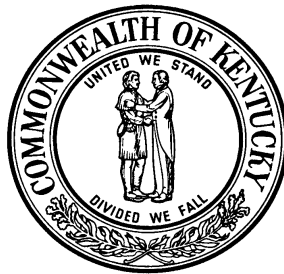


**KENTUCKY TEACHERS' RETIREMENT SYSTEMS
REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING
AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN AUDIT
OF FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE
WITH *GOVERNMENT AUDITING STANDARDS***

**For The Fiscal Year Ended
June 30, 2014**



**ADAM H. EDELEN
AUDITOR OF PUBLIC ACCOUNTS
www.auditor.ky.gov**

**209 ST. CLAIR STREET
FRANKFORT, KY 40601-1817
TELEPHONE (502) 564-5841
FACSIMILE (502) 564-2912**

CONTENTS

PAGE

TRANSMITTAL LETTER.....	1
REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN AUDIT OF FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH <i>GOVERNMENT AUDITING STANDARDS</i>	5
SCHEDULE OF FINDINGS AND RECOMMENDATIONS	9



ADAM H. EDELEN
AUDITOR OF PUBLIC ACCOUNTS

Board of Trustees
Kentucky Teachers' Retirement Systems
Frankfort, Kentucky

As Auditor of Public Accounts, I am pleased to transmit herewith our Kentucky Teachers' Retirement Systems' Report On Internal Control Over Financial Reporting And On Compliance And Other Matters Based On An Audit Of Financial Statements Performed In Accordance With *Government Auditing Standards* for the year ended June 30, 2014. This report contains financial statement findings identified during our audit of the Kentucky Teachers' Retirement Systems as well as the Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*.

On behalf of the Office of Financial Audits of the Auditor of Public Accounts, I wish to thank the employees of the Kentucky Teachers' Retirement System for their cooperation during the course of our audit. Should you have any questions concerning this report, please contact Libby Carlin, Assistant Auditor of Public Accounts.

Respectfully submitted,

Adam H. Edelen
Auditor of Public Accounts



**REPORT ON INTERNAL CONTROL OVER FINANCIAL REPORTING
AND ON COMPLIANCE AND OTHER MATTERS BASED ON AN AUDIT OF
FINANCIAL STATEMENTS PERFORMED IN ACCORDANCE WITH
*GOVERNMENT AUDITING STANDARDS***



ADAM H. EDELEN
AUDITOR OF PUBLIC ACCOUNTS

Report On Internal Control Over Financial Reporting And
On Compliance And Other Matters Based On An Audit Of Financial
Statements Performed In Accordance With *Government Auditing Standards*

Independent Auditor's Report

Board of Trustees
Kentucky Teachers' Retirement System
Frankfort, Kentucky

We have audited, in accordance with the auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States, the financial statements of the Kentucky Teachers' Retirement System (KTRS) as of and for the year ended June 30, 2014, and the related notes to the financial statements, which collectively comprise the KTRS' basic financial statements, and have issued our report thereon dated December 15, 2014.

Internal Control Over Financial Reporting

In planning and performing our audit of the financial statements, we considered the KTRS' internal control over financial reporting (internal control) to determine the audit procedures that are appropriate in the circumstances for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the KTRS' internal control. Accordingly, we do not express an opinion on the effectiveness of the KTRS' internal control.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control, such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. A *significant deficiency* is a deficiency, or a combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.

Our consideration of internal control over financial reporting was for the limited purpose described in the first paragraph of this section and was not designed to identify all deficiencies in internal control that might be material weaknesses or significant deficiencies and therefore, material weaknesses or significant deficiencies may exist that were not identified. Given these limitations, during our audit we did not identify any deficiencies in internal control that we consider to be material weaknesses.



