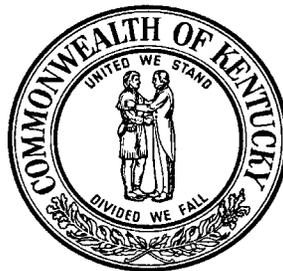


**LETTER FROM THE AUDITOR OF PUBLIC ACCOUNTS
DEPARTMENT OF EDUCATION**

**In Reference to the Statewide Single Audit
of the Commonwealth of Kentucky**

**For the Year Ended
June 30, 2006**



**CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS
www.auditor.ky.gov**

**105 SEA HERO ROAD, SUITE 2
FRANKFORT, KY 40601-5404
TELEPHONE (502) 573-0050
FACSIMILE (502) 573-0067**

TABLE OF CONTENTS

MANAGEMENT LETTER.....	1
LIST OF ABBREVIATIONS/ACRONYMS.....	3
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS	4
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS	7
FINANCIAL STATEMENT FINDINGS	10
<i>Reportable Conditions Relating to Internal Controls and/or</i>	
<i>Reportable Instances of Noncompliance</i>	<i>10</i>
FINDING 06-EDU-01: The Kentucky Department Of Education Office Of District Support Services Should Update And Consistently Apply Its Change Management Process	10
FINDING 06-EDU-02: The Kentucky Department Of Education Office Of District Support Services Should Formalize And Consistently Apply Its Logical Security Policies	13
FINDING 06-EDU-03: The Kentucky Department Of Education Office Of District Support Services Should Ensure Proper Segregation Of Duties	17
FINDING 06-EDU-04: The Kentucky Department Of Education Should Implement A Comprehensive Information Technology Policy And Ensure Adequate Oversight Authority Is Established	18
FINDING 06-EDU-05: The Kentucky Department Of Education Office Of Education Technology Should Formalize And Consistently Apply Logical Security Policies For The KETS Network And MUNIS	21
FINDING 06-EDU-06: The Kentucky Department Of Education Should Formalize The Task Order Process And Ensure Business Units Review Contractor Performance.....	24
<i>Other Matters Relating to Internal Controls and/or Instances of Noncompliance</i>	<i>28</i>
FINDING 06-EDU-07: The Kentucky Department Of Education Should Ensure That All Open Ports On Agency Machines Have A Business- Related Purpose	28
FINDING 06-EDU-08: The Kentucky Department Of Education Should Ensure That All Agency Web Servers Have Updated Software And Security Patches Installed	30
FINDING 06-EDU-09: The Kentucky Department Of Education Should Develop A Formal Disaster Recovery Plan.....	31
FINDING 06-EDU-10: The Kentucky Department Of Education Office Of Education Technology Should Update And Consistently Apply Its Change Management Process	33
FINDING 06-EDU-11: The Kentucky Department Of Education Should Formalize And Consistently Follow Formalized Procedures For Terminating Contract Employees	36
SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS.....	38



CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

To the People of Kentucky
Honorable Ernie Fletcher, Governor
Kevin Noland, Interim Commissioner
Department of Education

MANAGEMENT LETTER

KRS 43.090 (1) requires the Auditor of Public Accounts, upon completion of each audit and investigation, to prepare a report of all findings and recommendations, and to furnish copies of the report to the head of the agency to which the report pertains, and to the Governor, among others. This KRS also requires the Department of Education to, within 60 days of the completion of the final audit, notify the Legislative Research Commission and the Auditor of Public Accounts of the audit recommendations it has implemented and those it has not implemented and any reasons therefore. We are providing this letter to the Department of Education in compliance with KRS 43.090.

The work completed on the Department of Education is part of the overall opinions included in the audit of the Commonwealth of Kentucky's Comprehensive Annual Financial Report (CAFR) and Statewide Single Audit of Kentucky (SSWAK). Findings and recommendations for agencies, audited as part of the CAFR and SSWAK, if applicable, can be found in the Statewide Single Audit Report. This report can be obtained on our website at www.auditor.ky.gov.

In planning and performing our audits of the Commonwealth for the year ended June 30, 2006, we considered the Department of Education's internal control over financial reporting and compliance with laws, regulations, contracts and grant agreements in order to determine our auditing procedures for the purpose of expressing opinions included in the audit of the CAFR and SSWAK and not to provide an opinion on internal control or on compliance.

However, during our audit we became aware of certain matters that are opportunities for strengthening internal controls and operating efficiency. The SSWAK is a separate report dated March 28, 2007, and contains all reportable conditions and material weaknesses in the Commonwealth's internal control over financial reporting and internal control over compliance and also contains all reportable instances of noncompliance. This letter does contain the Department of Education findings and our recommendations that have been extracted from the SSWAK report along with other matters that have been identified.

We will review the status of these comments during our next audit. We have already discussed many of these comments and suggestions with various Department of Education personnel, and we will be pleased to discuss them in further detail at your convenience, to perform any additional study of these matters, or to assist you in implementing the recommendations.



To the People of Kentucky
Honorable Ernie Fletcher, Governor
Kevin Noland, Interim Commissioner
Department of Education

Included in this letter are the following:

- ◆ Acronym List
- ◆ Schedule of Expenditures of Federal Awards
- ◆ Notes to the Schedule of Expenditures of Federal Awards
- ◆ Findings and Recommendations
- ◆ Summary Schedule of Prior Audit Findings

Respectfully submitted,



Crit Luallen
Auditor of Public Accounts

March 28, 2007

LIST OF ABBREVIATIONS/ACRONYMS

CAFR	Comprehensive Annual Financial Report
CFDA	Catalog of Federal Domestic Assistance
CIO	Chief Information Officer
CMA	Change Management Administrator
COT	Commonwealth Office of Technology
CRO	Change Request Owners
CSO	Centralized Security Officer
DBA	Database Administrator
DPMR	Data Policy Management and Research
EDU	Department of Education
FTP	File Transfer Protocol
FY	Fiscal Year
HR	Human Resources
IT	Information Technology
KAR	Kentucky Administrative Regulations
KDE	Kentucky Department of Education
KETS	Kentucky Education Technology System
KRS	Kentucky Revised Statutes
MAP	Management Advisory Procedures
MUNIS	Municipal Information System(s)
NA	Not Applicable
OCR	Operations Change Request
ODSS	Office of District Support Services
OET	Office of Education Technology
OIAS	Office of Internal Administration and Support
OMB	Office of Management and Budget
ProCard	Procurement Card
RFP	Request for Proposal
SA	Server Administrator
SDS	Systems Development Services
SEEK	Support Education Excellence in Kentucky
SQL	Structured Query Language
SSWAK	Statewide Single Audit of Kentucky
TPC	Technology Planning Council
U.S.	United States

SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2006

CFDA #	Program Title	Expenditures		Provided to Subrecipient
		Cash	Noncash	
DEPARTMENT OF EDUCATION				
<u>U.S. Department of Agriculture</u>				
Direct Programs:				
Child Nutrition Cluster:				
10.553	School Breakfast Program (Note 2)	\$ 41,729,192		\$ 41,621,569
10.555	National School Lunch Program (Note 2)	121,606,547		121,410,126
10.556	Special Milk Program for Children (Note 2)	73,945		47,772
10.559	Summer Food Service Program for Children (Note 2)	8,102,061		7,911,208
10.558	Child and Adult Care Food Program (Note 2)	25,966,265		25,833,683
10.560	State Administrative Expenses for Child Nutrition	2,166,042		
<u>U.S. Department of Labor</u>				
Passed Through From the Department for Workforce Investment:				
Workforce Investment Act Cluster:				
17.259	WIA Youth Activities	107,790		107,820
17.260	WIA Dislocated Workers	641,825		590,831
<u>U.S. Department of Education</u>				
Direct Programs:				
84.010	Title I Grants to Local Educational Agencies (Note 2)	185,351,725		183,324,053
84.011	Migrant Education - State Grant Program	6,679,176		6,526,430
84.013	Title I Program for Neglected and Delinquent Children	12,067		
Special Education Cluster:				
84.027	Special Education - Grants to States (Note 2)	149,250,349		145,740,425
84.173	Special Education - Preschool Grants (Note 2)	9,860,785		9,433,793
84.184	Safe and Drug-Free Schools and Communities: National Programs	271,324		173,269
84.185	Byrd Honors Scholarships (Note 3)(Note 4)			
84.186	Safe and Drug-Free Schools and Communities - State Grants	4,600,367		4,478,822
84.196	Education for Homeless Children and Youth	628,777		697,349
84.213	Even Start - State Educational Agencies	3,226,662		2,959,859

SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2006

CFDA #	Program Title	Expenditures		Provided to Subrecipient
		Cash	Noncash	
DEPARTMENT OF EDUCATION				
84.215	Fund for the Improvement of Education (Note 5)	2,342		
84.281	Eisenhower Professional Development State Grants (Note 3)			
84.287	Twenty-First Century Community Learning Centers	9,488,118		9,421,108
84.298	State Grants for Innovative Programs	3,429,682		3,148,550
84.318	Education Technology State Grants	7,730,824		7,366,339
84.323	Special Education - State Personnel Development	1,425,322		1,425,322
84.326	Special Education - Technical Assistance and Dissemination to Improve Services and Results for Children with Disabilities	131,564		163,404
84.327	Special Education - Technology and Media Services for Individuals with Disabilities	133,560		155,088
84.330	Advanced Placement Program	420,191		72,861
84.332	Comprehensive School Reform Demonstration	4,314,591		4,181,372
84.350	Transition to Teaching	154,166		121,998
84.352	School Renovation Grants (Note 3)			
84.357	Reading First State Grants	14,186,198		13,171,531
84.358	Rural Education	7,417,599		7,418,220
84.365	English Language Acquisition Grants	2,022,788		1,963,106
84.366	Mathematics and Science Partnerships	1,652,831		1,639,222
84.367	Improving Teacher Quality State Grants (Note 2)	41,950,206		41,703,236
84.369	Grants for State Assessments and Related Activities	10,250,673		200,329
84.372	Statewide Data Systems	62,307		
84.938	Hurricane Education Recovery	2,725,791		2,727,291
Passed Through From Department for Workforce Investment:				
84.048	Vocational Education - Basic Grants to States	6,403,883		6,103,298
<u>U.S. Department of Health and Human Services</u>				
Direct Programs:				
93.243	Substance Abuse and Mental Health Services Projects of Regional and National Significance	7,418		
93.576	Refugee and Entrant Assistance - Discretionary Grants	130,352		130,352
93.600	Head Start	179,477		64,480

SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2006

CFDA #	Program Title	Expenditures		Provided to Subrecipient
		Cash	Noncash	
DEPARTMENT OF EDUCATION				
93.938	Cooperative Agreements to Support Comprehensive School Health Programs to Prevent the Spread of HIV and Other Important Health Problems	588,626		465,043
Passed Through From the Cabinet for Health and Family Services:				
93.110	Maternal and Child Health Federal Consolidated Programs	5,215		
<u>U.S. Corporation on National and Community Service</u> Direct Programs:				
94.004	Learn and Serve America - School and Community Based Programs	265,796		249,977
TOTAL DEPARTMENT OF EDUCATION		\$ 675,354,419		\$ 657,670,261

NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2006

Note 1 - Purpose of the Schedule and Significant Accounting Policies

Basis of Presentation - OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*, requires a Schedule of Expenditures of Federal Awards showing each federal financial assistance program as identified in the *Catalog of Federal Domestic Assistance*. The accompanying schedule includes all federal grant activity for the Commonwealth, except those programs administered by state universities, and is presented primarily on the basis of cash disbursements as modified by the application of Kentucky Revised Statute (KRS) 45.229. Consequently, certain expenditures are recorded in the accounts only when cash is disbursed. The Commonwealth elected to exclude state universities from the statewide single audit, except as part of the audit of the basic financial statements.

KRS 45.229 provides that the Finance and Administration Cabinet may, “for a period of thirty (30) days after the close of any fiscal year, draw warrants against the available balances of appropriations made for that fiscal year, for the payment of expenditures incurred during that year or in fulfillment of contracts properly made during the year, but for no other purpose.” However, there is an exception to the application of KRS 45.229 in that regular payroll expenses incurred during the last pay period of the fiscal year are charged to the next year.

The basic financial statements of the Commonwealth are presented on the modified accrual basis of accounting for the governmental fund financial statements and the accrual basis of accounting for the government-wide, proprietary fund, and fiduciary fund financial statements. Therefore, the schedule may not be directly traceable to the basic financial statements in all cases.

Clusters of programs are indicated in the schedule by light gray shading.

Programs that do not have CFDA numbers are identified using the two-digit federal identifier prefix, and the letters “NA” to denote that no specific number is applicable. Each program is numbered in parentheses, following the NA for each federal grantor.

The state agencies’ schedule is presented on the cash, modified cash, or accrual basis of accounting.

Inter-Agency Activity - Certain transactions relating to federal financial assistance may appear in the records of more than one (1) state agency. To avoid the overstatement of federal expenditures, the following policies were adopted for the presentation of the schedule:

NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2006

Note 1 - Purpose of the Schedule and Significant Accounting Policies

- (a) Federal moneys may be received by a state agency and passed through to another state agency where the moneys are expended. Except for pass-throughs to state universities as discussed below, this inter-agency transfer activity is reported by the agency expending the moneys.

State agencies that pass federal funds to state universities report those amounts as expenditures.

- (b) Federal moneys received by a state agency and used to purchase goods or services from another state agency are reported in the schedule as an expenditure by the purchasing agency only.

Note 2 - Type A Programs

Type A programs for the Commonwealth mean any program for which total expenditures of federal awards exceeded \$20 million for FY 06. The Commonwealth had the following programs (cash and noncash) that met the Type A program definition for FY 06, some of which were administered by more than one (1) state agency. Certain component units and agencies audited by certified public accounting firms had lower dollar thresholds. The Commonwealth identified clusters among the Type A programs by gray shading. These Type A programs and clusters were:

CFDA #	Program Title	Expenditures
Child Nutrition Cluster:		
10.553	School Breakfast Program	\$41,729,192
10.555	National School Lunch Program	121,606,547
10.556	Special Milk Program for Children	73,945
10.559	Summer Food Service Program for Children	8,102,061
10.558	Child and Adult Care Food Program	25,966,265
84.010	Title I Grants to Local Educational Agencies	185,351,725
Special Education Cluster:		
84.027	Special Education - Grants to States	149,250,349
84.173	Special Education - Preschool Grants	9,860,785
84.367	Improving Teacher Quality State Grants	41,950,206
Total Type A Programs		<u><u>\$583,891,075</u></u>

NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2006

Note 3 - Zero Expenditure Programs

The zero expenditure programs included programs with no activity during the year, such as old programs not officially closed out or new programs issued late in the fiscal year. They also included programs with activity other than expenditures.

Note 4 - Byrd Honors Scholarships Program (CFDA #84.185)

The Byrd Honors Scholarships Program was moved from the Kentucky Department of Education to the Kentucky Higher Education Assistance Authority.

Note 5 - Pass Through Programs

OMB Circular A-133 Section 105 defines a recipient as “a non-Federal entity that expends Federal awards received directly from a Federal awarding agency to carry out a Federal program” and a pass-through entity as “a non-Federal entity that provides a Federal award to a subrecipient to carry out a Federal program.”

Federal program funds can be received directly from the federal government or passed through from another entity. Below is a list of all federal programs that are either (1) passed through, or (2) both direct and passed through.

<u>Received From</u>	<u>Direct/Pass Through (Grantor #)</u>	<u>State Agency</u>	<u>Amount</u>
<u>Fund for the Improvement of Education (CFDA #84.215)</u>			
U.S. Department of Education	Direct	EDU	\$ 2,342
Total Fund for the Improvement of Education			<u>\$ 2,342</u>

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-01: The Kentucky Department Of Education Office Of District Support Services Should Update And Consistently Apply Its Change Management Process**

During the FY 2006 audit of the Kentucky Department of Education (KDE) system controls, it was discovered that the Office of District Support Services (ODSS) has a general program change control review and approval process in place; however, KDE had not formalized this process in standards or procedure statements specific to the agency. Further, the current process is not sufficient or adequately designed to ensure that only authorized changes to key applications are made.

Specific to the Seeking Education Excellence in Kentucky (SEEK) calculation program, the current KDE programmer makes changes to the code and places comments within the program code identifying the change made. Prior to implementation, two members of the ODSS supervisory staff review the proposed code changes and manually calculate the anticipated output figures to be produced by the programmer. Once changes are approved, the programmer then moves the executable files into production and executes the code. However, this process was not formalized or sufficiently documented. No program change forms were developed and the process of requests, reviews, and approvals for program changes was not adequately documented. Further, no log of requests or changes was maintained by the ODSS staff or programmer to monitor program change requests.

We have issued a separate audit finding presented at 06-EDU-03 concerning the issue of the KDE programmer's excessive access to the production library.

Without a formalized program change control process and monitoring of the compliance with the process, the agency is at risk that procedures that are deemed vital to the process will be overlooked. For example, disregarding the procedure established to review supporting documentation for evidence that a change has been tested and approved for promotion to production increases the likelihood that unauthorized or inappropriate program changes could be placed in production.

