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

FOR RELEASE   May 23, 2008   515/281-5834

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) payroll system for the period March 27 through May 11, 2007.

Vaudt recommended Iowa State University develop and implement procedures to improve information system controls related to security profile changes, system access, independent reviews and written office manuals.

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/reports.htm.

# # #

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

March 27 Through May 11, 2007

===== 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 10, 2008

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, 2007, we conducted an information technology review of selected general and application controls for the period March 27, 2007 through May 11, 2007. Our review focused on the general and application controls of the University's payroll 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 payroll 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 payroll system are listed on page 8 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
      Charles J. Krogmeier, Director, Department of Management
      Dennis C. Prouty, Director, Legislative Services Agency

Payroll System General and Application Controls

A. <u>**Background**</u>

The payroll system at Iowa State University (University) is used to calculate and distribute salaries and wages to the employees of the University.

B. <u>**Scope and Methodology**</u>

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 payroll system for the period March 27 through May 11, 2007. 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 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 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. <u>**Results of the Review**</u>

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) <u>Security Profile Changes</u> – Security profiles or authorized access rights protect against tampering or unauthorized changes. Changes to security profiles by security managers granting administrative or system rights should be automatically logged and periodically reviewed by management independent of the security function. Security profile changes are not automatically logged or reviewed by management.

    <u>Recommendation</u> – University Information Technology Services (ITS) should enable or establish security features to ensure all security profile changes granting administrative or system rights are logged, including individuals employed prior to November 1, 2006, and are periodically reviewed by management independent of the security function. Security profiles for all employees working in this area need to be created to allow easier review of administrative or system rights for each individual employee.

    <u>Response</u> – ITS defined the formal process and form for employees and managers to use to request changes to their administrative or systems access rights. The process includes an annual review of the requested changes against the record of authority at the time of implementation of this process. The process was implemented on November 1, 2006. ITS has security profiles for new employees, but does not have security profiles for our long-term system administrators. ITS will begin discussion of the last part of this recommendation and work to create security profiles for all employees working in this area.

    <u>Conclusion</u> – Response accepted.

2) <u>System Access</u> – Information Technology Services (ITS) provides user level access to the central information system. Each department of the University is responsible for granting, deleting and checking the appropriateness of employee access to departmental resources. ITS relies on each department to notify it when access to the system is no longer required. The following instances were noted where procedures did not appear to be effectively restricting access according to management's wishes:

    - From a University provided listing of 400 user id's which had not accessed the University systems during the previous six months, we identified 118 user id's which have not accessed the system for the past two years and have not been revoked.

    - Three individuals out of five tested had access to a subsystem allowing them to initiate and create correction vouchers when view only access would have been more appropriate.

    - Access rights for one individual who terminated at the end of January were not removed until April.

    <u>Recommendation</u> – ITS should work with departmental resource owners to establish procedures to periodically review users' access rights to ensure access rights granted remain appropriate for the current job responsibilities and needs of the employee.

    <u>Response</u> – On September 24, 2007, ITS made changes to expire the passwords of AccessPlus users with uBusiness and Advisor/Faculty tabs which had not accessed the systems during the past 90 days.

    The three individuals with access to the system were programmers with Information Technology Services who provide system support. While we concur, in general, system

support staff should have view-only access to production data, there are situations when it becomes necessary to grant them full access rights to perform global updates or other system maintenance. Accordingly, we have now restricted the access of these individuals, but temporary rights may need to be granted at some point in the future.

Every month, Payroll reviews a listing of individuals with systems access. This listing includes the employee termination date, if applicable. The exception noted was an oversight of an existing control. Access rights for this individual have since been removed.

Conclusion – Response accepted.

Application Controls

3) Hourly Timesheets – After employee timesheets are approved by their supervisor, the timesheets are entered on the Hourly Payroll System by a department employee. The following day, an email is sent from the centralized payroll department to each University department requesting verification of all payroll information. The last page of the verification is signed and returned to centralized payroll. The person who entered the payroll also performed the verification the following day for three of three departments reviewed. Also, the hourly rate paid did not agree with the timesheet rate for one individual and the hours were not properly entered for another employee.

Recommendation – An employee independent of the employee who originally entered the information should verify the timesheets entered on the Hourly Payroll System.

Response – We concur that ideally, the person who enters the hourly payroll information should not also verify the timesheets and will remind all departments this practice should be followed whenever possible. However, in some small departments with limited staff, other compensating controls may need to be utilized.

Conclusion – Response accepted.

4) Formal Procedures Manual – We encourage the development of an office procedures and standardized payroll manual for the centralized payroll department. The written manual should provide the following benefits.

   (1) Help in achieving uniformity in payroll and application of written policies and procedures.

   (2) Save supervisory time by recording decisions so they will not have to be made each time the same or similar situation arises.

   (3) Aid in training additional or replacement personnel.

Recommendation – A written office procedures and standardized payroll manual should be prepared.

Response – The Payroll Department has written procedures for most processes and is currently in the process of compiling these procedures into a manual.

Conclusion – Response accepted.

5) <u>Payroll Department Independent Review of Changes</u> – The centralized payroll department makes corrections to the payroll system. An independent person does not review these changes.

<u>Recommendation</u> – A person independent of the payroll change process should review all changes. Evidence of review should be indicated by initials of the independent reviewer.

<u>Response</u> – This recommendation has been implemented. Any corrections are reviewed and annotated by a second Payroll staff member.

<u>Conclusion</u> – Response accepted.

<u>Staff:</u>

Questions or requests for further assistance should be directed to:

    Erwin L. Erickson, CPA, Director
    Ernest H. Ruben, Jr., CPA, Manager
    Andrew E. Nielsen, CPA, Deputy Auditor of State

Other individuals who participated on this review include:

    Timothy D. Houlette, CPA, Senior Auditor II
    Philip J. Cloos, Staff Auditor
    Michael P. Piehl, Staff Auditor
    Jenny R. Schneider, Assistant Auditor