Report On Internal Control Over Financial Reporting And
On Compliance And Other Matters Based On An Audit Of Financial
Statements Performed In Accordance With *Government Auditing Standards*
(Continued)

We did identify certain deficiencies in internal control, described in the accompanying schedule of findings and recommendations that we consider to be significant deficiencies as items 2014-KTRS-01, 2014-KTRS-02, 2014-KTRS-03, 2014 KTRS-04, 2014-KTRS-05, and 2014-KTRS-06.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the KTRS' financial statements are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit and, accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

KTRS' Response to the Findings and Recommendations

KTRS' responses to the findings identified in our audit are described in the accompanying schedule of findings and recommendations. KTRS' responses were not subjected to the auditing procedures applied in the audit of the financial statements and, accordingly, we express no opinion on them.

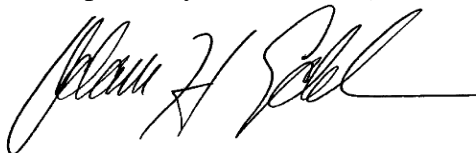
Additional Management Communication

We noted certain matters that we have reported to management of the KTRS' in a separate letter dated December 15, 2014.

Purpose of this Report

The purpose of this report is solely to describe the scope of our testing of internal control and compliance and the result of that testing, and not to provide an opinion on the effectiveness of the entity's internal control or on compliance. This report is an integral part of an audit performed in accordance with *Governmental Auditing Standards* in considering the entity's internal control and compliance. Accordingly, this communication is not suitable for any other purpose.

Respectfully Submitted,



Adam H. Edelen
Auditor of Public Accounts

December 15, 2014

SCHEDULE OF FINDINGS AND RECOMMENDATIONS

KENTUCKY TEACHERS' RETIREMENT SYSTEMS
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014

2014-KTRS-01: KTRS Did Not Properly Calculate and Post Compensatory Leave Time

During the FY14 audit of Kentucky Teachers' Retirement System (KTRS), employee timesheets were tested for proper posting of compensatory leave time earned. Employees accumulate compensatory leave at the rate of one and one half hours for every hour worked in excess of 40 hours per work week. The testing revealed compensatory leave was awarded incorrectly. Three issues were noted:

1. Employees using compensatory time during the work week did not receive compensatory time and a half if more than 40 hours were physically worked in total during the week. For example, based on the KTRS application of the policy, an employee using eight hour of compensatory time on one day and working 10 hours over during the rest of the work week only received 10 hours and should have received 11 hours. By not receiving comp time and a half, Federal policy is violated.
2. Employees using other types of leave, such as annual or sick, received compensatory time and a half if their hours totaled over 40, even if less than 40 hours were physically worked in total during the week. For example, an employee who used eight hours of annual time and then worked 10 hours over during the same work week received time and a half for the entire 10 hours worked over, or 15 hours, even though only 42 hours were physically worked. The employee should have only earned time and a half for any hours physically worked over 40, or 3 hours in this example, instead of 15 hours.
3. Compensatory time and a half was awarded based upon pay period instead of the seven day work week. For example, if an employee worked 2 hours overtime on Monday and the pay period ended on Wednesday, the employee received compensatory time and a half for those 2 hours, even if 2 hours compensatory leave was used on Friday. The employee would have earned 2 under KTRS' policy interpretation, when the employee should have earned zero hours since the same amount worked was taken off during the same work week.

Payroll for six of the 24 pay periods were tested during FY14 and errors were identified on each payroll for the calculation of compensatory time. The total difference between the compensatory time earned and the compensatory time awarded resulted in a net posting of 46.68 hours more than what should have been posted. The difference varied by individual so some employees received more compensatory time than they were due and others less.

Insufficient training of KTRS staff members responsible for payroll led to the miscalculation of compensatory hours earned causing employees hours earned or paid to be either over or understated for approximately the past two years.

