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 September 12, 2005

Auditor of State David A. Vaudt today released a report on a review of selected general and application controls over the Iowa State University of Science and Technology (Iowa State University) accounts payable and purchasing systems for the period of March 28 through April 28, 2005.

Vaudt recommended Iowa State University develop and implement procedures to improve information system controls related to risk assessments and security profile changes.

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

# # #

REPORT OF RECOMMENDATIONS TO IOWA STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY ON THE REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE UNIVERSITY'S ACCOUNTS PAYABLE AND PURCHASING SYSTEMS

March 28 Through April 28, 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

State Capitol Building
Des Moines, Iowa 50319-0004

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

David A. Vaudt, CPA
Auditor of State

May 18, 2005

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

In conjunction with our audit of the financial statements of Iowa State University of Science and Technology (Iowa State University) for the year ended June 30, 2005, we have conducted an information technology review of selected general and application controls for the period March 28, 2005 through April 28, 2005. Our review focused on the general and application controls of the University's accounts payable and purchasing systems 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 University's accounts payable and purchasing systems. 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 Iowa State University, citizens of the State of Iowa and other parties to whom Iowa State University 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 University's accounts payable and purchasing systems 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
Michael L. Tramontina, Director, Department of Management
Dennis C. Prouty, Director, Legislative Services Agency

Accounts Payable and Purchasing Systems General and Application Controls

A. Background

The accounts payable system at Iowa State University (University) is used to pay vendors for goods and services purchased as well as reimburse faculty and staff for travel and other business related expenses. The purchasing system at the University is used to process requests to order goods and services.

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 accounts payable and purchasing systems for the period March 28 through April 28, 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) Risk Assessments – A comprehensive high-level risk assessment is the starting point for developing or modifying the University's security policies and plan. Such risk assessments are important to help ensure all threats and vulnerabilities are identified, the greatest risks are considered and appropriate decisions are made regarding which risks to accept and which to mitigate through security controls.

Administrative Technology Services personnel indicated no formal risk assessments have been conducted as of April 28, 2005. The ISU Information Technology Security Policy does touch on the subject of risk assessments, but our review of the policy found it was missing four key factors that have been identified in the U.S. Government Accountability Office Federal Information System Controls Audit Manual as important to a successful risk assessment program.

- Designation of a central group to coordinate and schedule risk assessments at both a high level and lower levels. The frequency of performing risk assessments should also be addressed.

- Provide guidance encouraging the involvement of both business operation and technical staff in performing risk assessments.

- Require a final sign-off by the business manager of the organization doing the risk assessment indicating agreement with risk reduction decisions and acceptance of the residual risk as defined in their risk assessment.

- Require final documentation of risk assessments be filed with senior management and internal audit so participants can be held accountable for their decisions.

Recommendation – Administrative Technology Services should work with University administration to establish procedures to conduct periodic formal risk assessments of critical financial applications and revise the security policy addressing risk assessments to include the above factors.

Response – Administrative Technology Services (ATS), which will no longer exist as an individual department but will become part of the combined IT organization called Information Technology Services as of July 1, 2005, will work with the departments in ISU's Business and Finance unit to 1) identify what they consider to be "critical financial applications" and 2) establish procedures to conduct periodic formal risk assessments of those applications. We will also forward your recommendation to the Information Security Policy Committee along with the suggestion that revisions be made to the Risk and Impact portion of the ISU IT Security Policy based on the four items identified above.

Conclusion – Response accepted.

2) Security Profile Changes – Security profiles or authorized access rights 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.

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

Response – ATS will establish a formal process for employees to use when requesting changes to their administrative or system access rights. The log of those changes will be reviewed by team leaders annually.

Conclusion – Response accepted.

Application Controls

No recommendations were noted in our review of application controls for the University's accounts payable and purchasing systems.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Brian R. Brustkern, CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Scott P. Boisen, Staff Auditor
Marc D. Johnson, Staff Auditor
Donna R. Neubauer, Assistant Auditor