons access rights for the HRIS system. These logs will be reviewed every 60 days by one of the co-Directors of IMFO.

Conclusion – Response accepted.

Application Controls

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

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Gwen D. Fangman, CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Kathleen S. Caggiano, Senior Auditor
Daniel L. Grady, Staff Auditor
Kip M. Druecker, Staff Auditor
Carrie L. Livingston, Assistant Auditor