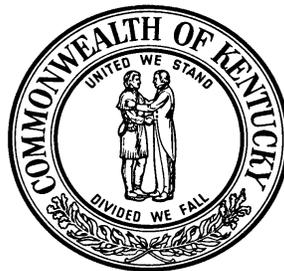


**REPORT OF THE STATEWIDE SINGLE AUDIT OF THE
COMMONWEALTH OF KENTUCKY**

VOLUME I

**For the Year Ended
June 30, 2010**



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

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

The Statewide Single Audit of the Commonwealth of Kentucky
Volume I
For the Year Ended June 30, 2010

Background

The Single Audit Act of 1984, subsequent amendments, and corresponding regulations, requires an annual audit of the financial statements and compliance with requirements applicable to major federal programs. The Auditor of Public Accounts (APA) meets these requirements and submits audit findings required to be reported by auditing standards generally accepted in the United States of America, *Government Auditing Standards* and OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*, through our opinion on the Commonwealth's Comprehensive Annual Financial Report (CAFR) and through the Statewide Single Audit of Kentucky (SSWAK). Our SSWAK report is contained in two volumes as noted below.

SSWAK - Volume I contains financial reporting information based on our audit of the CAFR. It includes the APA's opinion on the Schedule of Expenditures of Federal Awards (SEFA) in relation to the financial statements, the *Report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with Government Auditing Standards*, and financial statement findings related to internal control and compliance.

SSWAK - Volume II will present elements required under OMB Circular A-133, including the *Report on Compliance with Requirements Applicable to Each Major Program and on Internal Control over Compliance in Accordance with OMB Circular A-133*, and the Schedule of Findings and Questioned Costs.

Comprehensive Annual Financial Report

The CAFR, including our report thereon based on our audit and the reports of other auditors, has been issued under separate cover. We identified in our Independent Auditor's Report on the CAFR the percentages of various funds and component units audited by other auditors. The agencies and funds audited by other auditors, as well as contact information, are presented in the Appendix of this report.

The scope of the CAFR audit included:

- An audit of the basic financial statements and combining financial statements;
- Limited procedures applied to required supplementary information;
- An audit of the SEFA sufficient to give an opinion in relation to the basic financial statements; and,
- Tests of compliance with certain provisions of laws, regulations, contracts, and grants, and tests of internal controls, where applicable.

The Statewide Single Audit of the Commonwealth of Kentucky
Volume I
For the Year Ended June 30, 2010

Background (Continued)

Schedule of Expenditures of Federal Awards

The SEFA presented within this report is organized by federal grantor. The Catalog of Federal Domestic Assistance (CFDA) numbers and program names are listed under the federal grantor administering the program. The state agencies expending the federal funds are listed beside each CFDA number. The notes to the SEFA provide more detailed information on certain aspects of the expenditures. Clusters of programs are indicated in the schedule by light gray shading. The identification of major federal programs and our report thereon will be presented in our report *SSWAK - Volume II*.

For fiscal year ended June 30, 2010, the total federal dollars expended by the Commonwealth of Kentucky was \$ 10,401,012,066 in cash awards and \$ 1,245,313,065 in noncash awards. For fiscal year 2010, the total federal cash expenditures as reported on the SEFA increased in comparison with the total for June 30, 2009.

Component Units

The reporting entity of the Commonwealth of Kentucky for the purposes of the CAFR includes various discretely presented component units, including state universities, identified in accordance with GASBS No. 14 and 39. However, except for CAFR reporting, the Commonwealth has elected to exclude discretely presented component units from the statewide single audit. Thus, these discretely presented component units, including state universities, are not included in the accompanying SEFA and reports on internal control and compliance over financial reporting. These entities are still required to have audits performed in accordance with the provisions of OMB Circular A-133, *Audits of States, Local Governments, and Non-Profit Organizations*, if applicable, based on their total federal expenditures.



CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

February 11, 2011

Honorable Steven L. Beshear, Governor
Cabinet Secretaries and Agency Heads
Members of the Commonwealth of Kentucky Legislature

As Auditor of Public Accounts, I am pleased to transmit herewith our report of the Statewide Single Audit of Kentucky - Volume I for the year ended June 30, 2010. Volume I contains financial statement findings identified during our audit of the Comprehensive Annual Financial Report (CAFR), the Schedule of Expenditures of Federal Awards (SEFA), related notes, and our opinion thereon, as well as the report on Internal Control over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with *Government Auditing Standards*.

We will subsequently report to you the required elements of the Federal government's Office of Management and Budget (OMB) Circular A-133 in Volume II of this report upon completion of our audit of the Commonwealth's major federal programs.

On behalf of the Office of Financial Audits of the Auditor of Public Accounts, I wish to thank the employees of the Commonwealth for their cooperation during the course of our audit. Should you have any questions concerning this report, please contact Sally Hamilton, Executive Director, Office of Financial Audits, or me.

Respectfully submitted

A handwritten signature in black ink that reads "Crit Luallen".

Crit Luallen
Auditor of Public Accounts



CONTENTS

Page

List of Abbreviations/Acronym	1
Independent Auditor’s Report.....	5
Schedule of Expenditures of Federal Awards:	
U.S. Department of Agriculture.....	9
U.S. Department of Commerce.....	10
U.S. Department of Defense	10
U.S. Department of Housing and Urban Development	10
U.S. Department of the Interior	10
U.S. Department of Justice	11
U.S. Department of Labor.....	13
U.S. Department of Transportation.....	14
U.S. Department of Treasury	15
U.S. Appalachian Regional Commission.....	15
U.S. Equal Employment Opportunity Commission.....	15
U.S. General Services Administration	15
National Aeronautics and Space Administration	15
U.S. National Foundation on the Arts and the Humanities.....	15
U.S. Department of Veterans Affairs.....	15
U.S. Environmental Protection Agency.....	15
U.S. Department of Energy.....	16
U.S. Department of Education.....	17
U.S. National Archives and Records Administration	19
U.S. Election Assistance Commission.....	19
U.S. Department of Health and Human Services	19
U.S. Corporation for National and Community Service.....	21
U.S. Office of National Drug Control Policy	22
U.S. Social Security Administration.....	22
U.S. Department of Homeland Security	22
Other Federal Assistance	23
Notes to the Schedule of Expenditures of Federal Awards	24
Report on Internal Control Over Financial Reporting and on Compliance and Other Matters Based on an Audit of Financial Statements Performed in Accordance with Government Auditing Standards	37
<i>Financial Statement Findings</i>	
Material Weaknesses Relating to Internal Controls and/or Noncompliances	
<u>FINDING 10-KST-1</u> : The Kentucky State Treasury Should Reconcile The Commonwealth’s Bank Accounts To eMARS In A Timely Manner	41

CONTENTS

(Continued)

Page

Financial Statement Findings (Continued)

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-CHFS-2: The Cabinet For Health And Family Services Should Develop Procedures To Ensure Accuracy And Completeness Of Non-Cash Expenditures Reported In The SEFA..... 42

FINDING 10-CHFS-3: The Cabinet For Health And Family Services Should Have Controls In Place To Ensure Financial Reports Are Complete And Accurate..... 44

FINDING 10-CHFS-4: The Cabinet For Health And Family Services Hazelwood Facility Should Ensure Invoices Are Paid In A Timely Manner..... 45

FINDING 10-CHFS-5: The Cabinet For Health And Family Services Should Provide Additional Guidance And Oversight At The Hazelwood Facility 47

FINDING 10-CHFS-6: The Cabinet For Health And Family Services Should Improve Policies And Procedures Over Its Imprest Cash Accounts 49