In the case of overstating of compensatory leave time, employees may owe hours to KTRS. The employees could have already used that time and KTRS would be unable to recoup the excess in compensatory hours given to the employee. In the case of understating compensatory leave, Federal law

KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)

2014-KTRS-01: KTRS Did Not Properly Calculate and Post Compensatory Leave Time
(Continued)

requires employers to pay time and a half to employees who work in excess of 40 hours in a seven day work week period therefore by incorrectly calculating compensatory leave; KTRS is not in compliance with federal regulations.

Excessive over- or under-payments of overtime could cause a misstatement of the financial statements, though no material misstatements were noted. Expenses for compensatory time are recorded in the financial statements when earned by the employees.

KTRS' misapplied the employee overtime compensation policy and this resulted in noncompliance with federal regulations. The KTRS' Employee Handbook states:

If you are paid by the hour or perform "non-exempt" duties, you will be paid for the hours worked up to and including forty (40) hours in the week. You will receive compensatory time for hours worked beyond forty (40) in a work week, and you will be entitled to either paid time at one and one-half time your regular rate of pay or you will receive compensatory leave at one and one-half hours for each hour worked over (40) hours.... When you use your compensatory leave time during the same week you earn it, it does not count as "hours worked" for figuring overtime compensation.

Code of Federal Regulations (CFR) §778.110 Hourly rate employee states:

Earnings at hourly rate exclusively. If the employee is employed solely on the basis of a single hourly rate, the hourly rate is the "regular rate." For overtime hours of work the employee must be paid, in addition to the straight time hourly earnings, a sum determined by multiplying one-half the hourly rate by the number of hours worked in excess of 40 in the week.

29 United States Code section 207 (o) Compensatory time states:

- (1) Employees of a public agency which is a State, a political subdivision of a State, or an interstate governmental agency may receive, in accordance with this subsection and in lieu of overtime compensation, compensatory time off at a rate not less than one and one-half hours for each hour of employment for which overtime compensation is required by this section.

**KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)**

**2014-KTRS-01: KTRS Did Not Properly Calculate and Post Compensatory Leave Time
(Continued)**

Recommendation

We recommend KTRS:

- Provide additional training to KTRS staff members responsible for payroll regarding computing compensatory leave correctly.
- Review compensatory balances for employees and determine if adjustments to an individual employee's time is necessary.

Management's Response and Corrective Action Plan

KTRS staff members responsible for payroll have received additional training regarding computing compensatory leave time. In November 2014, KTRS initiated adjustments to accruals of compensatory leave time for employees. The KTRS Executive Secretary reviewed and initiated adjustments to accruals of compensatory leave time for employees.

**KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)**

2014-KTRS-02: KTRS Did Not Adequately Segregate Duties For The Payroll Process

During the FY14 audit of Kentucky Teachers' Retirement System, the employee payroll process was reviewed. The payroll clerk prepares the payroll and submits hardcopies of the payroll reports to the executive secretary for approval. Once the payroll is approved by the executive secretary, the payroll reports are returned to the payroll clerk for submission into the electronic payroll system. There is no review or reconciliation after the clerk submits the payroll. A segregation of duties issue exists because the payroll clerk prepares and submits the payroll in the electronic system.

Without segregation of the preparation and submission duties for employee payroll, the amount of pay, overtime hours, or leave hours could intentionally or unintentionally be altered in the electronic payroll system after approval by the executive secretary.

The objective of segregation of duties is to ensure job duties are separated so no one employee is in a position both to commit and conceal errors while performing their job duties. Adequate segregation of duties reduces the likelihood that errors, either intentional or unintentional, will remain undetected. This is carried out by providing for separate processing by different individuals at various stages of a transaction and by independent reviews of the work performed.

Recommendation

We recommend KTRS consider:

- Segregating the duties of preparing payroll from the submission of payroll by requiring an independent manager to submit payroll in the electronic payroll system.
- Implementing a reconciliation to ensure the pay amounts, overtime hours, and leave hours approved are also the amounts submitted in the electronic payroll system.