A strong program change control process will ensure policies and procedures are formalized, distributed, and understood by all applicable agency personnel. This process should be consistently applied to all code changes to existing programs and the development of new programs.

All program modifications are to be monitored and thoroughly documented, with procedures established to log all program change requests, review and approval processes to be followed, and supporting documentation to be maintained for the process.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-01: The Kentucky Department Of Education Office Of District Support Services Should Update And Consistently Apply Its Change Management Process (Continued)**

Recommendation

We recommend that ODSS formalize, implement, and consistently apply adequate program change controls. Specifically, the agency should, at a minimum:

- Develop a formal procedure for the program change control process. This formalized document should include the procedures to adequately identify program specifications and program objectives, to specifically identify changes in code by developing a code comparison listing between the original code and the revised code, to adequately test proposed program code changes, and to verify that all approvals are in place for the program code change before implementation to the production environment. If emergency situations are anticipated that might require this process to be accelerated, then that should be taken into consideration and an alternative process developed that properly applies compensating controls over that accelerated process.
- Develop a change request form that indicates what changes are to be made and what files/programs are involved, who is requesting the change, testing of the change, and authorization that the change was approved. This process should be included in the overall formalized procedure to ensure all employees involved with the process understand how to properly complete the form.
- Process all new programs or modifications to existing programs through the established program change control process as documented in the formal procedure.
- Ensure all changes comply with established program change control procedural requirements. Requirements should include procedures to ensure that an individual other than the programmer properly reviews and tests all changes for accuracy and that proper approvals are documented authorizing implementation of the change into production before the librarian moves the change to the production environment. After implementation of changes, the librarian should sign and date the change request form to affirm that this process has been completed.
- Establish a logging feature within the program change control process. This log should include the name of the originator, origination date, brief description of problem, programs affected, completion date, and implementation date.
- Establish a centralized location for maintaining all complete change request forms.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-01: The Kentucky Department Of Education Office Of District Support Services Should Update And Consistently Apply Its Change Management Process (Continued)**

Management Response and Corrective Action Plan

In response to the recommendation that the Office of District Support Services formalize, implement and consistently apply adequate program change controls, the following corrective actions are planned:

- 1. ODSS will develop a formal procedure for the program change control process. In February 2006, ODSS hired an individual to serve as Technology Project Manager who has the responsibility to develop the change control process. The procedures will be documented and implemented as a standard operation. The procedures will include program identification, requirement specifications, test plans, and management approval. ODSS has also implemented Visual SourceSafe as the code repository (provides version control and code comparison functionality). The procedure will also document an alternative for emergency situations when the standard process must be expedited. The change control process will be documented and functional by August 1, 2006.*
- 2. ODSS has instituted a project request form that encompasses the recommendations for a change request form.*
- 3. The procedures will apply to new application development as well as modification of existing programs.*
- 4. The Technology Project Manager will monitor compliance with the change control procedural requirements. This includes the validation of user testing and authorization to implement the change into production. ODSS has designated a librarian to move the change to the production environment and add the completion to the change request form.*
- 5. The Technology Project Manager will maintain a portfolio of all maintenance and new development requests as the recommended logging feature.*
- 6. All change requests and supporting documentation will be maintained in the ODSS Projects folder on the server.*

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-02: The Kentucky Department Of Education Office Of District Support Services Should Formalize And Consistently Apply Its Logical Security Policies**

During the FY 2006 audit of controls for KDE, it was determined that the ODSS did not properly secure the critical financial data associated with the SEEK program. Also, ODSS had not developed or implemented a formalized security policy that identifies management and user responsibilities concerning IT security surrounding the SEEK program and other applications developed and maintained by ODSS. Our audit identified multiple security issues concerning logical security of ODSS related servers as explained below.

The audit revealed that critical SEEK executable programs were placed on a KDE server that was not adequately secured. The Office of Education Technology (OET) server on which the SEEK production executables were placed was a server intended only for temporary storage of general information and it was accessible by all KDE employees and contractors during the audit period to date. The executable programs were originally moved to OET by a SEEK programmer from an ODSS file server without the knowledge of OET. We have reported on the control weakness concerning programmer access to the SEEK production executables in a separate audit finding at 06-EDU-03 as a segregation of duties weakness. Upon auditors notifying ODSS that program executables were accessible to all KDE employees, the folder on the OET server where the SEEK executables resided was restricted to certain ODSS employees. However, the SEEK programmer in question is still one of the users who retains access to those executable programs. Further, we noted that the original ODSS server location from where the SEEK executables were moved was not adequately secure, as all ODSS employees had access to that SEEK directory. That access was not necessary for the performance of their job duties.

In addition, we noted various security issues concerning user accounts accessing ODSS servers. One user account was being shared by four separate users on one of the two structured query language (SQL) ODSS servers where the SEEK code had previously been housed. That same user ID and the associated password was also hard coded into the program code designed to retrieve information from other programs to be utilized in the SEEK calculation. It should be noted that a copy of these scripts was stored on the unsecured OET server with the executables discussed above and was also accessible by all KDE employees and contractors until our fieldwork identified the issue. We also noted two unnecessary system accounts and three unnecessary individual user accounts on this SQL server, two of which belonged to users who initially worked for ODSS, but no longer works in ODSS and one of whom works in OET but does not require this access. This access has been subsequently removed.

We tested to ensure that confidentiality forms were on file for the 11 individual users with directory level and/or System Administrator access to the ODSS server. One of the forms was not available. Since ODSS is responsible for determining the access needed by ODSS

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-02: The Kentucky Department Of Education Office Of District Support Services Should Formalize And Consistently Apply Its Logical Security Policies (Continued)**

employees to OET's file transfer protocol (FTP) server, we also tested to ensure that confidentiality forms were on file for the 10 ODSS individuals who were able to download district-level MUNIS reports from that server. Our testing revealed that confidentiality forms were not on file for two ODSS users with access to that FTP server. In addition, one other employee who was previously responsible for the distribution of MUNIS reports, but no longer works for ODSS, had an improperly authorized confidentiality form on file. Furthermore, two employees had access to this FTP server that was not required, given their job duties.

Due to security control weaknesses identified with the ODSS servers, we requested to review the server logs that would identify users who accessed the servers and specific programs during our audit period. However, KDE/OET did not have object access audit logging established on these servers so we could not identify nor determine the appropriateness of any user access to the servers during the audit period.

It was also noted that a Database Administrator (DBA) had not been appointed to oversee one of the two SQL servers where SEEK data is housed, nor for the ODSS file server on which the SEEK executables originally resided.

Without strong, formalized, logical security controls, the opportunity increases for unauthorized modification to production files as well as the likelihood of errors or losses occurring from incorrect use of data and other resources. The lack of formal security policies was key in allowing the various security weaknesses noted. The fact that the SEEK program was executed in an unsecured environment could affect the reliability of any resulting output from that system that might be used for management decision-making purposes or for the distribution of SEEK funds. Even though access has now been further restricted, the SEEK programmer still has access to the executables, and ODSS is not monitoring file access because the programs reside on a server for which OET is responsible. This gives evidence to the fact there is not a clear understanding between the various Business Units and OET as to who has the responsibility for maintaining adequate security over KDE IT resources, which we have addressed in the audit finding presented at 06-EDU-03.

Formalized and consistently applied security policies set the tone of management concern for strong system security and provide a security framework used to educate management and users on their responsibilities. System security should be administered in such a way as to ensure proper segregation of duties. System access should be limited to the level necessary to perform assigned duties. Granting users system access that would allow the ability to alter or delete programs or financial data prior to or subsequent to processing increases the risk of financial misstatements or fraudulent reporting. The use of group

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-02: The Kentucky Department Of Education Office Of District Support Services Should Formalize And Consistently Apply Its Logical Security Policies (Continued)**

accounts does not provide an adequate audit trail for transaction processing. Audit logging should be implemented to capture user access of critical programs and data. Default system or user accounts are some of the first accounts that a hacker would attack and should, therefore, be assigned strong passwords or, if possible, be renamed or removed immediately upon installation.

