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
515/281-5834

FOR RELEASE September 21, 2004

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) accounts receivable system for the period of April 6 through May 14, 2004.

Vaudt recommended Iowa State University develop and implement procedures to improve information system controls related to risk assessments, system access, security profile changes and the migration of programs to production.

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

# # #

REPORT OF RECOMMENDATIONS TO
IOWA STATE UNIVERSITY OF SCIENCE AND TECHNOLOGY
ON THE REVIEW OF SELECTED GENERAL AND
APPLICATION CONTROLS OVER
THE UNIVERSITY'S ACCOUNTS RECEIVABLE SYSTEM

APRIL 6 TO MAY 14, 2004

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

July 1, 2004

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, 2004, we have conducted an information technology review of selected general and application controls for the period April 6, 2004 through May 14, 2004. Our review focused on the general and application controls of the University's accounts receivable 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 University's accounts receivable 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 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 University's accounts receivable system are listed on page 9 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 Thomas J. Vilsack, Governor
Cynthia P. Eisenhauer, Director, Department of Management
Dennis C. Prouty, Director, Legislative Services Agency

Accounts Receivable System General and Application Controls

A. Background

The accounts receivable system at Iowa State University (University) is used to record charges and payments to the accounts of ISU customers (the general public, staff and students).

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 accounts receivable system for the period April 6 through May 14, 2004. 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 of 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 within our review scope. We developed an understanding of the University's internal control relevant to the operations included in our review scope. 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 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 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) Risk Assessments – A comprehensive high-level risk assessment should be the starting point for developing or modifying the University's security policies and plan. Such risk assessments are important to help ensure all threats and vulnerabilities are identified, the greatest risks are considered and appropriate decisions are made regarding which risks to accept and which to mitigate through security controls.

University personnel indicated no formal risk assessments have been conducted as of May 14, 2004.

Recommendation – The University should establish procedures to conduct periodic formal risk assessments.

Response – A University-wide assessment of IT risks is outside the scope of ATS responsibility since ATS does not have authority over all aspects of the University's technology. ATS has conducted risk assessments of IT activities within its scope of responsibility. The ATS disaster recovery plan was developed based upon a review of relevant technology needs and risks.

ISU's Chief Information Officer (CIO) has overall responsibility for the security of the University's information technologies. This new office/position was effective July 1, 2004. The University's new Information Security Policy also became effective July 1, 2004. Section 3.4 of the Information Security Policy requires colleges, departments and units to conduct risk assessments for information and information systems in their areas of responsibility.

The ISU Office of Internal Audit did perform an information technology risk assessment in Fiscal 2004. They also provided guidance during the development of the ISU Information Security Policy regarding departmental responsibilities for assessing risks.

Conclusion – Response acknowledged. The information technology risk assessment was performed by the Office of Internal Audit primarily for audit planning purposes and did not necessarily follow the approach recommended by the National Institute of Standards and Technology (NIST) in Special Publication 800-30. The University should establish procedures to periodically conduct risk assessments following NIST guidance.

2) Password Change Frequency – User ID's and passwords are used to identify and authenticate users in controlling access to system resources. Passwords, however, are not conclusive identities of specific individuals since they may be guessed, copied, overheard or recorded and played back. One of the typical controls for protecting the confidentiality of passwords includes the requirement they be changed every 60 to 90 days. Passwords are not currently changed every 90 days.

   Recommendation – The University should implement security features to require passwords are changed every 60 to 90 days.

   Response – An initiative to change the AccessPlus four digit login PIN to a six to eight character password was begun February 18, 2004. It affects all faculty, staff, students and affiliates that use AccessPlus. This transition will continue through the end of this calendar year as students and faculty return for the fall semester. This has resulted in new, improved and formalized procedures for resetting passwords. ATS needs the opportunity to evaluate the support staff needs for password resets after the conversion is complete. ATS will continue to closely study the issues related to passwords and will take this audit recommendation under advisement.

   The current password expiration time period was established in response to a specific recommendation in a previous General and Application Controls Audit conducted by the State Auditors Office.

   Conclusion – Response acknowledged. Technology advances have continued to drive changes in best practices since the previous recommendation to increase the frequency of password changes was made. The University should require passwords be changed every 60 to 90 days.

3) System Access Removal – IT Security should be notified immediately when system users are terminated or transferred to prevent unauthorized access to system resources. Departments or Offices authorizing access to their records (resource owners) should also periodically review individual user access rights to ensure they remain appropriate.

Iowa State University has not implemented University-wide policies and procedures to ensure IT Security is notified when employees terminate or are transferred. Also, procedures have not been established to periodically review those with system access to determine access remains appropriate. A review of 5 inactive user ID's found all 5 to have unnecessary or inappropriate access to the AccessPlus/ADIN system.