Management's Response and Corrective Action Plan

KTRS employee payroll functions are administered through a web based electronic payroll system. The system includes rigorous security controls and an audit log of entries and adjustments to pay amounts, leave time used or accrued, and other transactions. Payroll reports approved by the Executive Secretary are reconciled monthly to the General Ledger. Additionally, beginning in November 2014, payroll reports approved by the Executive Secretary, including leave time used or accrued, and other transactions, will be reconciled to the electronic payroll system. Implementation of these enhanced reconciliation processes will provide adequate internal controls to ensure that correct data is maintained in the payroll system. The KTRS Executive Secretary will perform the reconciliation of payroll.

**KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)**

2014-KTRS-03: The Procurement Process Is Not Adequately Documented And Contracts Are Not Adequately Monitored

During the FY14 audit of Kentucky Teachers' Retirement System (KTRS), the procurement process was reviewed relating to KTRS' administrative expenses especially as it relates to contract awards and monitoring. For the purposes of this finding, the APA defines a contract as a signed written agreement between KTRS and one or more parties for the purchase of goods, supplies, or services. The procurement process had several internal control concerns:

- There are no written policies related to tracking and monitoring individual contracts, or for ensuring that contracts containing spending limits are not overspent. KTRS does not maintain a list or log of all contracts awarded, date awarded, contract period, dollar limit (if applicable), and the amount spent. Also, its accounting system does not have, as a compensating control, built-in functions to prevent expenditures from exceeding contract limits.
- Three of seven contracts reviewed were signed and executed by the Executive Director after each contract's effective date.

There are no written policies with regard to the process of contract awarding and monitoring the contract after the award. The contracts are not tracked and monitored through a central location. Although the majority of the contracts reviewed did not have a spending limit, there is no mechanism for determining if the contract terms were followed and/or if any contract limits were exceeded.

KRS 161.340(3) states:

The board shall contract for actuarial, auditing, legal, medical, investment counseling, and other professional or technical services, and commodities, as are required to carry out the obligation of the board in accordance with the provisions of this chapter without limitation, including KRS Chapters 12, 13B, 45, 45A, 56, and 57, and shall provide for legal counsel and other legal services as may be required in defense of trustees, officers, and employees of the system who may be subjected to civil action arising from the performance of their legally assigned duties if counsel and services are not provided by the Attorney General.”

Good internal controls dictate KTRS establish written policies to issue, track, and monitor contracts. This ensures contracts are properly awarded, tracked, and monitored; thus, all contractual payments relate to valid contracts.

KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)

2014-KTRS-03: The Procurement Process Is Not Adequately Documented And Contracts Are Not Adequately Monitored (Continued)

Recommendation

We recommend KTRS:

- Document the procurement award process in the policy and procedure manual.
- Implement written procedures for tracking contracts, such as manually via an excel spreadsheet or using the capabilities in eMARs.

Management's Response and Corrective Action Plan

No contract is issued by KTRS unless authorized by the Board of Trustees directly or through the administrative budget process. No contract is paid by KTRS unless authorized by the KTRS Executive Secretary, the KTRS Deputy Executive Secretary of Operations, or the KTRS Deputy Executive Secretary of Finance and Administration. Contracts are tracked and monitored through the office of the KTRS Executive Secretary. Any contract limits or administrative budget limits on contracts are carefully monitored by the KTRS Executive Secretary, the KTRS Deputy Executive Secretary of Operations, and the KTRS Deputy Executive Secretary of Finance and Administration. Any substantive changes in authorized contracts are reported to the Board of Trustees. Contracts are issued and paid subject to fiduciary duty, which is the highest obligation under law. However, consistent with the recommendation, KTRS will adopt a policy reflecting current procurement processes and monitoring procedures for contracts for fiscal year 2016 and thereafter. The KTRS Deputy Executive Secretary of Finance and Administration is responsible for documenting procurement processes and monitoring procedures for contracts.

**KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)**

2014-KTRS-04: The Employer Wages And Contributions In KTRS Computer System Were Not Reconciled To The Employer's Payroll Reporting System

Employers and employees make contributions to the Kentucky Teachers' Retirement System (KTRS) based on gross wages. Employers submit wage and contribution information to KTRS using the Pathway system, which was implemented at the beginning of FY14. The employers maintain separate payroll reporting systems for handling the employers' payroll information, including employee wages and employer contributions for each employee.

During the FY14 audit of KTRS, contributions from the employer's payroll reporting system for 22 employers were compared to KTRS' Pathway system to ensure accurate reporting of the employer and employee contributions. As of September 29, 2014, the employer gross wages, and employee and employer contributions from the employer's payroll reporting system did not agree to Pathway for 18 of the 22 employers. KTRS did not have a process in place and functioning to reconcile Pathway contribution information to the member employers' records at June 30, 2014. Throughout the audit, attempts were made to reconcile selected KTRS and the employer information. During this time, differences between employee contributions, employer contributions, and wages for the 22 employers selected for testing fluctuated in aggregate between \$285,809 and \$3,250,556. Reconciliations of Pathway and employer information would have identified the variances and provided KTRS the opportunity to resolve the variances and thus ensure the accuracy of contributions in a timely manner.

Prior to the implementation of Pathway, employers had been required to submit contributions within 15 days after the pay date with an annual reconciliation detailing the employees and their wages before August 1st following the fiscal year end. Thus, employers had the option to hold all reporting (not payments) until July, or report on a monthly basis or any other desired timeframe. When KTRS implemented Pathway which allowed for timelier reporting of member and employer contributions, employers could submit data files with each payroll. In FY14, KTRS did not initiate the annual reconciliation process until September 2014.

Due to the lack of timely reporting and reconciliation requirements, the participating employers have not reconciled payroll records to KTRS' system. Without reconciliation between employers and Pathway, a misstatement of contributions and contributions receivable on the financial statements could occur.

According to KRS 161.560:

- (1) Each agency employing members of the retirement system shall deduct from the compensation of each member for each payroll period subsequent to the date the individual became a member, the percentage of his compensation due under the rates prescribed in KRS 161.540. No later than fifteen (15) days following the end of each payroll period, the agency shall forward all amounts deducted to the Teachers' Retirement System.

**KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)**

2014-KTRS-04: The Employer Wages And Contributions In KTRS Computer System Were Not Reconciled To The Employer's Payroll Reporting System (Continued)

According to KRS 161.643:

Each school district and agency employing annuitants of the retirement system shall maintain a record of the days employed and the compensation paid to each annuitant and submit an annual report on forms prescribed by the retirement system no later than August 1, following the completion of each fiscal year.

Recommendation

We recommend KTRS:

- Ensure Pathway records are reconciled to employer and employee contribution records by August 31st of each year. KTRS should consider performing a quarterly or monthly reconciliation. This could make an annual reconciliation easier.
- Review Kentucky Revised Statute for reporting of contributions in light of the capabilities of the new computer system.

Management's Response and Corrective Action Plan

Employer reporting through the KTRS Pathway System began in July 2013. Employers have overwhelmingly reported positive experiences using the KTRS Pathway System. Using the Pathway System, KTRS reconciled contributions for employers each pay period during the fiscal year. In September 2014, KTRS undertook additional reconciliation measures to confirm individual member service credit earned during the fiscal year. In future years, because of planned enhancements to the payroll systems of employers, and modifications to the KTRS Pathway System, additional reconciliation measures should be unnecessary.

During the 2015 regular session of the Kentucky General Assembly, KTRS will recommend appropriate amendments to KRS 161.560 and KRS 161.643 to reflect the enhanced capabilities of the Pathway System and particular needs of participating employers. The KTRS Executive Secretary is responsible for presenting the Board of Trustees legislative recommendations to the General Assembly.

**KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)**

2014-KTRS-05: The Kentucky Teachers' Retirement System Did Not Adequately Protect Sensitive And Confidential Data

Our fiscal year 2014 audit revealed weaknesses in the Kentucky Teachers' Retirement System (KTRS) internal controls involving the security of confidential and sensitive data. We are aware KTRS has taken steps to strengthen security over certain types of data and is evaluating risk analysis tools that will assist with data protection; however, discussions with the agency revealed not all KTRS member data was adequately protected from potential intentional or unintentional access or misuse of information.

Detailed information that could potentially increase the risk of agency security being compromised was intentionally omitted from this comment. However, the auditors thoroughly discussed this issue to KTRS staff.

KTRS has not established adequate procedures to classify and ensure the protection of sensitive and confidential data.

Failure to adequately protect data increases the risk that Personally Identifiable Information (PII) or other sensitive and confidential data could be accessed or made available to the general public, which could compromise information related to members, employees, or vendors. This control weakness could potentially be exploited either internally or externally.

Sensitive and confidential data should be protected from unauthorized internal or external users or from exposure to the general public. The National Institute of Standards and Technology Publication 800-111 states, "[m]any threats against end user devices could cause information stored on the devices to be accessed by unauthorized parties. To prevent such disclosures of information, particularly of personally identifiable information (PII) and other sensitive data, the information needs to be secured."

Kentucky Revised Statute 161.585 states:

- (2) Each member's account shall be administered in a confidential manner and specific data regarding a member shall not be released for publication unless authorized by the member; however, the board of trustees may release member account information to the employer or to other state and federal agencies as it deems necessary or in response to a lawful subpoena or order issued by a court of law.

The Health Insurance Portability and Accountability Act of 1996 (HIPAA) Security Rule, located within the Code of Federal Regulations (CFR) at 45 CFR Part 164 Subpart C states:

§ 164.308 Administrative safeguards.

(a) A covered entity must, in accordance with § 164.306:

- (1) (i) Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.

KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)

2014-KTRS-05: The Kentucky Teachers' Retirement System Did Not Adequately Protect Sensitive And Confidential Data (Continued)

(ii) Implementation specifications:

(A) **Risk analysis** (Required). Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity.

(B) **Risk management** (Required). Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a).

(C) **Sanction policy** (Required). Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity.

(D) **Information system activity review** (Required). Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.

Recommendation

We recommend KTRS ensure confidential and sensitive data is sufficiently protected. Management should ensure sufficient resources are dedicated to address this weakness in a timely manner and ensure the maintenance of confidential and sensitive data remains a top priority. Further, we recommend KTRS management create an agency policy regarding data protection to, at a minimum, comply with applicable statutes and HIPAA, and reflect the actions and tools implemented by the agency. Once developed, the policy should be distributed to all staff to ensure they are aware of their responsibility in relation to agency security requirements.

Management's Response and Corrective Action Plan

The KTRS Pathway System will be substantially completed by July 1, 2015. The Pathway System will include appropriate protection and segregation of confidential and sensitive data. Preparation, consolidation, and revision of policies concerning protection and segregation of confidential and sensitive data, which reflect the actions and tools included in the KTRS Pathway System, will be completed by July 1, 2015. KTRS will also conduct staff training on the policies by July 1, 2015.

Concerning the legacy system, KTRS's confidential and sensitive data will be maintained under existing security procedures until the system is decommissioned beginning in January 2015. Hard drives, back-up tapes, and other media will be destroyed as part of the decommissioning processes. The actions will be performed under the direction of the KTRS Chief Information Officer.

**KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)**

2014-KTRS-06: The Kentucky Teachers' Retirement System Did Not Provide Sufficient Segregation Of Duty Controls Over The Legacy System

Our Fiscal Year (FY) 2014 review of the Kentucky Teachers' Retirement System (KTRS) system controls revealed KTRS did not employ sufficient segregation of duties between the system security administration, operation, and programming functions in relation to their legacy system.