Recommendation

We recommend that ODSS formalize, implement and consistently apply a security policy that standardizes security responsibilities for all ODSS employees and ensures critical ODSS programs and data are properly secured. Specifically, the agency should, at a minimum:

- Ensure that the SEEK executables are returned to their original location on the ODSS server so that they are maintained and supervised by ODSS.
- Ensure that programmers, as well as any employees that do not specifically require access, are not allowed access to the executables in order to maintain proper segregation of duties.
- Ensure that any other SEEK program scripts or code that were placed on the OET file server are returned to the ODSS SQL servers.
- Object access audit logging should be established on all ODSS servers.
- User authentication should be used in any processes or code requiring authorization rather than maintaining hard coded usernames and passwords in the code. Hard coded usernames and passwords in program code should be eliminated.
- The practice of using shared user accounts should be terminated immediately.
- All individual user accounts should be analyzed to determine if they are necessary. If not, they should be removed. This process should be re-performed on a periodic basis.
- Any default system accounts should be reviewed to determine their necessity. Unnecessary accounts should be disabled.

A DBA should be appointed with oversight over the SQL server where the SEEK data resides, as well as the server on which the executables are placed. Accordingly, the DBA should be responsible to establish and monitor all current employee's access levels on an ongoing basis to ensure access levels facilitate a proper segregation of duties and do not allow inappropriate access to production data. This review should be thoroughly documented for audit purposes.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-02: The Kentucky Department Of Education Office Of District Support Services Should Formalize And Consistently Apply Its Logical Security Policies (Continued)**

Recommendation

- Ensure that access to electronic resources is removed promptly upon termination of employment.
- Ensure that confidentiality forms are properly authorized and maintained on behalf of all ODSS employees.

Management Response and Corrective Action Plan

1. *The Office of District Support Services is in the process of moving all files, databases, and programs to new servers. This migration is scheduled for completion by July 1, 2006, and KDEC PFN1 and KDEC PFN2 will no longer be used.*
2. *In order to preserve separation of duties, the servers KDEODSSOA1 and KDEODSSOS1 are managed by an ODSS Server Administrator and the MS SQL Server databases are managed by the ODSS DBA.*
3. *The Server Administrator will take the necessary steps to implement object access audit logging by July 1, 2006.*
4. *All ODSS files, databases, and programs will be on ODSS Servers by July 1, 2006.*
5. *ODSS will review all production applications for hard-coded user names and passwords. Any applications requiring modification to replace hard-coded user names and passwords will be handled through the change control process.*
6. *Shared User Accounts will be identified and eliminated by July 1, 2006.*
7. *The Server Administrator will provide ODSS management with a report of individual user accounts for verification by July 1 of each year. The SA will maintain documentation for all requests to add, change or delete a user account.*
8. *The SA will provide a listing of default system accounts to the ODSS Leadership team by July 1 of each year.*
9. *ODSS has designated a DBA to monitor access to production level databases and facilitate the proper segregation of duties.*
10. *The ODSS leadership team will route EP-1 documents received from HR to the SA for appropriate action. For a terminated employee, the SA will disable access as quickly as possible and notify leadership upon completion.*
11. *The Division of Human Resources in OIAS is responsible for the maintenance of confidentiality forms on behalf of ODSS.*

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 06-EDU-03: The Kentucky Department Of Education Office Of District Support Services Should Ensure Proper Segregation Of Duties

During the FY 2006 audit of KDE system controls, it was determined that ODSS did not employ proper segregation of duties between the system programming and operation functions. Specifically, one KDE programmer was also functioning as the librarian and computer operator for the SEEK calculation program.

As a result, the programmer had the ability to make changes to the program code, move those changes to the production environment, and execute the code. The programmer also had a backup copy of the SEEK executables saved within his personal drive on the server. Although a current authorization process is in place for change controls, the process was not formalized and does not provide compensating controls concerning these incompatible duties performed by the programmer.

The lack of formalized policies and procedures governing the change control process at ODSS was addressed in a separate audit finding presented at 06-EDU-01.

In addition, it was determined that the same programmer noted above moved the SEEK executables and other program code to an unsecured location on an OET server without the knowledge of OET. The security of the SEEK executables and program code was addressed in a separate audit finding at 06-EDU-02 regarding logical security.

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.

Computer programmers should not have direct access to the production version of program source code or be able to directly affect the production environment. The reason for this control is to ensure that the programmer does not intentionally or unintentionally introduce unauthorized or malicious source code into the production environment. Smaller organizations that cannot easily segregate programmer duties from computer operator duties should implement compensatory controls to supervise and monitor programmer activities to ensure only properly tested and authorized programs are migrated into production.

Recommendation

We recommend ODSS ensure that someone other than the programmer be required to move changes into the production environment and execute the program code. Consequently, it is unnecessary for the programmer to have access to the production executables, and the executables should not be maintained on the programmer's personal drive. All production programs and data should be secured separately from the change and testing environment in order to maintain proper segregation of duties. ODSS supervisory staff should continue to thoroughly review and document all program changes made by the programmer to ensure they are appropriate prior to processing.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-03: The Kentucky Department Of Education Office Of District Support Services Should Ensure Proper Segregation Of Duties (Continued)**

Management Response and Corrective Action Plan

The Office of District Support Services will restrict developer's access to 'Read Only' in the production environment. ODSS will maintain separate environments for development, testing, and production. The segregation of duties will be documented in the change control process and monitored by the Technology Project Coordinator. ODSS will be fully operational with the change control process by August 1, 2006.

FINDING 06-EDU-04: The Kentucky Department Of Education Should Implement A Comprehensive Information Technology Policy And Ensure Adequate Oversight Authority Is Established

During the audit of system controls at KDE for FY 2006, it was determined that a governance model or oversight authority was not adequately established to ensure adequate information technology (IT) control policies and procedures were implemented to secure IT resources of the various KDE Business Units.

A "Business Champion" concept was implemented within KDE so that critical projects or processes within KDE would be provided adequate leadership and oversight by management and other stakeholders that are involved with and operate the projects on a daily basis. The current KDE business approach involves various Business Units. This structure provides the Business Units with input into the IT infrastructure decisions involving its projects. Though OET provides certain operating services, the ownership of certain portions of the infrastructure lies with the Business Units. Having infrastructure that is not centrally maintained and is outside the core functions of the OET staff has created a situation where the responsibility for the development and implementation of formal IT control and security policies is unclear to both OET and the business units.

OET creates 'guidelines' and disseminates best practice information to assist KDE Business Unit personnel with the configuration and settings related to the IT network or the implementation of new technology products. However, the delineation between OET and the business units is unclear as to the authority and responsibility to ensure compliance with IT standards and policies. Because a decentralized structure has been created to provide business units with more control over sub-systems that require program input, KDE does not have a Centralized Security Officer (CSO).

Based on our testing and discussions, it is apparent that Business Unit leaders or champions are not fully aware of the need or responsibility to establish and implement IT

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

controls. We tested IT controls within one Business Unit responsible for the operation of MUNIS and the SEEK systems. These were the primary systems included in the audit scope. Our testing revealed weaknesses with IT security controls for those systems. The IT security weaknesses identified with these two programs have been commented on separately in audit findings presented at 06-EDU-02, 06-EDU-03, and 06-EDU-05. Weaknesses noted included a lack of any basic formal IT security control policies within the audited Business Unit responsible for these systems. Testing within this area revealed that the Business Unit managers were not aware of the responsibility to develop and implement formal IT control policies and procedures. When OET directed the auditors to the Business Unit management for answers to IT control questions related to those systems, the auditors were often redirected back to OET by the Business Unit with management's assumption that IT controls were OET's responsibility.

We did note during our testing that all employees of the Education Cabinet are required to sign an Acceptable Use Policy, which was established as a result of legislative regulations (701 KAR 5:120) to ensure employees did not use technical resources to access inappropriate material on the Internet. However, this was the only formalized IT policy identified during our fieldwork that required compliance by the Business Unit system operators or end users.

We also noted that KDE has created the Technology Planning Council (TPC) to ensure that technology-enabled business initiatives are successful. The TPC guides the deployment of IT resources to meet the priorities of KDE, the Kentucky Board of Education and the local school districts. Key management employees from OET are members of TPC. This approach by TPC and KDE appears to have assisted in providing Business Units more input into IT infrastructure decision making and the standards to be met for IT resource procurement and installation, but standardized IT control policies and procedures have not been developed or implemented.

Therefore, in summary, though we agree that Business Units should be involved in developing IT strategies and making other technology decisions, we believe a centralized IT governance authority is needed to ensure that standardized IT control policies and procedures are established and consistently implemented within KDE for all IT systems. This same conclusion concerning centralized IT control oversight had been provided to KDE within a report provided by Gartner, Inc (Gartner) in 2004 as a result of their IT assessment and optimization study. Discussions revealed that KDE had intended to comply with the Gartner recommendations but it appears the decisions for authorizations and responsibilities to establish and implement IT controls was not properly established or communicated to all parties.