FINDING 10-CHFS-7: The Cabinet For Health And Family Services Should Strengthen Policies And Procedures To Ensure That Appropriate Documentation And Authorization For Expenditures Are Maintained At The Hazelwood Facility..... 51

FINDING 10-DOC-8: The Department Of Corrections Should Expand, Finalize, And Implement A System Development Life Cycle Policy To Govern System Development, Testing, Modifications And Implementation 53

FINDING 10-DOC-9: The Department Of Corrections Should Strengthen And More Closely Adhere To The Kentucky Offender Management System (KOMS) Defect Management Process 55

FINDING 10-DOC-10: The Department Of Corrections Should Formalize And Consistently Apply Logical Security Controls Over KRONOS..... 58

FINDING 10-DOC-11: The Department Of Corrections Should Complete Implementation Of Information Technology Security Policies 60

FINDING 10-DOC-12: The Department Of Corrections Should Ensure All Agency Machines Are Properly Configured To Include Only Necessary Services 62

FINDING 10-DOC-13: The Department Of Corrections Should Ensure Sufficient Authentication Is Required To Access Potentially Sensitive Information 63

FINDING 10-DOC-14: The Department Of Corrections Should Ensure Necessary Steps Are Taken To Mitigate Identified Vulnerabilities On Agency Machines 64

FINDING 10-DWI-15: Unemployment Insurance Should Implement Procedures To Ensure Its Accounts Payable Estimate Is Accurate And Complete..... 65

FINDING 10-DWI-16: The Department For Workforce Investment Should Strengthen The Disaster Recovery Plan..... 66

FINDING 10-DWI-17: The Office Of Employment And Training Should Develop Formal System Documentation To Support Processing Performed By The Workforce Investment Act Online Reporting Of Kentucky System 68

FINDING 10-DWI-18: The Office Of Employment And Training Should Strengthen And Consistently Apply Administrative Logical Security Procedures Over The Workforce Investment Act Online Reporting Of Kentucky System..... 70

CONTENTS

(Continued)

Page

Financial Statement Findings (Continued)

Significant Deficiencies Relating to Internal Controls and/or Noncompliances (Continued)

FINDING 10-DWI-19: The Office Of Employment And Training Should Ensure Programmatic Logical Security Controls Are Properly Designed And Configured 74

FINDING 10-FAC-20: The Finance And Administration Cabinet Should Ensure Formalized Policies Are Developed And Implemented Governing Security Over Microsoft Outlook Public Folders..... 78

FINDING 10-FAC-21: The Finance And Administration Cabinet Should Ensure Anonymous Access Is Limited Through Network Neighborhood..... 80

FINDING 10-FAC-22: The Finance And Administration Cabinet Should Expand Logical Security Over The UNIX Servers 81

FINDING 10-FAC-23: The Finance And Administration Cabinet Should Formalize And Consistently Apply A Policy To Govern The Security Of The eMARS Production Databases 84

FINDING 10-FAC-24: The Finance And Administration Cabinet Should Develop And Implement A Formal Policy To Govern Security Of The eMARS Checkwriter Interface Process 87

FINDING 10-FAC-25: The Finance and Administration Cabinet Should Ensure All Reporting From infoAdvantage Is Accurate and Complete 89

FINDING 10-KDE-26: The Kentucky Department Of Education Should Develop A Formal Disaster Recovery Plan And Formalize Backup Procedures 92

FINDING 10-KDE-27: The Kentucky Department Of Education’s Office Of Education Technology Should Expand And Consistently Apply Logical Security Policies For The KETS Network And MUNIS..... 94

FINDING 10-KDE-28: The Kentucky Department Of Education’s Office Of Education Technology Should Consistently Apply Program Modification Procedures..... 99

FINDING 10-KDE-29: The Kentucky Department Of Education Should Ensure All Agency Machines Are Properly Configured To Include Only Necessary Services..... 101

FINDING 10-KDE-30: The Kentucky Department Of Education’s Office Of District Support Services Should Expand And Consistently Apply Its Logical Security Policies 102