Out of 20 user accounts related to 11 users or groups tested to determine whether proper segregation of duties existed, four users had profiles associated with one or more of their accounts with functions that present segregation of duties issues. Specifically, the QPGMR, QSYSOPR, and QSECOFR profiles were established for the legacy system. The QPGMR profile grants the user programming functions whereas the QSYSOPR profile is used to perform system operation functions. Further, the QSECOFR profile allows the user to perform security administration functions. We found that these four users had concurrent and unlimited access to two or more of these profiles during the audit period. As such, security controls could potentially be circumvented without detection.

We are aware that KTRS anticipates completely replacing the legacy system in January 2015, which will alleviate our concerns associated with segregation of duties for this system.

In addition, after fieldwork was completed, KTRS implemented a review process to monitor the audit log of security-related activities on the legacy system. The audit log is reviewed weekly by the KTRS Deputy Secretary for Finance and Administration and the Chief Information Officer for anomalies or suspicious activity. Since the inception of the process, there has been no such activity detected in the audit logs. Furthermore, the legacy application development activities were formalized within the "AS400 Application Development-Deployment Overview" document. The document expands on the controls in place to provide for the separation of the development and deployment activities of the programming staff in the legacy system.

However, these corrective actions were not implemented until October 2014, after fieldwork was completed. Additionally, KTRS does not have an adequate review process in place as it is following an informal process to monitor the audit log. Therefore, while there are compensating controls in place, the access/security weaknesses are still present until the system is completely decommissioned.

The agency set up legacy system users with access to multiple profiles for specific reasons; however, the access currently allowed to the four users identified in testing is excessive and does not allow for proper segregation of duties.

Employing strong segregation of duty controls decreases the opportunity for unauthorized modification to files and programs, and decreases the likelihood of errors or losses occurring because of incorrect or unauthorized use of data, programs, and other resources.

**KENTUCKY TEACHERS' RETIREMENT SYSTEM
SCHEDULE OF FINDINGS AND RECOMMENDATIONS
For the Year Ended June 30, 2014
(Continued)**

2014-KTRS-06: The Kentucky Teachers' Retirement System Did Not Provide Sufficient Segregation Of Duty Controls Over The Legacy System (Continued)

An individual should not have concurrent access to a system as a programmer, as an operator, or as a security administrator. Any combination of these functions, at once, could allow, intentionally or unintentionally, the introduction of unauthorized or malicious source code into the production environment. Additionally, strong segregation of duties control will ensure an independent and objective testing environment without jeopardizing the integrity of production data. Smaller organizations that cannot easily segregate duties among servers should implement compensatory controls to supervise and monitor program change activities to ensure no simultaneous development and production activities are taking place.

Recommendation

We recommend KTRS ensure the newly implemented corrective actions, which include the weekly review of the audit log for legacy security related activities, are consistently performed and thoroughly documented until the legacy system is completely decommissioned. Documentation should be maintained by the agency to show when the review was performed, by whom, and the results of the review. This documentation should be readily available for audit purposes.

Management's Response and Corrective Action Plan

The KTRS legacy system, which has been in service since 1987, will be decommissioned beginning in January 2015. The legacy system was updated in 1990 to include an application and development/deployment system to track changes to the production environment. KTRS's security practices include compensatory controls to supervise and monitor program change activities to ensure no simultaneous development and production activities are taking place. These security practices, which are monitored by the KTRS Chief Information Officer, will continue until the legacy system is decommissioned.

Additionally, to mitigate the risk of unauthorized security activity in the legacy system, in October 2014, KTRS began monitoring the audit log of users performing the security administrator functions. The enhanced security monitoring is being performed by the KTRS Deputy Executive Secretary for Finance and Administration and the KTRS Chief Information Officer. These processes are performed and documented on a weekly basis and will continue until the legacy system is decommissioned.