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
515/281-5834

FOR RELEASE July 27, 2010

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) Purchase Order/Requisition System for the period of March 20 through April 28, 2009.

Vaudt recommended Iowa State University ensure risk assessments are conducted in a timely manner, obtain signed confidentiality agreements from employees and contractors, require the authorization and testing of system software upgrades and modifications, and update and test the disaster recovery plan.

A copy of the report is available for review at Iowa State University, in the Office of Auditor of State and on the Auditor of State's web site at http://auditor.iowa.gov/reports/1061-8020-BT01.pdf

# # #

REPORT OF RECOMMENDATIONS TO IOWA STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY ON A REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE UNIVERSITY'S PURCHASE ORDER/REQUISITION SYSTEM

MARCH 20 THROUGH APRIL 28, 2009

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 22, 2010

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, 2009, we conducted an information technology review of selected general and application controls for the period March 20, 2009 through April 28, 2009. Our review focused on the general and application controls of the University's Purchase Order/Requisition 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 University's general and application controls over the Purchase Order/Requisition system. These recommendations have been discussed with University personnel and their responses to these recommendations are included in this report. While we have expressed our conclusions on the University's responses, we did not audit the University's responses and, accordingly, we express no opinion on them.

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 Purchase Order/Requisition 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 Chester J. Culver, Governor
Richard C. Oshlo, Jr., Director, Department of Management
Glen P. Dickinson, Director, Legislative Services Agency

Purchase Order/Requisition System General and Application Controls

A. Background

The purchase order/requisition system at Iowa State University (University) allows requisitions to be entered via the Internet and routed for completion and approval with email notifications from the E-Forms Approval system. Departmental verifiers are responsible for establishing users within their respective departments, verifying and completing requisitions before routing for approvals and resolving any objections which may arise. Purchase orders are created from the completed requisitions.

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 purchase order/requisition system for the period March 20, 2009 through April 28, 2009. 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 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 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 – Periodic risk assessments should be conducted to help ensure all threats and vulnerabilities are identified and considered, the greatest risks are identified and appropriate decisions are made regarding which to accept and which to mitigate through security controls. The University's risk assessment policy identifies seven critical functions and requires risk assessments to be performed on a three year rotational basis.

Assessments have only been conducted for two of the seven critical functions and one has not been finalized and is still in draft form. The risk assessment for the purchasing function has not been conducted.

Recommendation – Steps should be taken to ensure risk assessments are completed in a timely manner for the seven functional areas identified.

Response – IT Services reductions in staff last year forced us to make decisions which reflected our risk assessment from an IT perspective. There are some serious cyber attacks on financial related targets and these pose a higher risk than those identified a few years ago. The cyber warfare is extremely active and this is where we have had to place our resources. In these times, we have to make choices because there are not enough resources to do it all. While little progress was made on creating risk assessment documentation for new critical function systems, the Treasurer's Office risk assessment was reviewed after three years and appropriate changes made. We will investigate ways to make progress in this area in the year ahead.

Conclusion–Response accepted.

(2) Confidentiality Agreements–Confidentiality agreements serve as a reminder to staff of their responsibilities regarding the protection and safeguarding of confidential resources and information maintained by the University. All ITS employees with access to confidential information are required to sign a confidentiality agreement upon employment and annually thereafter. Four out of 21 ITS employees tested did not have current signed confidentiality agreements on file. Purchasing Office employees have access to vendor taxpayer identification numbers but are not required to sign annual confidentiality agreements.

Recommendation – The University should ensure all employees with access to confidential information sign confidentiality agreements annually and the signed agreements are retained on file.

Response - The Purchasing department had all their staff sign confidentiality agreements on April 15, 2009 and filed them in their departmental personnel files. IT Services is currently in the process of conducting annual performance evaluations and part of that yearly process is for IT Services employees to sign an Employee Confidentiality Agreement to be filed in their departmental personnel file. We are double-checking to ensure all employees sign a new agreement.

Conclusion–Response accepted.

(3) System Software Modifications – Configuration management provides strict control over the implementation of system changes and thus minimizes the risk for corruption to information systems. System software changes should be documented, tested and approved before implementation. Modifications/upgrades to the operating system are not logged or tested before being placed into production.

Recommendation - ITS should implement procedures requiring all system software upgrades/modifications to be authorized, logged and tested before they are placed into production.

Response – While individual IT Services systems analysts working in this unit have processes they are to follow and personal documentation on implemented systems software upgrades/modifications, there is currently no formal process which ensures the process is being followed to log and date the authorization to proceed with review/testing and implementation of all systems software upgrades/modifications. We will work this year to validate and implement appropriate processes to capture this information for later retrieval.

Conclusion–Response accepted.

(4) Disaster Recovery Planning – Disaster recovery plans are designed to help ensure an entity remains functional in the unlikely event of a loss of facilities or personnel. These plans should be updated regularly, periodically tested, distributed to key individuals and maintained in written form at an off-site location. The University has prepared a disaster recovery plan for its IT systems, but the main section has not been updated since 2004 and the appendices have not been updated in over a year. In addition, the plan has not been tested with a full walk through of a disaster situation.

Recommendation – The University should update its disaster recovery plan regularly and distribute it to all individuals who are expected to play a key role if the plan is put into action. Also, a copy of the plan should be stored at an off-site location and the plan should be tested periodically.

Response – IT Services embarked on a comprehensive disaster recovery plan for all its buildings and units two years ago. The IT Services work group developing the plan are scheduled to meet weekly and recently completed work on drafting an Emergency Operations/Response Information template using NFPA 1600 standards. Each of the four IT Services facilities are now completing this template for their facility. The work of this group has centered on the overall disaster recovery structure for IT Services. They are doing planning preparation for a disaster response including detailed action plans should a disaster occur. Aside from these discussions, the IT Services Data Center Operations Manager and ASB Site Coordinator are reviewing and updating the computer operations recovery documentation this year to ensure all information is up-to-date.

Conclusion–Response accepted.

Application Controls

No recommendations were noted in our review of application controls for the University's purchase order/requisition system.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Patricia J. King, CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Janet K. Mortvedt, CPA, Staff Auditor
Adam D. Steffensmeier, Staff Auditor
Rosemary E. Nielsen, Assistant Auditor