Because of the organizational structure of KDE, Business Units do not report to OET and OET does not have primary responsibility for maintaining all IT systems. This situation resulted in inconsistent and incomplete controls over the KDE network and IT resources. Business Units were not required to establish and implement formal IT control policies and procedures.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-04: The Kentucky Department Of Education Should Implement A
Comprehensive Information Technology Policy And Ensure Adequate Oversight
Authority Is Established (Continued)**

A comprehensive IT policy defines management and user responsibilities and obligations for the maintenance, security, legal, and appropriate use of the KDE network and IT resources. Much of the information that KDE employees use or rely on is provided via the data network and the Internet itself. While these networks offer invaluable opportunities for sharing information and for working more efficiently, they also offer potential points of unauthorized access into KDE's data, e-mail accounts, and other valuable and often confidential information. IT control policies and procedures should be standardized, consistently applied, and monitored for compliance to ensure proper system and control development, implementation, and management.

Recommendation

We recommend that KDE establish an appropriate IT governance authority to design and implement standard IT controls and to provide centralized oversight of these controls for all KDE IT resources. We recommend that any authority that is established for this purpose have the necessary qualifications to ensure established IT control policies and procedures are adequately designed and implemented. We recommend that management of all Business Units and the applicable system users be properly advised of the responsibility to comply with established IT control policies and procedures.

Consideration of IT controls, at a minimum, should include acceptable use of network resources, physical and logical access security controls, program change controls, and business recovery.

Management Response and Corrective Action Plan

KDE acknowledges that additional IT controls and policies need to be formalized and implemented throughout all of the business units within KDE. Because this issue affects a number of different offices throughout KDE, the solutions will require significant planning and collaboration between OET and the other various business units. These issues will be addressed initially by the Technology Planning Council and consideration will be given to a centralized authority for oversight of IT controls and procedural implementation.

KDE will develop policies to address program change controls, logical security access controls and disaster recovery, as well as, any other IT security control weaknesses. These standards and procedures will then be communicated across all business units in KDE. We expect that a comprehensive plan, procedure development and implementation across all business units will take at least one year. KDE expects to implement the changes by July 1, 2007.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 06-EDU-05: The Kentucky Department Of Education Office Of Education Technology Should Formalize And Consistently Apply Logical Security Policies For The KETS Network And MUNIS

During the FY 2006 audit KDE, OET did not develop or implement a formalized security policy that identifies management and user responsibilities concerning security surrounding the Kentucky Education Technology System (KETS) network. Further, adequate controls were not established to properly secure the critical financial and personal data that is transferred from the 176 Kentucky school districts to OET's MUNIS gateway server.

As noted in a separate audit finding at 06-EDU-04, KDE has established various Business Units that have been given the responsibility of maintaining adequate information technology controls for resources used to support its major programs. However, there remain various central workstations and servers, as well as related OET employee and contractor network access, for which OET management is responsible. Our audit revealed that OET had not implemented a formalized security policy to control system access by these employees and contractors, nor to control access to OET maintained servers by system users within other business units.

The school districts primarily use the MUNIS financial system to manage its finances. In addition, certain financial and staffing reports exist that KDE uses from the districts for state and federal purposes. When districts are ready to forward reports to KDE, the KYTRANSFER utility is used in order to place the reports in an outbox located on their MUNIS server located at the school district. From there the KYCOLLECTION utility automatically collects and transports the reports to KDE's MUNIS gateway server that OET manages. These reports are then moved to the FTP server for pickup by ODSS staff.

During the course of our fieldwork, we identified seven OET employees with access to the MUNIS Gateway server through group account, individual user account, or both. We examined the confidentiality statements for all seven users to ensure this access was properly authorized. Our examination revealed that three of the users accessing this server were contractors and had this access since as early as the year 2000. However, the KDE supervisor for these three contractors did not provide documented authorization for this access until February 2006.

Our testing also identified that eight group accounts that were established for accessing the MUNIS gateway server in order for OET to provide technical support to the school districts. These group accounts are also used when accessing a school district's server. Review of these accounts indicated that one group account established on the MUNIS gateway server was unnecessary in relation to the function of the server.

However, group accounts with a shared password should never be employed, especially for users with system access greater than READ capabilities, as they provide an inadequate audit trail of the actual user's identity.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 06-EDU-05: The Kentucky Department Of Education Office Of Education Technology Should Formalize And Consistently Apply Logical Security Policies For The KETS Network And MUNIS (Continued)

Discussions did reveal that although KDE/OET had not implemented a formal security policy, an informal policy was in place requiring OET/KDE staff to first obtain authorization from the school district before accessing that district's MUNIS server or software. However, logs are not maintained that track access to district servers. We also noted that OET does not generally have Object Access audit logging implemented on its critical servers.

Our testing also revealed that many of the MUNIS reports submitted to KDE contain confidential information that is not encrypted during transmission. Though this information does remain within the KDE network and is not accessible from external machines, we still consider this a security concern. Based on our discussions with district personnel, this issue has also been a concern expressed by districts in the past. Discussions revealed that OET does plan to use secure tunnels (IPSec) in the future to protect the data that is transferred from the districts. This security feature was not available until the 2004 version of MUNIS and not all school districts had been upgraded to this version at the time of our fieldwork. Once all districts have upgraded to MUNIS 2004, OET plans to ensure IPSec is implemented.

Our testing also revealed that all KDE users were granted Local Administrator rights on their workstations. This is considered unnecessary access for all KDE employees to have. Technical and support staff should be the only personnel with this level of access to prevent the accidental or intentional introduction of viruses or the loss of programs or data and to ensure workstations utilize only approved software.

Without strong, formalized, logical security controls, the opportunity increases for unauthorized modification to financial and staffing reports as well as the likelihood of errors or losses occurring from incorrect use of data and other resources. Failure to properly encrypt confidential information during transfer within the KETS network exposes KDE/OET to unnecessary liability that could result from a failure to adequately secure such data should that data be captured and used inappropriately. Granting users local administrator rights to their workstations allows those users the ability to download and install unauthorized software as well as possibly pirated data.

Formalized security policies set the tone of management concern for strong system security and provide a security framework used to educate management and users of their responsibilities. System security should be administered in such a way as to ensure proper segregation of duties. System access should be limited to the level necessary for performing assigned duties. Granting users system access that would allow the ability to alter or delete programs or financial data prior to or subsequent to processing increases the risk of financial misstatements or fraudulent reporting.

FINANCIAL STATEMENT FINDINGS

Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance

FINDING 06-EDU-05: The Kentucky Department Of Education Office Of Education Technology Should Formalize And Consistently Apply Logical Security Policies For The KETS Network And MUNIS (Continued)

Confidential data that is transmitted over networks should be properly secured by strong encryption or other similar measures. Further, access to servers that house critical financial and staffing data should be restricted to only necessary employees. Intruders often use inactive accounts to break into a network. If an account was not used for a reasonable period of time, the account should be disabled until it is needed. This minimizes the possibility that an unauthorized user will access the account. Finally, system user accounts and audit trails should be established in a manner to enable proper identification and tracking of user activity.

Recommendation

We recommend that OET develop and implement a formalized security policy that standardizes security responsibilities for all OET employees and ensures critical programs and data, as well as the servers housing such data, are properly secured. Also, OET should ensure that when all school districts upgrade to the most current version of MUNIS that IPSec Tunnels be implemented and used to secure the data being transmitted. This should be made a priority by the agency. Object Access audit logging should be enabled on all OET servers so that inappropriate use of resources can be further investigated, if the need arises. A security log should be established for all KDE employees to use that must access a school district's MUNIS server. OET should review the user and group accounts that are currently being used to ensure there is a legitimate business necessity for having them. If it is determined they are not necessary, they should be disabled.

Management Response and Corrective Action Plan

OET agrees with all recommendations and will implement a formal policy and controls to standardize security responsibilities for all OET employees that ensure critical programs, data and associated hardware are properly secured. Completion date is February 1, 2007.

OET has just completed the upgrade of all districts to the most current version of MUNIS. OET has also initialized a project to move all districts to a secure data transfer mode before Jan 1, 2007. The project is well into the design and vendor engagement steps.

OET will enable the audit logging function on all OET agency servers by August 30, 2006. After implementation OET will monitor the performance cost on each server and provide options to overcome any identified performance deficits. For the servers physically located in each school district, that provide shared

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-05: The Kentucky Department Of Education Office Of Education Technology Should Formalize And Consistently Apply Logical Security Policies For The KETS Network And MUNIS (Continued)**

Management Response and Corrective Action Plan

services such as Active Directory and Exchange, OET will engage Microsoft to assist in analyzing this change to a productive environment before January 30, 2007. The extent of this project will depend on the analysis and recommended approach.

