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 July 27, 2005 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 of Iowa, Human Resource Information System (HRIS) and payroll system for the period May 10, 2004 through June 4, 2004.

Vaudt recommended the Department take steps to implement the security program (including risk and vulnerability assessments), develop and implement procedures to improve information system access controls, establish program test standards, maintain copies of system and application documentation off-site, update and test the contingency plan, and improve segregation of duties.

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

###

REPORT OF RECOMMENDATIONS TO
IOWA DEPARTMENT OF ADMINISTRATIVE SERVICES
ON THE REVIEW OF GENERAL AND APPLICATION CONTROLS
OVER THE HRIS AND PAYROLL SYSTEMS

MAY 10, 2004 to JUNE 4, 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

June 24, 2005

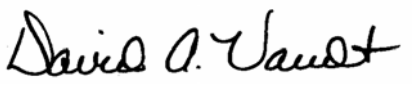
To Mollie Anderson, Director of the
Iowa Department of Administrative Services:

In conjunction with our audit of the financial statements of the State of Iowa for the year ended June 30, 2004, we have conducted an information technology review of selected general and application controls of the Iowa Department of Administrative Services for the period May 10, 2004 through June 4, 2004. Our review focused on selected general and application controls of the Department's Human Resource Information System (HRIS) and payroll system. The review was more limited than would be necessary to give an opinion on internal control. Accordingly we do not express an opinion on internal control or ensure all deficiencies in internal control are disclosed.

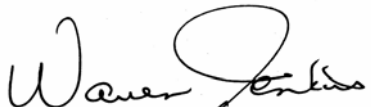
In conducting our review, we became aware of certain aspects concerning information technology controls for which we believe corrective action is necessary. As a result, we have developed recommendations which are reported on the following pages. We believe you should be aware of these recommendations which pertain to the Department's general and application controls over the HRIS and payroll systems. These recommendations have been discussed with Department 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 Iowa Department of Administrative Services, citizens of the State of Iowa, and other parties to whom the Iowa Department of Administrative Services 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 Iowa Department of Administrative Services 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 HRIS and payroll systems are listed on page 11, 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
Michael L. Tramontina, Director, Department of Management
Dennis C. Prouty, Director, Legislative Services Agency

HRIS, and Payroll Systems General and Application Controls

A. Background

The Human Resource Information System (HRIS) is the state-wide human resource system. The payroll system is the state-wide payroll system.

The HRIS and payroll systems were supported by the Information Technology Department for the Departments of Revenue and Finance and Personnel prior to July 1, 2003. On July 1, 2003 the Departments of Personnel, Information Technology, and the accounting function of the Department of Revenue and Finance were combined with the Department of General Services to form the new Department of Administrative Services (Department). The new Department is organized into four enterprises, the State Accounting Enterprise, General Services Enterprise, Human Resources Enterprise and Information Technology Enterprise.

Effective July 1, 2003, the Information Technology Enterprise maintains and supports the Payroll system for the State Accounting Enterprise and HRIS for the Human Resources Enterprise.

B. Scope and Methodology

In conjunction with our audit of the financial statements of the State of Iowa, we reviewed selected general and application controls in place over the Human Resource Information System (HRIS) and payroll system for the period May 10, 2004 through June 4, 2004. Specifically, we reviewed the following general controls: security program, access controls, application software development and change controls, system software controls, segregation of duties and service continuity; and the following application controls: input, processing and output controls. We interviewed staff from the Department and we reviewed Department 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 Department operations within the scope of our review. We developed an understanding of the Department'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 used our finite review resources to identify where and how improvements can be made. Thus, we devoted 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 Department's responses, are listed in the remainder of this report.

