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 June 4, 2012

Auditor of State David A. Vaudt today released a report on a review of selected application controls over the Iowa State University of Science and Technology (Iowa State University) Facilities Planning and Management (FP&M) - Facilities Administrative Management Information System (FAMIS) for the period of April 18, 2011 through May 16, 2011.

Vaudt recommended Iowa State University strengthen password controls, develop written procedures to clearly define access levels for FP&M positions to ensure proper segregation of duties, develop procedures to ensure only authorized modifications to the FAMIS system can be placed into production, modify FAMIS to e-mail a warning to management when an employee performs conflicting duties and periodically review user access rights. The University has responded positively to the recommendations.

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/1261-8020-BT01.pdf.

# # #

REPORT OF RECOMMENDATIONS TO IOWA STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY ON A REVIEW OF SELECTED APPLICATION CONTROLS OVER THE FACILITIES PLANNING & MANAGEMENT (FP&M) - FACILITIES ADMINISTRATIVE INFORMATION MANAGEMENT SYSTEM (FAMIS)

APRIL 18, 2011 THROUGH MAY 16, 2011

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

April 27, 2012

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, 2011, we conducted an information technology review of selected application controls for the period April 18, 2011 through May 16, 2011. Our review focused on the application controls of the Facilities Planning and Management (FP&M) - Facilities Administrative Information Management System (FAMIS) 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 application controls over FAMIS. 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 FAMIS 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 Terry E. Branstad, Governor
David Roederer, Director, Department of Management
Glen P. Dickinson, Director, Legislative Services Agency

Facilities Planning and Management - Facilities Administrative Management Information System Application Controls

A. Background

The FP&M - FAMIS system at Iowa State University (University) has modules for payroll, maintenance management, inventory control, space management, capital projects, key control, utility management, visual map and discoverer reports. Our focus for this audit was the payroll module which is used to track employee's time and facilitate client billing.

B. Scope and Methodology

In conjunction with our audit of the financial statements of the University, we reviewed selected aspects of the application controls in place over the FP&M-FAMIS system for the period April 18, 2011 through May 16, 2011. Specifically, we reviewed the application controls: access controls, configuration management, segregation of users, 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.

Application Controls

(1) Password Controls – User ID's and passwords are used to identify and authenticate users in controlling access to system resources. Typical controls for protecting information resources include the use of strong passwords which are at least 8 characters in length, include a combination of alpha, numeric and special characters, are changed every 60 to 90 days, are not allowed to be reused, are locked out after a limited number of consecutive unsuccessful attempts and require default passwords to be changed after the first login. Passwords for the Facilities Planning and Management – Facilities Administrative Management Information System (FAMIS) system include several, but not all of these control features.

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

Response – ISU plans to implement additional security features to strengthen password controls in the fall of 2012.

Conclusion – Response accepted.

(2) Written Segregation of Duties Procedures – Users are authenticated to the FAMIS system utilizing unique user ID's and passwords. They are assigned to a base security group which provides the access authorization for the user needed to perform their job responsibilities. Authorization to perform functions beyond the established base is requested by the user's supervisor and an additional security role is assigned to the user. Written procedures do not exist to provide guidance on maintaining the necessary segregation of duties.

Recommendation – FP&M management should develop written procedures to clearly define the access level required for the various FP&M positions and ensure proper segregation of duties is maintained.

Response – FP&M management has created procedures which we have now provided to you to provide staff with guidance.

Conclusion – Response accepted.

(3) Program Change Controls – FP&M has established procedures to control the modification of the FAMIS programming code. These procedures require a notification e-mail be sent by FP&M IT personnel to the manager of business and finance systems when program code is updated or modified. However, since the e-mail is not automatically generated when changes are moved into production, FAMIS upgrades or modifications could be put into production without management's knowledge or approval.

Recommendation – The FP&M management staff should develop procedures to ensure only authorized upgrades or modifications to the FAMIS system are moved into production.

Response – Only a select few individuals have these privileges to update or modify program code. These individuals are ISU ITS staff who are assigned to FP&M from the ISU ITS division. ISU ITS staff working in FP&M follow ITS protocol in these regards.

The ITS protocol requires an e-mail request from the customer to modify program code. Once the code has been modified and tested, the ITS Analyst replies to the original e-mail request and copies a mailbox named "Source Changes" with a description of the changes made and the name of the program(s) moved into production. As part of the process, the ITS Analyst works with the customer to test the changes to ensure the program is working correctly.

Conclusion – Response acknowledged. Procedures should be strengthened to prevent or detect unauthorized modifications to the FAMIS system.

(4) Segregation of Duties Conflicts – User rights within FAMIS are controlled by security groups and roles within the groups. When an employee with access rights for conflicting duties performs both duties on the same timecard, there is no warning or need for additional approval generated by FAMIS and, as a result, an employee could enter and authorize the same timecard and go undetected.

Recommendation – The FP&M IT staff should consider modifying FAMIS to prompt for additional approval or e-mail a warning to management when an employee who has conflicting duties performs both duties on a timecard.

Response – Since bringing this issue to our attention, a modification has been made so no individual can supervisor-approve his/her own timecard in FAMIS.

Conclusion – Response accepted.

(5) Review of Access Rights – An FP&M employee's access to FAMIS is controlled by their assigned security groups and roles. When an employee begins employment with FP&M, they are assigned to a specific security group based on duties performed. Their access is altered when a supervisor submits a request for additional security roles. FP&M has not established procedures to require periodic reviews of user security groups and roles to ensure they remain appropriate.

Recommendation – FP&M IT staff should establish procedures to perform and document periodic reviews of user security groups and roles.

Response – The FAMIS manager will annually review all employees assigned security group privileges to ensure continued need. A Reoccurring Outlook Task will be used as a reminder.

Conclusion – Response accepted.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Patricia J. King, CPA, CGFM 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
Jennifer M. Kopp, Staff Auditor
Leanna J. Showman, Staff Auditor