Recommendation – The University should develop and implement procedures to ensure IT Security is notified when employees terminate employment or are transferred within the University so system access is appropriately modified. Also, procedures should be established to periodically review those individuals with system access to identify any no longer needing access.

Response – During the past year, ATS has been looking at several possible ways to address this issue. We commit to working with the ISU Department of Human Resources, the HR Liaison group and the Employee Personnel Action (EPA) group to develop an automated notification process to identify employees who terminate or transfer within the University. We will also work to develop a realistic process for reviewing individual employee system access.

Conclusion – Response accepted.

4) Security Profile Changes – Security profiles or authorized access rights should be protected against tampering or unauthorized changes. Changes to security profiles by security managers should be automatically logged and periodically reviewed by management independent of the security function.

Security profile changes are not logged.

Recommendation – The University Administrative Technology Services Department should put security features in place to ensure all security profile changes are logged and the log is periodically reviewed by management independent of the security function.

Response – ATS will study the feasibility of logging these changes. Authority to make changes is system controlled. Update rights are granted only to those individuals who have been identified as responsible for specific applications systems and departments. We will seek the guidance of the ISU CIO as to the recommendation of periodic and independent review.

Conclusion – Response accepted.

5) Change Control Process – For both application programs and system software, a programmer may check out a program, change the program and place the program back into production. This activity is logged at the Administrative Technology Services Department by the Source Control System utility and a report is sent to supervisors each day of the programs checked in.

Manager approval is not required before a program is placed into production and no separate independent group moves programs from test to production. There are no procedures in place to ensure the log created by the Source Control System utility is routinely reviewed. Therefore, unauthorized program changes could be implemented without management oversight. Also, there is no documentation management periodically reviews production program changes to determine whether access controls and change controls have been followed or user needs have been met.

Recommendation – The Administrative Technology Services Department should implement procedures to ensure proper segregation of duties between programmer, manager approval and promotion to production.

Response – Administrative Technology Services has implemented a number of significant program (software) source controls in the past several years. An automated and auditable log of all program changes is maintained which collects: 1. The Person making the change, 2. The date of the change, 3. The person or process requesting the change, 4. The method of communicating the request for the change, 5. The reason or justification for the change, 6. A before and after audit trail of every line of code being added, deleted, or changed, and 7. The creation and retention of a program version with every change moved into production. An automated electronic notice containing the above information is sent to Administrative Technology Services managers daily informing them of every program being moved into production. The daily notices are permanently archived. An electronic e-mail notice sent by the analyst further documenting every program change is also required and permanently archived. An Administrative Technology Services staff person has been assigned the responsibility of doing monthly spot checks to verify the confirming e-mails were sent. In addition, source code authorizations are assigned to every program. This means that the individuals granted authorization rights to a specific program are the only individuals who can checkout, change and check a program back into the production source code library.

We believe these controls provide ample evidence of our commitment to the importance we put on the integrity and reliability of the software for which we are responsible. We also believe these controls provide a strong deterrent and do include a significant degree of management oversight. As such, including an additional manager sign-off step into the process of moving new software and software changes into our production environment would do little to strengthen the controls and would actually lengthen and slow down our ability to quickly respond to software change needs. We will continue to look for practical and effective ways to further improve and strengthen this process.

Conclusion – Response acknowledged. Procedures to detect unauthorized changes after the fact are not as effective as controls to prevent unauthorized changes from occurring.

6) System Software – Because of the powerful capabilities at the disposal of those who have access to system software, its use should be monitored to identify any inappropriate or unusual behavior. For monitoring to be effective in both detecting and deterring inappropriate use, those authorized to use the system software should understand (1) which uses are appropriate and which are not and (2) their activities may be monitored. Such policies should be documented and distributed to all personnel.

No specific written policies and procedures have been developed for using and monitoring the use of system software.

Recommendation – The Administrative Technology Services Department should develop written policies and procedures over using and monitoring the use of system software.

Response – ATS commits to developing a written policy covering system software use and will implement, as part of the annual employee review, a process of review and employee acceptance similar to that used for the current Employee Confidentiality Agreement.

Conclusion – Response accepted.

Application Controls:

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

Staff:

Questions or requests for further assistance should be directed to:

Erwin L. Erickson, CPA, Director
Brian R. Brustkern, CPA, Senior Auditor II
Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

Patricia J. King, CPA, Senior Auditor II
Cory A. Warmuth, CPA, Staff Auditor
Sarah M. Wright, Staff Auditor
Heather L. Templeton, Assistant Auditor