FINDING 10-KDE-31: The Division Of Nutrition And Health Services Should Develop, Implement, And Consistently Apply A Formal Logical Security Policy 106

FINDING 10-KDE-32: The Division Of Nutrition And Health Services Should Ensure Proper Segregation Of Duties..... 109

FINDING 10-KDE-33: The Division Of Nutrition And Health Services Should Develop Formal System Documentation To Support Processing Performed By The Nutrition And Health Services Payment Application..... 111

FINDING 10-KDE-34: The Division Of Nutrition And Health Services Should Enable System Auditing On Its Nutrition And Health Services Payment System..... 113

FINDING 10-KHP-35: The Kentucky Horse Park Should Enforce Controls Regarding Payroll Records And Segregate Duties For Payroll And Personnel Activities 115

CONTENTS

(Continued)

	Page
<i>Financial Statement Findings (Continued)</i>	
Significant Deficiencies Relating to Internal Controls and/or Noncompliances (Continued)	
<u>FINDING 10-KHP-36</u> : The Kentucky Horse Park Should Ensure Invoices Are Paid Timely	118
<u>FINDING 10-KSP-37</u> : The Kentucky State Police Clothing Allowance Payments Should Be Reported As Taxable Fringe Benefits	120
<u>FINDING 10-KST-38</u> : The Kentucky State Treasury Should Strengthen System Security Settings And Values.....	122
<u>FINDING 10-KST-39</u> : The Kentucky State Treasury Should Improve Segregation Of Duty Controls.....	124
<u>FINDING 10-KST-40</u> : The Kentucky State Treasury Should Strengthen Logical Security Controls To Ensure Only Authorized Users Can Access The Data Processing System	128
<u>FINDING 10-KST-41</u> : The Kentucky State Treasury Should Ensure Critical Libraries Are Adequately Secured To Protect System Resources	132
<u>FINDING 10-KST-42</u> : The Kentucky State Treasury Should Update Formal System Documentation To Reflect Processing Performed.....	134
<u>FINDING 10-KST-43</u> : The Kentucky State Treasury Should Develop And Implement An Application Security Policy Related To The Data Processing System.....	137
<u>FINDING 10-KST-44</u> : The Kentucky State Treasury Should Enable System Auditing On Its Data Processing System	139
<u>FINDING 10-KST-45</u> : The Kentucky State Treasury Should Expand And Strengthen Formal Program Change Control Procedures.....	140
<u>FINDING 10-PARKS-46</u> : The Department Of Parks Should Ensure That Vendors Are Paid Timely In Compliance With Statute	143
<u>FINDING 10-PARKS-47</u> : The Department Of Parks Should Ensure That Timesheets And Leave Forms Are Completed And Approved To Support Payroll Expenditures	144
<u>FINDING 10-PC-48</u> : The Personnel Cabinet Should Ensure Sufficient Authentication Is Required To Access Potentially Sensitive Information	146
<u>FINDING 10-PC-49</u> : The Personnel Cabinet Should Strengthen Logical Security Procedures Over The Uniform Personnel And Payroll System.....	147
<u>FINDING 10-REV-50</u> : The Department Of Revenue Should Strengthen Logical Security Controls Over The On-Line System For The Collection Of Accounts Receivable.....	149
<u>FINDING 10-TC-51</u> : The Transportation Cabinet Should Ensure Inventory Values Entered By Personnel Are Reasonable.....	151
<u>FINDING 10-TC-52</u> : The Transportation Cabinet Should Implement Procedures To Ensure Compliance With Kentucky Laws For Transferring Property.....	152
<u>FINDING 10-TC-53</u> : The Transportation Cabinet In Coordination With The Commonwealth Office Of Technology Should Strengthen The Security Of System Accounts.....	154
Appendix	159