General Controls

(1) Security Program – An entity wide program for security planning and management is the foundation of an entity's security control and a reflection of senior management's commitment to addressing security risks. Such a program would establish a framework and continuing cycle of activity for assessing risk, developing and implementing effective security procedures, and monitoring the effectiveness of these procedures. Without a well designed program, security controls may be inadequate; responsibilities may be unclear, misunderstood, and improperly implemented; and controls may be inconsistently applied. Such conditions may lead to insufficient protection of sensitive or critical resources and disproportionately high expenditures for controls over low-risk resources.

An Electronic Enterprise Security Policy for the State of Iowa has been drafted but procedures have not been developed to implement the policy.

Recommendation – The Department should develop procedures and implement the Electronic Enterprise Security Policy.

Response – The Governor's Cyber Security Task Force recommendation to create an Information Security Office (ISO) separate from the Information Technology Enterprise with responsibility across the executive branch has been adopted. A Chief Information Security Officer (CISO) reporting directly to the Administrative Services Department Director has been hired. The new ISO has updated the Enterprise Information Security Policy and is working with departments, divisions and offices to develop an effective security program and implementation plan.

Conclusion – Response accepted.

(2) Risk Assessments – A comprehensive high-level risk assessment should be the starting point for developing or modifying an entity's security policies and program. Such assessments are important because they help make certain all threats and vulnerabilities are identified and considered, the greatest risks are identified, and appropriate decisions are made regarding which risks to accept and which to mitigate through security controls.

Risk assessments consider data sensitivity, the need for integrity and the range of risks an entity's systems and data may be subjected to, including those risks posed by authorized internal and external users, as well as unauthorized outsiders who may try to "break into" the systems.

The State of Iowa Electronic Enterprise Security Policy establishes the requirement that each department perform an information system risk assessment at least every two years following the assessment methodology developed by the Information Security Office.

A risk assessment methodology has not yet been developed or made available to departments and formal risk assessments have not been conducted.

Recommendation – A risk assessment methodology should be developed and made available to departments.

Response – The CISO and ISO are working collaboratively with agencies to develop peer-based risk and vulnerability assessment programs to assure effectiveness and sustainability. In those cases where peer-assisted assessments are appropriate, significant cost savings are possible. ISO staff has visited all agencies twice to discuss risk and needs as a pre-cursor to a formal analysis process and began discussions with the CIO Council Security Committee on development of an enterprise risk assessment tool. All agencies are to have risk assessments completed by November 1, 2005.

Conclusion – Response accepted.

(3) Security Officers – A security program generally consists of a core of personnel who are designated as security managers. These personnel play a key role in developing, communicating and monitoring compliance with security policies and reporting those activities to senior management.

The State of Iowa Electronic Enterprise Security Policy indicates Agency Security Officers should function as liaisons to the State Information Security Office.

Security Officers have not been identified for all agencies or departments.

Recommendation – The State Information Security Office should coordinate the identification and appointment of security officers for all agencies or departments.

Response – When the new ISO was established, each department, division or office provided a single point of contact (POC). The ISO worked through the POCs to communicate with the many different organizations while the office was being set up. All agencies are now being asked to name a security officer and alternate security officer, however, some organizations are too small to have staff meeting the requirements. The ISO is developing a communications plan adequate for security officers that will also provide appropriate information to non-security professionals. In addition, the ISO has drafted a plan for a Computer Security Incident Response Team (CSIRT) to react quickly to adverse cyber security incidents. The team will be led by the CISO and have representation from ITE, ICN, Homeland Security and Emergency Management and participating agencies on a rotating basis. A key role of the CSIRT will be communication of critical information in the event of a cyber security emergency.

Conclusion – Response accepted.

(4) Vulnerability Assessments – 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.

Vulnerability assessments have not been performed.

Recommendation – The Department should establish procedures to ensure annual vulnerability assessments are conducted for critical systems.

Response – The recently-approved Enterprise Information Security Policy requires each agency to perform an annual vulnerability assessment. However, many agencies do not have resources in this year's budget to conduct vulnerability assessments and they already have the risk assessment requirement. The CISO and ISO will work collaboratively with agencies to develop a peer-based vulnerability assessment program to assure effectiveness and sustainability. In those cases where peer-assisted assessments are appropriate, significant cost savings are possible. The ISO has set a target of all agencies to complete vulnerability assessments during FY06 and annually thereafter.

