

**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 \_\_\_\_\_ September 13, 2011

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 Iowa Department of Administrative Service's (DAS) Human Resource Information System (HRIS), Payroll, Integrated Information for Iowa (I/3) and E-Payment Engine Systems for the periods April 13, 2009 through May 15, 2009 and April 5, 2010 through May 7, 2010.

Vaudt recommended the Department establish additional security policies to limit physical access to the Data Center/Server Farm, implement change control procedures to ensure activity is monitored and program changes are approved before placed into production, perform a periodic review of server builds and improve HRIS segregation of duties.

A copy of the report is available for review at the Iowa Department of Administrative Services, in the Office of Auditor of State and on the Auditor of State's web site at <http://auditor.iowa.gov/reports/1160-8990-BI06.pdf>.

###

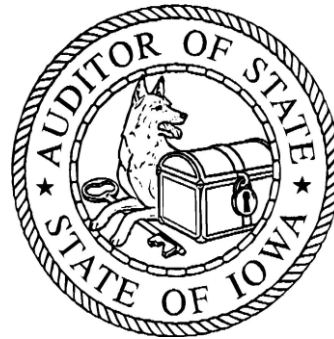


**REPORT OF RECOMMENDATIONS TO THE  
IOWA DEPARTMENT OF ADMINISTRATIVE SERVICES  
ON A REVIEW OF SELECTED GENERAL  
AND APPLICATION CONTROLS OVER THE HUMAN  
RESOURCE INFORMATION SYSTEM (HRIS), PAYROLL,  
INTEGRATED INFORMATION FOR IOWA (I/3)  
AND E-PAYMENT ENGINE SYSTEMS**

**April 13, 2009 THROUGH MAY 15, 2009 AND  
APRIL 5, 2010 THROUGH MAY 7, 2010**

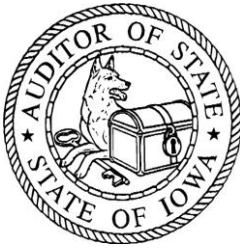
Office of  
**AUDITOR  
OF STATE**

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

August 10, 2011

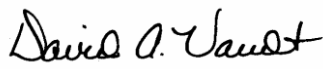
To Michael R. Carroll, Director of the  
Iowa Department of Administrative Services:

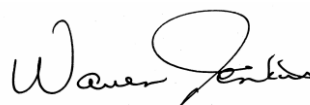
In conjunction with our audit of the financial statements of the State of Iowa for the years ended June 30, 2009 and June 30, 2010, we conducted an information technology review of selected general and application controls over the Iowa Department of Administrative Services' (DAS) Human Resource Information System (HRIS), Payroll, Integrated Information for Iowa (I/3) and E-Payment Engine Systems for the periods April 13, 2009 through May 15, 2009 and April 5, 2010 through May 7, 2010. Our review focused on the general and application controls of the HRIS, Payroll, I/3 and E-Payment Engine Systems 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 Department's general and application controls over the HRIS, Payroll, I/3 and E-Payment Engine Systems. These recommendations have been discussed with Department personnel and their responses to these recommendations are included in this report. While we have expressed our conclusions on the Department's responses, we did not audit the Department'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 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, Payroll, I/3 and E-Payment Engine Systems 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 Terry E. Branstad, Governor  
David Roederer, Director, Department of Management  
Glen P. Dickinson, Director, Legislative Services Agency

## **HRIS, Payroll, I/3 and E-Payment Engine Systems General and Application Controls**

### **A. Background**

The Human Resource Information System (HRIS) is the state-wide human resource system used to manage the qualification of applicants, employee classifications, time reports, compensation, benefits, leave, performance, training and development. The Payroll system is the state-wide system used to process the bi-weekly payroll. The Integrated Information for Iowa (I/3) system is the State Enterprise Resource Planning System. I/3 supports the State's financial processes such as accounts payable, accounts receivable, general accounting and budget preparation. The E-Payment Engine is used by departmental e-commerce websites to accept and process electronic payments.

### **B. Scope and Methodology**

In conjunction with our audits of the financial statements of the State of Iowa, we reviewed selected aspects of the general and application controls in place over the Department of Administrative Services' (DAS) HRIS, Payroll, I/3 and E-Payment Engine Systems for the periods April 13, 2009 through May 15, 2009 and April 5, 2010 through May 7, 2010. Specifically, we reviewed the overall general controls: security management and contingency planning; the mainframe general controls: access controls, change controls, system software and segregation of duties; and the server platform general controls: access controls, configuration management and segregation of duties. For HRIS and Payroll, we reviewed the application controls: data input, data processing, data output and master data controls. For I/3, we reviewed the application controls: access controls, configuration management, segregation of users, data input, data processing, data output, master data and data management system controls. For the E-Payment Engine, we reviewed compliance with selected parts of the Payment Card Industry (PCI) Data Security Standard. We interviewed staff of 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.

