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

FOR RELEASE January 28, 2013

Contact: Andy Nielsen
515/281-5834

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) Room and Board System for the period of April 9, 2012 through May 1, 2012.

Vaudt recommended Iowa State University limit deletion capabilities for utility assessments to a few key individuals, eliminate generic user ID's to maintain accountability, establish procedures to periodically review access rights and implement a policy to require the encryption of laptop computers.

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/1361-8020-BT01.pdf.

# # #

REPORT OF RECOMMENDATIONS TO
IOWA STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY
ON A REVIEW OF SELECTED
GENERAL AND APPLICATION CONTROLS OVER THE
ROOM AND BOARD SYSTEM

APRIL 9, 2012 THROUGH MAY 1, 2012

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

January 2, 2013

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, 2012, we conducted an information technology review of selected general and application controls for the period April 9, 2012 through May 1, 2012. Our review focused on the general and application controls of the Room and Board 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 Room and Board 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 Room and Board System are listed on page 7 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 Terry E. Branstad, Governor
David Roederer, Director, Department of Management
Glen P. Dickinson, Director, Legislative Services Agency

Room and Board System Application Controls

A. Background

The Room and Board System at Iowa State University (University) is used to calculate and assess room and board for enrolled students based on room assignments and meal plans selected by students and rates as determined by the Board of Regents. The system also generates student billing information for the accounts receivable system.

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 Room and Board System for the period April 9, 2012 through May 1, 2012. Specifically, we reviewed the general controls: access controls, configuration management, segregation of duties and contingency planning and the application controls: interface controls and business process controls, including input, processing and output. We interviewed University staff 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 which 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 which 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) Generic User ID's – The Room and Board System processes student billings and includes confidential student data. Access should be limited to individuals who need access to the system to perform their job responsibilities and accountability should be maintained. We noted 20 generic user ID's which did not uniquely identify and authenticate to a specific user. Eight of these had add and update capabilities, 1 had delete capabilities and access to the Room and Board database. As a result, it may not be possible to hold specific individuals accountable for actions performed with generic user ID's.

Recommendation – The Department of Residence (DOR) should require specific user ID's be assigned for each employee/student having system access in order to maintain accountability and provide the ability to track activity to a specific user.

Response – The DOR is in the process of removing all generic user ID's having any type of update access from our system. In these cases, as we identify the owner, we are giving them the opportunity to request formal, individualized user names for the staff specifically responsible for doing updates.

We will maintain some generic usernames having view only access.

Conclusion – Response accepted.

(2) Review of Access Rights – Employee access to the Room and Board System is controlled by the system ID they are assigned to and the related screens made available to them. When an employee begins employment with the DOR, they are assigned to a specific system based on job responsibilities. Employee access is changed when a supervisor submits a request for additional system access. The DOR has not established procedures to require periodic review of user's system ID's or available screens to ensure they remain appropriate.

Recommendation – The DOR should establish procedures to periodically review the systems and screens assigned to users to ensure they remain appropriate.

Response – The DOR has recently developed a procedure and form for granting access to our systems and screens in ADIN (Administrative Information System). The form will have to be filled out and approved for all new requests and will have to be resubmitted annually for users to maintain their existing access levels.

The DOR is also doing an internal review to verify individuals have only the levels of access necessary for the completion of their job functions.

Conclusion – Response accepted.

(3) Encryption of Laptops – Encryption helps protect sensitive information stored on portable devices by rendering data unintelligible to unauthorized users. The University has not established a policy requiring sensitive institutional data stored on portable devices to be encrypted. If someone is aware of sensitive data on their laptop and ask about it, Information Technology Services (ITS) will work with them to encrypt their laptop.

Recommendation – The University should establish a written policy to require the encryption of any portable device before any sensitive data is stored on it and take steps to ensure all laptops are properly encrypted.

Response – A data classification policy has been drafted by the Office of the CIO and is in policy review. This policy provides guidance regarding data classification based on confidentiality, integrity and availability. Data can be ranked as high, moderate or low. A minimum security standard for protected data is also in review and describes the appropriate steps to be taken to protect data based on the classification. Appropriate encrypted data storage is a requirement of the minimum security standard. See the *ITS Policies in Development* section under http://www.it.iastate.edu/policies/.

Conclusion – Response acknowledged. Portable devices and laptop computers present a risk until encrypted.

Application Controls

(1) Deletion Capabilities – Access to the Room and Board System is assigned according to the employee's job responsibilities and needs. Authorization is requested by the employee's department head/supervisor and approved by the application owner. 21 individuals (including 3 generic user accounts) have access to the Room and Board screen used to enter/adjust monthly utility billings for family housing and have the ability to delete assessments.

Recommendation – The DOR should consider limiting deletion capabilities to a few key individuals.

Response – The DOR is doing an internal review to verify individuals have only the levels of access necessary for the completion of their job functions. Individuals who do not require deletion capability will have it removed.

Conclusion – Response accepted.

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, Senior Auditor
Andi J. Kaufman, CPA, Staff Auditor
Leanna J. Showman, Staff Auditor
Laura E. Grinnell, Assistant Auditor