Conclusion – Response accepted.

(5) Access to Production Programs – The establishment of controls over the modification of application software programs helps to ensure only authorized programs and modifications are implemented. This is accomplished by instituting policies, procedures, and techniques that help make sure all programs and program modifications are properly authorized, tested and approved and that access to and distribution of programs is carefully controlled. Without proper controls, there is a risk security features could be inadvertently or deliberately "turned off" or processing irregularities or malicious code could be introduced.

Procedures have been established for the movement of programs into production, but the person modifying a program is not prevented from placing it back into production. Also, live data can be run against programs outside of the production library.

Recommendation – The Department should establish a build process for all production applications that does not permit unapproved code from being put into production.

Response – There were several issues identified, and I have addressed them individually.

- Person modifying a program is not prevented from placing it back into production.

  Online programs (IDMS or CICS) are not put into production without the involvement of someone outside of applications development, usually from database team or Software Support. All program changes are first loaded to the staging library before being moved to production. For all program changes (online and batch), we review test results with the customer, usually DAS/HRE or DAS/SAE, and obtain their approval before putting the modified code into production.

- Live data can be run against programs outside of the production library.

  We create test files that are copies of the production data in order to test more effectively. We do not do updates against batch production files in our testing. For online HRIS changes, we do use the shadow database, which is a copy of the production database, to test changes.

- Establish a building process for all production applications that does not permit unapproved code from being put into production.

  With these systems to be transitioned from their current platforms to the I/3 system by the end of calendar year 2005, it seems more efficient to make sure appropriate procedures are in place for that platform.

Conclusion – Responses acknowledged. Current practices involve someone outside of applications development but do not appear to prevent a programmer from accessing the staging library.

(6) Program Test Standards – A disciplined process for testing and approving new and modified programs prior to implementation is essential to make sure programs operate as intended and unauthorized changes are not introduced. Authorized changes are to be written into the program code and tested in a disciplined manner. Because testing is an interactive process generally performed at several levels, it is important the entity adhere to a formal set of procedures or standards for prioritizing, scheduling, testing and approving changes.

System and program testing standards have not been formalized or approved for all levels of testing that define responsibilities for each party.

Recommendation – The Department should formally adopt testing standards and identify at what levels testing is required.

Response – Staff size has previously prevented the establishment of a dedicated test organization. That is changing and the applications division is in the process of creating a test/quality assurance team. This organization will establish appropriate testing standards and procedures for all platforms and applications.

Conclusion – Response accepted.

(7) Management Review – One technique used to ensure compliance with established policies and standards is for data center management and/or security administrators to periodically review production program changes to determine whether access and change control procedures have been followed.

Production program changes are not periodically reviewed to determine if access and change controls have been followed.

Recommendation – The Department should develop policies to ensure production program changes are periodically reviewed to determine if access and changes controls have been followed.

Response – ITE management review and approve all change control requests prior to their implementation.

Conclusion – Response acknowledged. Periodic reviews after implementation help to ensure compliance with established procedures.

(8) System Software Access – Controls over access to and modification of system software and system software utilities are essential in providing reasonable assurance operating system-based security controls are not compromised. Access to system software and sensitive software utilities is to be restricted to a very limited number of personnel whose job responsibilities require they have access and security software should be even more tightly controlled.

A review of access rights to system software indicated:

- Two employees with RACF "Special" attribute had their password interval set to "No Interval". As a result, the system will not force them to change their password periodically.
- Twenty-three employees had access to the "Special" attribute in RACF. Nineteen did not appear to require that level of access.

- Two employees had two user ID's that allowed them to access all data sets and system software. This level of access is not necessarily needed for the employees' second ID.