OET will initiate a process development discussion with other KDE Agency Offices, which require access to school district MUNIS servers, to establish an overall security access policy and access log strategy. The completion date for the discussion and analysis is August 30, 2006. Completion goal for implementation is January 30, 2007.

OET will immediately engage the KDE MUNIS business owners to review user and group accounts that are currently being used to ensure there is a legitimate business need for each. Alternative methods for secure access will also be discussed and evaluated. Any accounts that are not necessary will be immediately disabled. Review and completion of this is before October 30, 2006.

FINDING 06-EDU-06: The Kentucky Department Of Education Should Formalize The Task Order Process And Ensure Business Units Review Contractor Performance

During the audit of system controls at KDE for FY 2006, it was determined that KDE did not provide adequate oversight of the contracting and procurement process associated with critical IT personnel services within the agency. Further, OET did not formalize procedures involving contractor oversight and the procurement process to assure that Task Orders, contractor invoices, and contractor timesheets are complete, reviewed, and approved.

The Office of Internal Administration and Support (OIAS) performs the process of establishing a contract for services or commodities used within KDE. Each Business Unit requiring contracted services or commodities assists OIAS in this process. OIAS staff stated that once a contract is in place, the Business Owner is ultimately responsible to monitor the contract. KDE provided a listing of 36 contracts managed by the OET and used to procure technology-related products and services using KETS funds. Our testing revealed that while a Business Owner was not formally assigned to any of these contracts, an Executive Sponsor and Product Manager were assigned. According to OET, Business Owner and Product Manager are interchangeable terms.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-06: The Kentucky Department Of Education Should Formalize
The Task Order Process And Ensure Business Units Review Contractor Performance
(Continued)**

OIAS does have a Management Advisory Procedures (MAP) Manual that defines contracting terms and provides guidance concerning some contractual issues; however, the job function and responsibilities associated with a Business Owner, Executive Sponsor, or Product Manager have not been formally documented within this manual. It was also noted the TPC, which was created to ensure that technology-enabled business initiatives are successful, has defined the roles associated with an Executive Sponsor and Product Manager; however, the responsibilities associated with contract oversight have not been defined. As a result, the procurement process may suffer without a clear understanding of the roles and associated responsibilities.

In addition, KDE uses the Systems Development Services (SDS) contract to obtain IT-related contractors from various vendors. The SDS contract is procured through the Commonwealth Office of Technology (COT) and is an avenue for all Executive agencies to obtain project managers, programmers, consultants, and database analysts without having to go through an RFP process. The SDS contract allows KDE to attract highly skilled technical staff that it otherwise would not be able to hire and retain. Funding to support the payments for contractor labor is formally requested through a Task Order that is first approved by OIAS and then gets final approval from the Finance and Administration Cabinet. Only two employees within OIAS can approve Task Orders and other agreements on behalf of KDE. However, approval from the requesting Business Unit is not required on the Task Orders prior to OIAS providing approval.

Our audit revealed there is generally a lack of documentation concerning KDE management oversight of contractors involved with system related duties working within OET or other Business Units. Discussions with the agency revealed that OET is involved in the contract personnel hiring process in that they have the ability to interview and select the contractor that is hired from a vendor, as well as request replacements if necessary. Contractors working within OET are assigned to specific service teams, which report to one of two agency Directors. It was noted that some of the service teams are lead by other contractors. This organizational structure of contractors reporting to other contractors may not allow OET to adequately monitor the work performed by a contractor. Discussions revealed that the Directors do meet with contract staff periodically to ensure the goals of OET are achieved. However, minutes from these meetings are not formally documented. The two Directors within OET review and approve vendor-supplied invoices for contract labor on a monthly basis. In addition, the vendor provides OET with weekly timesheets for each contract employee. OET maintains a spreadsheet to track the total hours worked by each contractor by month and year-to-date, as well as the cost associated with these hours. However, documentation obtained during the course of our fieldwork did not provide any indication that OET management approves the weekly timesheets for contractors. Further, our testing indicated that various contractors have access to the OET maintained spreadsheets as a result of their assigned job duties.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-06: The Kentucky Department Of Education Should Formalize
The Task Order Process And Ensure Business Units Review Contractor Performance
(Continued)**

Without formalized and consistent procurement and contract monitoring procedures, KDE may not be obtaining adequate value for the contract services being provided. In addition, work productivity may suffer without clearly defined contract labor performance measures to ensure they are complying with standards set forth in the formal Task Order. Furthermore, the opportunity exists for contractor labor to alter the total number of hours they worked and may not actually be working the hours formally requested.

A formalized contract administration program is essential to assuring adequate contractor performance. Also, clearly defined contract management practices will ensure the state receives goods and services in a timely fashion and within budgeted constraints.

Recommendation

We recommend that KDE develop and formalize a contract management policy that addresses the Task Order process including compilation, review and approval. Each Business Unit should ensure that a Business Owner is formally assigned to a contract. OIAS and OET should work in conjunction to ensure adequate oversight has been delegated for all KETS system related contracts.

Also, each Business Unit requiring contractor labor should formalize procedures to monitor hours worked and performance measurement. Meetings held with service teams and contractor labor should be formally documented to ensure KDE can provide proper feedback to the vendor concerning work performed. Documentation used to monitor hours worked should be properly secured in a location that prevents unauthorized contractor access. In addition, guidelines for procedures to review and monitor contractor performance should be added to the annual Task Order and MAP manual to ensure contracted employees meet the standards established within the Task Order. OIAS should also update the Task Order Agreement form to allow the Business Units to provide documented initial approval.

Management Response and Corrective Action Plan

KDE is in full agreement with the recommendations contained herein. In response to this recommendation, KDE will, within 90 days:

- 1. Update the Management Advisory Procedures (MAP) Manual to include job function and responsibilities associated with a Business Owner, Executive Sponsor, or Project Manager.*
- 2. Via the Technology Planning Council (TPC), outline and document the responsibilities associated with contract oversight and formalize a contract management policy.*

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 06-EDU-06: The Kentucky Department Of Education Should Formalize
The Task Order Process And Ensure Business Units Review Contractor Performance
(Continued)**

Management Response and Corrective Action Plan

3. *Require signature approval from the Business Unit on all Task Orders prior to OIAS approval.*
4. *Prepare appropriate documentation to define and guarantee management oversight for contractor services involved with system-related duties working within KDE.*
 - *Require all contractors be monitored by the Project Manager for hours worked and tasks performed.*
 - *Require documentation of meetings between directors/managers of KDE who meet with contract staff to ensure that goals/initiatives of KDE are achieved.*
 - *Require that KDE management approve and retain the weekly timesheets of contractors. Establish a retention schedule to support such.*
 - *Evaluate contractor access to KDE financial and procurement systems to ensure there is no unauthorized access. Eliminate any identified access.*
5. *Create and enforce a contractor evaluation system.*
6. *Conduct periodic audits of the process. Correct and improve process, as needed.*

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 06-EDU-07: The Kentucky Department Of Education Should Ensure That All Open Ports On Agency Machines Have A Business-Related Purpose

During the security vulnerability assessments for FY 2006, we tested a total of 212 machines that were owned or managed by KDE and the local school districts. Our examination revealed two machines with ports open that may not have a specific business-related purpose. We have grouped the findings below by port number and application.

Port 3132 – unassigned

One machine was identified as having port 3132. The purpose of this port could not be determined as it is an unassigned port.

Port 443 – HTTPS/SSL

One machine was identified as having port 443 open, but would not display a website. When no default page or restricted logon is required, normally this means that no application/web service is running at the port.

Port 554 – RTSP

Two machines were identified as having port 554 open, which is the Real Time Stream Control Protocol service. We could not determine the validity of the service. One of these machines was located at a school district.

Port 1755 – ms-streaming

Two machines were identified as having port 1755 open, which is a Microsoft Netshow Command Port. We could not determine the validity of the service. One of these machines was located at a school district.

The auditor could not determine the necessity of many of these ports being open. Some, however, could be vital in order for KDE to conduct business. Therefore, the agency should review these ports to ensure they have a business-related purpose. If these ports are required to be open, then the proper security measures should be taken to protect them from vulnerability and ensure that no excessive system information is provided by any of the services that are retained.

The existence of unnecessary open ports increases potential security vulnerabilities and is an invitation for intruders to enter the system. Further, improperly secured services can provide excessive information to unauthorized users.

The existence of open ports is an invitation for intruders to enter your system. To minimize the risk of unauthorized access to a machine, only necessary, business-related ports should be open. Further, the application residing at these ports should be secured to the extent possible.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 06-EDU-07: The Kentucky Department Of Education Should Ensure That All Open Ports On Agency Machines Have A Business-Related Purpose (Continued)

Though one of these machines may be physically located within a school district and managed by the applicable district, KDE should work with the district as needed to help ensure the appropriate remedial action is taken.

