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
FOR RELEASE January 5, 2004 515/281-5834

Auditor of State David A. Vaudt today released a report on the review of selected general and application controls over the State University of Iowa purchasing/accounts payable system (APPO) for the period of June 2 through June 27, 2003.

Vaudt recommended the State University of Iowa develop and implement procedures to improve information system controls related to activity logs and system access.

A copy of the report is available for review at the State University of Iowa or in the Office of Auditor of State.

###

REPORT OF RECOMMENDATIONS TO
STATE UNIVERSITY OF IOWA
ON THE REVIEW OF SELECTED GENERAL AND
APPLICATION CONTROLS OVER
THE PURCHASING/ACCOUNTS PAYABLE SYSTEM

JUNE 2 TO JUNE 27, 2003

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

August 8, 2003

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 for the year ended June 30, 2003, we have conducted an information technology review of selected general and application controls for the period June 2 through June 27, 2003. Our review focused on the general and application controls of the purchasing/accounts payable system (APPO) as they relate to our audit of those 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 that 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 APPO system. These recommendations have been discussed with University personnel, and their responses to these recommendations are included in this report.

This report, a public record by law, is intended solely for the information and use of the officials and employees of the State University of Iowa, citizens of the State of Iowa, and other parties to whom the State 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 APPO system are listed on page 6, and they are available to discuss these matters with you.

David A. Vaudt

DAVID A. VAUDT, CPA
Auditor of State

cc: Honorable Thomas J Vilsack, Governor
Cynthia P. Eisenhauer, Director, Department of Management
Dennis C. Prouty, Legislative Services Agency

Purchasing/Accounts Payable System General and Application Controls

A. Background

The purchasing/accounts payable system (APPO) at the State University of Iowa (University) is used to issue and process purchase orders, generate and process voucher payments and maintain reporting information.

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 APPO system for the period June 2 through June 27, 2003. 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 from 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 that are within our review scope. We developed an understanding of the University's internal control that is relevant to the operations included in our review scope. We believe our review provides a reasonable basis for our recommendations.

We use a risk-based approach when selecting activities to be reviewed. We therefore focus our review efforts on those activities we have 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 that certain controls can be strengthened to further ensure the reliability of financial information. Our recommendations, along with the University's responses, are listed in the remainder of this report.

General Controls:

(1) Activity Logs – Activity logs or security software generally provide a means of determining the source of a transaction or an attempted transaction and monitoring users' activities. However, to be effective, this feature needs to be activated and management needs to review and take action on these reports.

Activity logs of remote access logons are not regularly reviewed and network and APPO system activity is not logged.

Recommendation – The University should establish procedures to record and monitor activity logs for unauthorized or unusual activity.

Response – The current version of the PeopleSoft APPO software does not have the capability to generate an activity log. Plans are underway to upgrade to a newer version that does have this capability. Once the new version is in production, the

Director of Purchasing and ITS Security Office Personnel, or his/her designee, will monitor the activity log for unauthorized or unusual activity. Direct read/write access to the PeopleSoft APPO system is reviewed and approved by security administrators in the accounts payable and purchasing departments.

Conclusion – Response accepted.

(2) Logical Access Controls – Passwords are used to authenticate users to the network and APPO system. The University has developed an enterprise password policy that includes minimum password standards that are designed to provide good authentication and defend against unauthorized use of the systems. Those standards indicate that password strength tests and/or controls (e.g. alpha-numerics, dictionary tests) will be employed to ensure that robust passwords at least 6 characters in length are used. The policy also states that passwords should be changed regularly.

Software solutions are not used to enforce the use of strong passwords. Manual steps are taken by the Purchasing Office to ensure that passwords for the APPO system are changed regularly but the network passwords do not expire and the minimum password length for the network is set at 5 characters.

Also, to help ensure that passwords cannot be guessed, attempts to log on to the system with invalid passwords should be limited by a lockout feature. While the lockout feature for the network has been enabled, the PeopleSoft APPO system version in use does not have a lockout capability.

Recommendation – The University should activate available features in NetWare and APPO software to enforce the use of strong passwords and ensure that they are changed regularly. Also, as lockout features become available for the APPO system, they should be employed.

Response – The Windows workstation PCs that access the PeopleSoft applications require authentication during the PC startup process. This is either through Novell NDS or Microsoft Active Directory authentication. These authentications are required before authorization is allowed to PeopleSoft application servers and data.

Each user of the PeopleSoft applications must log in to the application security layer to gain rights to specific functionality and data. Although PeopleSoft does not force password rotation, it is a standard practice for the functional units that use these applications. The Director of Purchasing keeps a separate log and notification process to require routine password changes for staff employed by the Purchasing and Accounts Payable departments. The University plans to deploy lockout features and other security protections as they become available in future updates to the APPO application software.

Conclusion – Response acknowledged. Network passwords should meet minimum standards.

Application Controls:

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

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Ted M. Wiegand, CPA, Senior Auditor
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Steven O. Fuqua, CPA, Senior Auditor
Beth A. Wichtendahl, CPA, Staff Auditor
Kristen E. Harang, CPA, Staff Auditor
Jeffery M. Evans, Assistant Auditor