- Two employees with access to system software database utilities have changed job duties and no longer need this level of access.

- System programmers access capabilities are not periodically reviewed to ensure their access corresponds to current job duties.

Recommendation – The Department should develop procedures to periodically review access to system software, system utilities and RACF attributes to ensure appropriate controls are maintained.

Response – ITE agrees with this recommendation and has a program underway that is making numerous improvements. Appropriate access to help desk personnel in resetting passwords has been reviewed. ITE is in the process of evaluating a "self-service" tool for password resets. The practice of sharing passwords has ended and this has improved our ability to track who performed any given task. Our RACF Administrator attended formal training to better enable us to evaluate and improve settings that control security. The training, Developing Effective RACF Administration Skills, was attended on September 15-19, 2003. In addition, the DAS Security Office has taken a lead in drafting policy and procedures that control and define access to sensitive system utilities.

Conclusion – Response accepted.

(9) Segregation of Duties – Work responsibilities should be segregated so one individual does not control all critical stages of a process. For example, one computer programmer should not be allowed to independently write, test and approve program changes. Dividing duties among two or more individuals or groups diminishes the likelihood errors and wrongful acts will go undetected because the activities of one group or individual will serve as a check on the other.

System design, application programming and quality assurance/testing are not performed by different individuals or groups. These functions are performed by the assigned team.

Recommendation – Duties should be segregated to the extent possible and policies outlining the responsibilities of groups and related individuals should be documented, communicated and enforced.

Response – Due to the severe limitations on staffing levels, the appropriate separation of these duties has not been practical. With the payroll system having been transitioned to the I/3 platform, and the HR system transition planned by the end of 2005, these issues should be addressed. The I/3 platform was developed by a 3rd party vendor. Some customization will be done by state staff in the I/3 group. Systems programming will be done by the Infrastructure and Database groups and testing should be the responsibility of the new Test group. Once the transition of the systems is complete, delineation of responsibilities will be done.

Conclusion – Response accepted.

(10) Off-site Storage – Routinely copying data files and software and securely storing these files at a remote location are usually the most cost-effective actions an entity can take to mitigate service interruptions. The Department has established procedures and maintains backup data sets at a separate off-site location, but copies of system and application documentation are not maintained at the off-site storage location.

Recommendation – The Department should develop procedures to maintain copies of system and application documentation at the off-site storage location.

Response – As the COOP/COG state planning effort is completed, copies of the planning materials will be stored at the state off site storage location and at the vendor location. Additionally, Networking Services monthly backups, a CD of all IP addresses and other necessary networking documentation is created on a monthly basis and stored both at the vendor location and at the off site storage location.

Conclusion – Response accepted.

(11) Contingency Plan – Losing the capability to process, retrieve and protect information maintained electronically can significantly affect an entity's ability to accomplish its mission. A contingency plan would include: (1) procedures to protect information resources and minimize the risk of unplanned interruptions and (2) a plan to recover critical operations should interruptions occur. The Department developed a contingency plan for data processing center recovery in the event of a disaster but this plan has not been formally adopted by senior program managers or tested and emergency processing priorities have not been documented.

Recommendation – The Department should update, adopt, distribute and test a contingency plan.

Response – ITE has gathered requirements to upgrade the offsite recovery location and is in the process of completing the renovation. The Hoover data center mainframe and the offsite mainframe are now able to share Medicaid data back and forth in test. Production is scheduled for July 1, 2005. Servers are also housed at Hoover and some servers are now located at offsite locations. Beginning July 1, 2005 the renovation will be complete and the server farm disaster recovery site will be fully operational.

Conclusion – Response accepted.

Application Controls

No recommendations were noted in our review of application controls for the Department's HRIS and payroll systems.

Staff:

Questions or requests for further assistance should be directed to:

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

Other individuals who participated on this review include:

Elvir Alicic, Staff Auditor
Jodi Simon, Staff Auditor
Cory A. Warmuth, CPA, Staff Auditor