LIST OF ABBREVIATIONS/ACRONYMS

**COMMONWEALTH OF KENTUCKY
LIST OF ABBREVIATIONS/ACRONYMS
FOR THE YEAR ENDED JUNE 30, 2010**

ACH	Automated Clearing House
ADB	Agriculture Development Board
AFR	Annual Financial Report
AGR	Department of Agriculture
AOC	Administrative Office of the Courts
APA	Auditor of Public Accounts
ARRA	American Recovery and Reinvestment Act
BCP	Business Contingency Plan
BDC	Backup Domain Controller
BHDID	Behavioral Health, Developmental and Intellectual Disabilities
CAFR	Comprehensive Annual Financial Report
CAMRA	Complete Asset Management Reporting and Accounting
CDC	Centers for Disease Control
CED	Cabinet for Economic Development
CFDA	Catalog of Federal Domestic Assistance
CHFS	Cabinet for Health and Family Services
CICS	Customer Information Control System
CIO	Chief Information Officer
CMA	Commission on Military Affairs
Commonwealth	Commonwealth of Kentucky
CORR	Department of Corrections
COT	Commonwealth Office of Technology
CPA	Certified Public Accountant
CW	Checkwriter
CWC	Checkwriter Cancellation
DC	Domain Controller
DCJT	Department of Criminal Justice Training
DCTRL	Document Control
DLA	Department of Libraries and Archives
DLG	Department for Local Government
DMS	Department for Medicaid Services
DNHS	Division of Nutrition and Health Services
DOC	Department of Corrections
DOR	Department of Revenue
DoS	Denial of Service
DPM	Data Protection Manager
DRP	Disaster Recovery Plan
DSC	Designated Security Contacts
DTS	Division of Technology Services
DWI	Department for Workforce Investment
EDU	Department of Education
EEC	Energy and Environment Cabinet
eMARS	enhanced Management Administrative Reporting System
ePAY	ePayment Gateway
EPPC	Environmental and Public Protection Cabinet

**COMMONWEALTH OF KENTUCKY
LIST OF ABBREVIATIONS/ACRONYMS
FOR THE YEAR ENDED JUNE 30, 2010
(Continued)**

EPSB	Education Professional Standards Board
ERQ	Event Requirements
F&W	Department of Fish and Wildlife Resources
FAC	Finance and Administration Cabinet
FAP	Finance and Administration Cabinet Policy
FICA	Federal Insurance Contributions Act
Finance	Finance and Administration Cabinet
FSC	Forward Schedule of Changes
FTP	File Transfer Protocol
FY	Fiscal Year
GASB	Governmental Accounting Standards Board
GAX	General Accounting Expense/Expenditure
GSA	Government Services Administration
HR	Human Resource
HRC	Kentucky Commission on Human Rights
HTTP	Hyper Text Transfer Protocol
ID	Identification
IRS	Internal Revenue Service
IT	Information Technology
ITSM	Information Technology Service Management
JUST	Justice and Public Safety Cabinet
JUV	Department of Juvenile Justice
KAC	Kentucky Arts Council
KASBO	Kentucky Association of School Business Officials
KBE	Kentucky Board of Elections
KDE	Kentucky Department of Education
KETS	Kentucky Education Technology System
KHC	Kentucky Heritage Council
KHEAA	Kentucky Higher Education Assistance Authority
KHP	Kentucky Horse Park
KHRIS	Kentucky Human Resource Information System
KHS	Kentucky Historical Society
KIP	Kentucky Immunization Program
KOEP	Kentucky Office of Energy Policy
KOHS	Kentucky Office of Homeland Security
KOMS	Kentucky Offender Management System
KRS	Kentucky Revised Statute
KSP	Kentucky State Police
KST	Kentucky State Treasury
KVE	Kentucky Vehicle Enforcement
KVP	Kentucky Vaccine Program
KY	Kentucky
KY OSCAR	Kentucky On-line System for Collection of Accounts Receivable
KYSTE	Kentucky Society for Technology in Education

