OFFICE OF AUDITOR OF STATE
STATE OF IOWA

Mary Mosiman, 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 November 12, 2013

Auditor of State Mary Mosiman today released a report on a review of selected general and application controls over the State University of Iowa (University) ePost and Effort Reporting (PAR) systems for the period May 29, 2013 through July 19, 2013.

Mosiman recommended the University comply with established policies and conduct or update its entity wide risk assessment. The University responded positively to the recommendation.

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/1461-8010-BT01.pdf.

# # #

REPORT OF RECOMMENDATIONS TO THE STATE UNIVERSITY OF IOWA ON A REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE UNIVERSITY'S EPOST AND EFFORT REPORTING (PAR) SYSTEMS

MAY 29, 2013 THROUGH JULY 19, 2013

Office of
AUDITOR OF STATE
State Capitol Building • Des Moines, Iowa

Mary Mosiman, 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

Mary Mosiman, CPA
Auditor of State

November 7, 2013

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) for the year ended June 30, 2013, we conducted an information technology review of selected general and application controls for the period May 29, 2013 through July 19, 2013. Our review focused on the general and application controls of the University's ePost and Effort Reporting (PAR) 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 a recommendation which is reported on the following pages. We believe you should be aware of this recommendation which pertains to the University's general and application controls over the ePost and Effort Reporting (PAR) systems. This recommendation has been discussed with University personnel and their response to this recommendation is included in this report. While we have expressed our conclusion on the University's response, we did not audit the University's response and, accordingly, we express no opinion on it.

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 ePost and Effort Reporting (PAR) systems are listed on page 6 and they are available to discuss these matters with you.

Mary Mosiman
Mary Mosiman, 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

ePost and Effort Reporting (PAR) System Controls

A. Background

The ePost system at the State University of Iowa (University) is a Windows-based client application. The ePost system tracks post-award data for each externally sponsored Federal project. The system is intended for use by the grant accountants. The Effort Reporting (PAR) system is a web-based Personnel Activity Report (PAR) and is used to identify how faculty and selected staff effort is distributed to a broad variety of activities. Federal guidelines (primarily OMB Circular A-21) and Board of Regent directives govern who is surveyed, how frequently they are surveyed, allowable variances between federal salary and federal effort and the time frame in which surveys must be distributed and completed. PARs are used to certify individual effort on federally sponsored grants and contracts.

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 ePost and Effort Reporting (PAR) systems for the period May 29, 2013 through July 19, 2013. Specifically, we reviewed the general controls: security management, access controls, configuration management and segregation of duties and the application controls: business process controls, including input, processing, output and interface controls. 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 recommendation.

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 recommendation, along with the University's response, is detailed in the remainder of this report.

General Controls

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. Best Practices suggest risk assessments be conducted periodically or whenever operations, use of technology or outside influences change.

The University's Information Security and Policy Office developed a policy titled "Enterprise Information System Program" which states, in part, the Information Security and Policy Office will facilitate an enterprise wide security risk assessment, as necessary, whenever significant changes to the computing environment are implemented or minimally within five years. The last risk assessment was conducted in October 2007.

Recommendation – The University should comply with established policies and conduct or update its enterprise wide security risk assessment.

Response – The Information Security and Policy Office regularly conducts risk assessments on critical university systems, as well as those presenting elevated risk to the university should they suffer a security breach. Examples are systems which process and store sensitive/restricted information and systems which support valuable research. We deferred planning and conducting an enterprise wide risk assessment in 2012 in order to focus our resources to support and securely manage the migration and firewalling of hundreds of servers and applications into the new Information Technology Facility (ITF) enterprise data center. The Information Security and Policy Office will begin planning an entity wide risk assessment in the second quarter of fiscal year 2014.

Conclusion – Response accepted.

Application Controls

No recommendations were noted in our review of application controls for the University's ePost and Effort Reporting (PAR) systems.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Daniel L. Grady, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated in this review include:

Kelly L. Hilton, Senior Auditor
Eric L. Rath, Staff Auditor
William B. Corley, Staff Auditor