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 November 29, 2010

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 State University of Iowa (University of Iowa) BuildUI System for the period June 14, 2010 through July 19, 2010.

Vaudt recommended the University of Iowa strengthen procedures for information system password controls and take steps to ensure the frequency and coverage of vulnerability scans and penetration testing are clearly defined. The University has responded positively to the recommendations.

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/1161-8010-BT01.pdf.

# # #

REPORT OF RECOMMENDATIONS TO THE STATE UNIVERSITY OF IOWA ON A REVIEW OF SELECTED GENERAL AND APPLICATION CONTROLS OVER THE UNIVERSITY'S BUILDUI SYSTEM

JUNE 14, 2010 THROUGH JULY 19, 2010

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

October 26, 2010

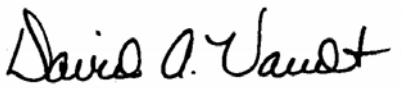
To the Members of the
Board of Regents, State of Iowa:

In conjunction with our audit of the financial statements of the State University of Iowa (University of Iowa) for the year ended June 30, 2010, we conducted an information technology review of selected general and application controls for the period June 14, 2010 through July 19, 2010. Our review focused on the general and application controls of the University's BuildUI 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.

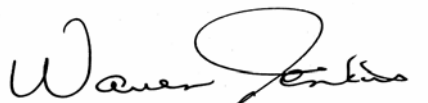
In conducting our review, we became aware of certain aspects concerning information technology controls for which we believe corrective action is necessary. As a result, we have developed recommendations which are reported on the following pages. We believe you should be aware of these recommendations which pertain to the University's general and application controls over the BuildUI 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 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 BuildUI 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 Chester J. Culver, Governor
Richard C. Oshlo, Jr., Director, Department of Management
Glen P. Dickinson, Director, Legislative Services Agency

BuildUI System Controls

A. Background

The BuildUI System at the State University of Iowa (University) is a Windows-based client application. The BuildUI System tracks capital project information throughout all stages of the project. The system is intended for use by project managers, budget officers, building coordinators, vendors and contractors. The BuildUI System provides project summary information, including a description of the project, project timeline dates and project budget information, once finalized.

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 BuildUI System for the period June 14, 2010 through July 19, 2010. Specifically, we reviewed the general controls: security management, configuration management and contingency planning, and the application controls: access controls, configuration management, segregation of users 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) Password Controls – User ID's and passwords identify and authenticate users in controlling access to system resources. Passwords, however, are not conclusive identifiers of specific individuals since they may be compromised. 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 and are locked out after a limited number of consecutive unsuccessful attempts. The BuildUI System includes a number of these controls, but the controls could be strengthened.

Recommendation – The University should implement security features to strengthen password controls for the BuildUI System when it is used to control access to sensitive information or critical financial systems.

Response – A revised enterprise password policy was approved in July 2010, and plans for implementation are underway. The revised password policy provides a framework to allow for differing levels of assurance for authentication. It will allow us to more appropriately manage institutional risk with stronger policy controls where they are warranted. The University will investigate whether the technical changes being implemented will allow us to reduce the number of invalid password attempts before an account is locked.

Conclusion – Response accepted.

(2) Vulnerability Scans – Internet–borne attacks targeting security vulnerabilities occur on a daily basis and can threaten assets and mission critical systems. A proven way to reduce risks from attack is to proactively test systems and implement appropriate counter measures. Vulnerability assessments are a valuable tool in this process and help in gauging the effectiveness of security measures.

Policies have been established to address vulnerability scans and penetration testing. The IT Security Office performs vulnerability scans of systems upon request by the business owner.

Recommendation – The University should strengthen policies for vulnerability scans and penetration testing to ensure the frequency and coverage provided are clearly defined.

Response – The UI Computer Vulnerability Scanning Policy authorizes the Information Security and Policy Office to perform vulnerability scans against all campus computer systems as necessary; vulnerability scans are conducted for campus systems on a regular basis. In addition, the Information Security and Policy Office offers a Penetration Testing service for the campus to assess the security controls implemented for critical IT systems. The Penetration Testing service incorporates network based vulnerability scanning with additional focused assessment methodology and tools. The University will update the Information Security Program to include and reference policy information that critical systems take advantage of these services.

Conclusion – Response accepted.

Application Controls

No recommendations were noted in our review of application controls for the University's BuildUI System.

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Gwen D. Fangman, CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated in this review include:

Daniel L. Grady, Senior Auditor
Scott P. Boisen, Senior Auditor II
Kristin M. Ockenfels, Assistant Auditor