April 13, 2009 through May 15, 2009 and April 5, 2010 through May 7, 2010

**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 detailed in the remainder of this report.

**Mainframe (HRIS/Payroll) General Controls:**

- (1) Data Center Physical Access – Physical access to the Department of Administrative Services – Information Technology Enterprise Data Center/Server Farm is controlled by access cards. On April 28, 2010, there were 257 active access cards with level 7 or level 77 access (master key access) giving the holder 24 hour access 7 days a week. Many of these employees have no reason to need access to the Data Center/Server Farm. Seven of those individuals retired prior to April 28, 2010 and a number were third party vendors or contractors.

Recommendation – Physical access should be limited to only those who need access to perform their job duties. DAS should also consider removing the Data Center/Server Farm from the master key level access group.

Response – DAS-ITE intends to limit access to the Data Center/Server Farm to approved DAS-ITE staff and approved State Employees (this will include the designated custodial staff provided they have met the confidentiality requirements). We intend to work with Post 16 to have the Data Center/Server Farm removed from level 77 and to have a new level added. The new level of access to the Data Center/Server Farm will be limited to Post 16 staff. Anyone who does not have access to the Data Center/Server Farm but needs to enter must sign the visitor log, wear a visitor badge or a State ID and be escorted into the area. The escorted individuals will continue to be monitored throughout the visit by cameras in the area. When the visitor leaves the area, the visitor will sign out of the visitor log and return the visitor badge.

Quarterly, the Information Security Officer (ISO) or designee will review the access lists provided by Post 16 and determine if anyone should be removed from the list. If a person should be removed, the ISO or designee will contact Post 16 to restrict the person's access.

Conclusion – Response accepted.

- (2) Change Control Segregation of Duties – Analysts and programmers who make changes to programs can also move the programs back into production without management approval. Also, production program changes are not periodically reviewed by management to ensure access control and change control policies are followed.

Recommendation – ITE should establish procedures to ensure changes to production programs are properly approved and unauthorized changes cannot be made without being detected. Data Center management should periodically review changes to production programs to ensure access control and change control policies are followed.

April 13, 2009 through May 15, 2009 and April 5, 2010 through May 7, 2010

Response – DAS-ITE will use Panvalet or a similar product to track changes made to mainframe code; for non-mainframe applications we will use GForge or a similar versioning/code repository tool. To ensure segregation of duties an employee, other than the one who generated the code, will put it into production. In addition, production changes will be reviewed and tracked through the DAS-ITE Change Advisory Board (CAB) process. This will allow us to track changes and ensure the necessary management approvals are secured before moving code to production.

Conclusion – Response accepted.

**I/3 Server General Controls:**

Server Build Review – The ITE AIX Server Build Guide V1.0 requires periodic port audits to be performed as well as periodic reviews of SUID and SGID files. Currently, port audits are not being done unless major changes to the build have been made and there is no evidence of the review of SUID and SGID files.

Recommendation – As required by the build guide, port audits and a review of SUID and SGID files should be done periodically. Documentation should also be retained to demonstrate each review was performed.

Response – DAS-ITE will automate a process to scan ports daily; a baseline is being established from the initial scan which will be used to identify any anomalies/concerns. Results of the daily scan will automatically be sent to the Server Team and to the ISO for review. In addition, a script will run daily which will report any changes in SUID/SGID files. The report documenting changes in SUID/SGID files will be sent to the Server Team and the ISO for review and handling.

Conclusion – Response accepted.

**HRIS/Payroll Application Controls:**

Segregation of Duties for HRIS P-1's – The HRIS application does not adequately separate user functions. Staff from a number of Departments or Agencies can initiate personnel actions (P-1's) as the Personnel Assistant (PA) and also apply the Departmental Approval. This could result in payroll changes with only one person's knowledge or approval.

Recommendation – The HRIS application should be modified to prevent the same person from initiating a P-1 and also approving it.

Response – The HRIS system requires approval at both the PA and Department level. Most departments have separate persons apply the approval at each level. If individual departments will provide separate persons for each level, DAS will set them up separately in the HRIS security system. This would not require any modification to the HRIS application.

Conclusion – Response acknowledged. PA and Departmental approval of a P-1 should not be allowed by the same individual.



Report of Recommendations to the Iowa Department of Administrative Services

April 13, 2009 through May 15, 2009 and April 5, 2010 through May 7, 2010

**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:

Michael J. Hackett, Senior Auditor  
Ainslee M. Barnes, Staff Auditor  
Tracey L. Gerrish, Staff Auditor