Recommendation

We recommend that KDE ensure that all noted open ports are reviewed on the applicable machines housing KDE resources to assure a specific business-related purpose required the port to be open. If not required, then that port should be closed. If the port is necessary, then KDE should ensure adequate controls are implemented to prevent unauthorized access. We further recommend KDE encourage school districts to perform a similar review and remediation process for district servers.

Management Response and Corrective Action Plan

OET agrees with the recommendations and has quickly completed review of the 2 computers identified in comment KDE-SC1. One of the computers is managed by OET. OET has identified and verified the business-related purpose for each identified concern for this computer. OET has also reviewed the current access privileges and controls on the OET computer and find the access privileges and controls to be appropriate. There are no changes to the OET computers current configuration necessary.

The second computer is identified as owned and managed by a private business called SchoolCenter, based in Carbondale Illinois. A Kentucky school district outsources their school district web site to this vendor. OET has formulated an appropriate communication to this district's CIO concerning this issue so they can communicate the concern with this vendor.

KDE will encourage school districts to perform similar review and appropriate remediation of district servers.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 06-EDU-08: The Kentucky Department Of Education Should Ensure That All Agency Web Servers Have Updated Software And Security Patches Installed

During the FY 2006 security vulnerability assessments performed for 212 machines that were owned or managed by KDE and the local school districts, our examination revealed web service vulnerabilities present on two machines.

One server was noted with a remote access service that may allow unauthorized users to bypass authentication controls and obtain update capabilities on the server. One other server was noted as running an outdated and vulnerable Apache web service software. This version of software allows a buffer overflow that could be used to obtain elevated unauthorized access privileges. This latter server was actually located within a school district.

The vulnerabilities identified appear to result from outdated or unpatched software, and possibly due to installation of unnecessary services. These vulnerabilities could possibly allow an attacker from a remote location to execute arbitrary code and gain unauthorized access to machines within the agency system.

To maintain adequate security it is necessary to ensure all required web services are appropriately updated and all applicable security patches have been installed. Only necessary services should be implemented.

Though one of these machines may be physically located within a school district and managed by the applicable district, KDE should work with the district as needed to help ensure the appropriate action is taken to resolve the issue.

Recommendation

We recommend that KDE take the necessary actions to properly secure its machine to ensure the identified web services are appropriately updated or patched, and take other security measures as needed to eliminate the specified web service vulnerabilities. We further recommend that KDE disseminate information to the districts that identify methods to properly secure the district's machines and encourage the districts to implement security controls as necessary.

Management Response and Corrective Action Plan

OET agrees with the recommendations and has quickly completed review of the 2 computers identified in comment 06-EDU-08. One of the computers is managed by OET. OET has identified and has applied the appropriate recommendation to the OET computer.

The second computer is identified as owned and managed by a private business called SchoolCenter, based in Carbondale Illinois. A Kentucky school district

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Instances of Noncompliance*****FINDING 06-EDU-08: The Kentucky Department Of Education Should Ensure That All Agency Web Servers Have Updated Software And Security Patches Installed (Continued)**

Management Response and Corrective Action Plan

outsources their school district web site to this vendor. OET has formulated an appropriate communication to this district's CIO concerning this issue so they can communicate the concern with this vendor.

KDE will disseminate information to school districts and identify methods to properly secure their computers and will encourage districts to implement security controls as necessary.

FINDING 06-EDU-09: The Kentucky Department Of Education Should Develop A Formal Disaster Recovery Plan

During our audit of the system controls at KDE for FY 2006, we found that KDE had not developed or implemented a formalized Business Contingency Plan to address the backup and recovery of critical business servers, applications, and data. We noted the OET has established informal procedures that are followed in the case of temporary computer service disruptions. OET has also commenced work on a formal recovery plan; however, it is currently in the early stages of development. Our audit testing also revealed that though OET backs up system programs and data identified by KDE departments or Business Units as critical, they do not store those backups off-site. It was noted during discussions that KDE has implemented a "Business Champions" approach whereby critical services or programs are handled by specific Business Champions and those Champions are responsible for ensuring proper backup and recovery of their specific programs and data. However, we noted no central level authority designated to ensure these controls had been implemented or to roll the various Business Champion area recovery plans into an overall KDE recovery plan.

We also noted that OET had provided the 176 Kentucky School Districts with guidelines to assist with the backup of critical programs and data files. However, again, our audit revealed that there is no central level KDE oversight authority to ensure that school districts have completed a formalized recovery plan, as the school districts are not required to submit their contingency plans to any central level authority.

We are aware that OET is currently developing a KDE Enterprise Backup System. OET has identified a number of servers that will be a part of this backup process including servers used for the school district financial and staffing data transfer. The new backup system was designed to be used in conjunction with COT's backup service with the data being stored off-site utilizing the COT Off-Site Service. However, as noted this backup system is still in development.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 06-EDU-09: The Kentucky Department Of Education Should Develop A Formal Disaster Recovery Plan (Continued)

Failure to develop and implement a formalized disaster recovery plan increases the possibility of loss due to excessive recovery time, costs, and disruption of processing capabilities in the case of a disaster or extended system outage.

Good management practices minimize risks through planning. The goal of a disaster recovery plan is to improve preparedness for extended system outages at minimal cost using available resources. Disaster Recovery or Business Recovery Plans should be documented, approved, properly distributed, tested on a consistent basis, and updated as needed.

Recommendation

We recommend that OET formalize and implement the Disaster Recovery Plan that is currently being developed. OET should work with the other Business Units or “Business Champions” at KDE to ensure all critical servers and applications are included in this plan. The following should be taken into consideration when compiling a comprehensive KDE recovery plan:

- Request each of the KDE offices and departments to develop a Business Contingency Plan. These plans should be reviewed and updated annually as necessary to reflect emergency contacts, potential alternative processing sites, system descriptions and process requirements, backup procedures, and planned testing procedures. These plans should be approved and incorporated as part of the overall Disaster Recovery Plan currently being developed for KDE.
- Request all Kentucky school districts to develop a Business Contingency Plan that, at a minimum, addresses the backup and recovery of their MUNIS server, which should then be incorporated by reference as part of the overall Disaster Recovery Plan for KDE. District staff can use KDE’s formalized Business Contingency Plan as a guideline, but should understand that they are responsible for creating, testing, and updating a contingency plan that is specific to their school district. OET or another central level oversight authority should be assigned to review and approve all school districts’ contingency plans.
- OET, in conjunction with COT, should continue to develop and implement a formalized backup and recovery plan that also ensures critical backups are stored off-site. Once a plan is in place, it should be tested periodically and updated as necessary.
- The comprehensive KDE Disaster Recovery Plan should be properly distributed to key personnel and training should be provided to those personnel as needed. Needs for applicable recovery training for school districts should be considered and provided as necessary.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Instances of Noncompliance*****FINDING 06-EDU-09: The Kentucky Department Of Education Should Develop A Formal Disaster Recovery Plan (Continued)**

Management Response and Corrective Action Plan

OET agrees with all recommendations. OET will formalize and implement the Disaster Recovery Plan for those services that OET has management responsibility and authority. The Disaster Recovery Plan will be distributed to key personnel with appropriate training, including necessary school district personnel. For current OET managed services the Disaster Recovery Plan should be in place before December 30, 2007.

Currently OET and DPMR (Business Owners for the MUNIS financial application) have jointly engaged the MUNIS vendor, Tyler Technologies, concerning disaster recovery for the MUNIS financial function in Kentucky school districts. Tyler Technologies has developed a Disaster Recovery Service for the MUNIS application. OET and DPMR have successfully piloted this service in several Kentucky school districts. The service is currently a contractual item that can be procured, by districts, from the MUNIS or Tyler Technologies contract.

OET will continue to move the Data Backup and Recovery project forward. This should be fully implemented, against the current scope of work (SOW), by October 30, 2006. A component of this project is to identify appropriate rotation schedules, including off site storage and recovery testing procedures. The current off site storage vendor will continue to be used. We will increase capacity and rotational frequency to match the implementation schedule and identified business requirements.

FINDING 06-EDU-10: The Kentucky Department Of Education Office Of Education Technology Should Update And Consistently Apply Its Change Management Process

During the FY 2006 audit at KDE, we noted the OET has established a change management control process. The process is documented within the Change Management Change Request Procedures policy. However, that document does not address all necessary aspects of a change management control process, nor does it incorporate all of the actual processes currently implemented.

To help standardize the change management process, OET developed an Operations Change Request (OCR) Form. The steps on the form require approvals from the team lead and operations managers. In the case of an emergency, the Division manager's approval is required in addition to the other two approvals. Once all of these approvals have been placed on the request form, the request is given to the Change Management Administrator (CMA), who assigns a change request number. The request is then discussed in a weekly meeting of the Change Management Board to ensure that the request is complete, correct, and conflict-free.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 06-EDU-10: The Kentucky Department Of Education Office Of Education Technology Should Update And Consistently Apply Its Change Management Process (Continued)

Again, the established change management policy mainly addresses the proper completion of the OCR form. It does not address the Change Management Board's involvement or discuss the CMA's duties involving the assignment of change request numbers or change log maintenance. Further, it was determined that current change control procedures differ when the Kentucky Engineers are involved. The Kentucky Engineers submit change requests on behalf of the local school districts and can submit its own change requests and then function as both a team lead and an operations manager on its own behalf. This distinction is not documented within the existing policy.

Review of documentation maintained in support of the change management process revealed that a log was maintained for change requests. However, it was noted that the actual start and completion dates were missing for many change requests. Discussions revealed this occurred because the Change Request Owners (CROs) do not always notify the CMA when a change was completed.

We tested a sample of ten OCR forms and noted that seven, or 70 percent, were not properly authorized. Two of these OCRs specifically related to the MUNIS software releases that are distributed to the 176 Kentucky school districts. In addition, the OCR forms are transmitted via email to obtain and document the authorizations from all the responsible parties. The CMA maintains these e-mails historically. For each of the seven OCRs noted above, one or more of the required authorizations were noted as having been provided verbally. Therefore, adequate documentation of proper authorization did not exist.

Failure to implement adequate formalized change management controls could place the agency at risk that procedures deemed vital for secure change control will be overlooked. This increases the likelihood that unauthorized or inappropriate program changes could be placed in production.

Formal change management controls should be designed and implemented. Those controls should be properly disseminated to all responsible parties and be updated as necessary. Documentation should be maintained to provide adequate evidence of compliance with established change controls. Change controls should be consistently applied to all changes to existing programs and services.

Recommendation

We recommend that KDE update the change control policy to incorporate all current procedures performed applicable to the change management control process and ensure consistent compliance with the established requirements for change control. Specifically, the policies and procedures document should include, at a minimum:

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 06-EDU-10: The Kentucky Department Of Education Office Of Education Technology Should Update And Consistently Apply Its Change Management Process (Continued)

Recommendation

- The types of change that are required to be addressed within the Change Management process.
- Steps necessary to complete, authorize, and submit the Operations Change Request Form, including a differentiation between day-to-day and emergency situations.
- Roles that would require different submission procedures (i.e. Kentucky Engineers), and elaborate on those procedures.
- Additional authorization procedures other than a “Yes/No” or verbal approval on the Operations Change Request Form. A digital signature is acceptable on the request form, but it should be accompanied by e-mail correspondence. All parties required to authorize a change should provide expressed approval on the e-mail.
- Steps necessary for the Change Management Administrator to log, approve, and assign a change request number to the requested changes.
- Procedures to ensure that the Change Management Request Log is properly maintained and monitored.
- Procedures for maintaining all necessary e-mail approvals and request forms.
- Procedures for providing an alternate contact in the event that the Team Lead, Operations Manager, or Director is absent.
- The functionality of the Change Management Board, including who is involved in the process and how the process works.
- The process of assigning changes for completion within the team.
- The process that the Team Lead is to follow in order to notify the CMA upon change completion.

We are aware that the agency initiated the process of updating its policies and procedures; however, we believe that the proposed recommendations can easily be incorporated into the new policy development.

Management Response and Corrective Action Plan

OET agrees with all recommendations and has already initiated improvements in the change control process and will follow up to include all suggested recommendations. A complete OET Change Management Process will be complete by November 30, 2006.

Concerning the functionality of the Change Management Board, OET produced a specific charter upon implementation of this process within OET. OET will review this charter and update as appropriate to include all recent and planned improvements.

FINANCIAL STATEMENT FINDINGS

Other Matters Relating to Internal Controls and/or Instances of Noncompliance

FINDING 06-EDU-11: The Kentucky Department Of Education Should Formalize And Consistently Follow Formalized Procedures For Terminating Contract Employees

During the FY 2006 audit at KDE, we determined that KDE did not develop formal termination procedures for contract employees. The majority of IT-related contract employees are procured through the SDS contract and work within OET. OET works in conjunction with the Division of Human Resources within the OIAS as well as the Personnel Cabinet to ensure such things as payroll, benefits, and system or building access are handled appropriately for terminating state employees. The process begins when Human Resources receives a resignation letter from OET, at which time formal documentation is completed to ensure the employee's system and building accesses are removed. However, similar procedures are not in place for contract employees. OET does follow informal procedures by initiating a Help Desk Ticket via the Remedy System to have a contractor's system access removed.

Our discussions also revealed that the formalized termination procedures for employees are currently stored on a server that is primarily used as a file repository for all KDE employees to use. Certain security measures have been placed over the folder in which these procedures are maintained; however, there are a number of OET personnel that have access to them, which is not necessary given their job duties.

Without formalized termination procedures in place over contract employees, both logical and physical security could be compromised.

Termination procedures are necessary to protect the agency from data and property loss. Since several business units within KDE utilize contract employees, KDE should formalize termination procedures specific to employees on contract to ensure that necessary procedures are performed consistently.

Recommendation

We recommend that KDE formalize and consistently apply a termination policy for contract employees. This policy should be applied to all KDE contract employees and should consist of, but not be limited to, the following processes:

- The contract employee's access should be immediately revoked to all applications, programs, and files upon termination.
- The contract employee should forfeit his/her computer, e-mail account, e-mail archives, and all paper documentation.
- The contract employee's badge or entry card that permits entry to secure locations should be forfeited and the associated access should be promptly revoked.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Instances of Noncompliance*****FINDING 06-EDU-11: The Kentucky Department Of Education Should Formalize And Consistently Follow Formalized Procedures For Terminating Contract Employees (Continued)**

Management Response and Corrective Action Plan

The Kentucky Department of Education (the Department), Division of Human Resources (the Division) took this Audit and subsequent Audit Report as an opportunity to improve a process. The Division is in complete agreement with these findings and has made the following changes to address such: the Division is implementing a formal tracking procedure for all contract staff. This procedure will mirror the current procedure used for 18A employees, to the extent appropriate for Contract Employees. Upon identification of the need for a contract employee, the requesting office will route a “Contract e P-1”. The request will then process through all necessary and appropriate internal channels. Upon designation of the Contract Employee, a Personnel Activity Report will be routed within the Department. This form will begin computer, data, phone, and security access, where appropriate. The Contract Employee will complete a Contract Employee Orientation with the Division. The Division, upon notification of termination of a Contract Employee by the individual supervising said Contract Employee, will complete all termination procedures, per process, including but not limited to: immediately revoking access to all applications, programs and files, termination of access to all computer, e-mail account, e-mail archives and all paper documentation, and badge or entry card revocation. In an effort to complete the process, a separating Contract Employee will be requested to complete an Exit Interview. In summary, the enhancements made to the Contract Employee process should better manage the physical and system security at the Department and improve the Contract Employee’s experience with the Department.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2006

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
----------------	-------------------	---------	----------------	---------------------	----------

Reportable Conditions

(1) Audit findings that have been fully corrected:

There were no findings to report in this category.

(2) Audit findings not corrected or partially corrected:

There were no findings to report in this category.

(3) Corrective action taken is significantly different from corrective action previously reported:

There were no findings to report in this category.

(4) Audit finding no longer valid:

There were no findings to report in this category.

Material Weaknesses/Noncompliances

(1) Audit findings that have been fully corrected:

There were no findings to report in this category.

(2) Audit findings not corrected or partially corrected:

There were no findings to report in this category.

(3) Corrective action taken is significantly different from corrective action previously reported:

There were no findings to report in this category.

(4) Audit finding no longer valid:

There were no findings to report in this category.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2006

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
----------------	-------------------	---------	----------------	---------------------	----------

Other Matters

(1) Audit findings that have been fully corrected:

FY 05	05-EDU-01	The Kentucky Department Of Education Should Implement Procedures To Ensure All Budget Information Is Adequately Reported For Procard Purchases	N/A	0	Resolved in FY 06.
-------	-----------	--	-----	---	--------------------

(2) Audit findings not corrected or partially corrected:

There were no findings to report in this category.

(3) Corrective action taken is significantly different from corrective action previously reported:

There were no findings to report in this category.

(4) Audit finding no longer valid:

There were no findings to report in this category.