**COMMONWEALTH OF KENTUCKY
LIST OF ABBREVIATIONS/ACRONYMS
FOR THE YEAR ENDED JUNE 30, 2010
(Continued)**

KYTC	Kentucky Transportation Cabinet
LABOR	Labor Cabinet
LWIA	Local Workforce Investment Area
MARS	Management Administrative Reporting System
MHMR	Department for Mental Health and Mental Retardation Services
MIL	Military Affairs
MSF	Microsoft Solutions Framework
MUNIS	Municipal Information System
NA	Not Applicable
NHSP	Nutrition and Health Services Payment
NSF	Non Sufficient Funds
OAG	Office of Attorney General
OB1	Management Budget
OC	Office of the Controller
ODSS	Office of District Support Services
OET	Office of Education Technology
OET	Office of Employment Training
OFM	Office of Financial Management
OMB	Office of Management and Budget
OMS	Operations Management System
PARKS	Department of Parks
PC	Personnel Cabinet
PDC	Primary Domain Controller
Personnel	Personnel Cabinet
PHA	Public Health Advisor
PPC	Public Protection Cabinet
PRC	Commodity Based Purchase Request
PRCI	Commodity Based Internal Payment Requisition
PUBAD	Department of Public Advocacy
R&D	Research and Development
REV	Department of Revenue
RFC	Request for Change
SAS	Statewide Accounting Services
SDLC	System Development Life Cycle
SEEK	Support Education Excellence in Kentucky
SEFA	Schedule of Expenditures of Federal Awards
SME	Subject Matter Expert
SNAP	Supplemental Nutritional Assistance Program
SOS	Secretary of State
SP	State Park
SR	Solicitation Response
SRP	State Resort Park
SRW	Solicitation Response Wizard
SSWAK	Statewide Single Audit of Kentucky

**COMMONWEALTH OF KENTUCKY
LIST OF ABBREVIATIONS/ACRONYMS
FOR THE YEAR ENDED JUNE 30, 2010
(Continued)**

T&A	Time and Attendance
TAH	Tourism, Arts, and Heritage Cabinet
TC	Transportation Cabinet
Treasury	Kentucky State Treasury
UI	Unemployment Insurance
UIA	Unemployment Insurance Accounts
UIB	Unemployment Insurance Benefits
UNIX	Uniplexed Information and Computing System
UPPS	Uniform Personnel and Payroll System
UPS	Unified Prosecutorial System
US	United States
USDA	United States Department Of Agriculture
VA	Department of Veterans' Affairs
VFC	Vaccines for Children
WIA	Workforce Investment Act
WORK	Online Reporting of Kentucky
WRX	Wage Records Systems
XSS	Cross Site Scripting
Y2K	Year 2000



CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

Honorable Steven L. Beshear, Governor
Cabinet Secretaries and Agency Heads
Members of the Commonwealth of Kentucky Legislature

Independent Auditor's Report

We have audited the financial statements of the governmental activities, business-type activities, the aggregate discretely presented component units, each major fund, and the aggregate remaining fund information of the Commonwealth of Kentucky as of and for the year ended June 30, 2010, and have issued our report thereon dated December 17, 2010. Our audit was conducted for the purpose of forming opinions on the financial statements that collectively comprise the Commonwealth's basic financial statements. The accompanying schedule of expenditures of federal awards is presented for purposes of additional analysis as required by OMB Circular A-133 and is not a required part of the basic financial statements. Such information has been subjected to the auditing procedures applied in the audit of the basic financial statements taken as a whole.

The schedule of expenditures of federal awards is prepared on the basis of cash disbursements as modified by the application of KRS 45.229. Consequently, certain expenditures are recorded in the accounts only when cash is disbursed and not when incurred.

In our opinion, except for the effects of the application of a different basis of accounting, as explained above, the schedule of expenditures of federal awards is fairly stated, in all material respects, in relation to the Commonwealth's basic financial statements taken as a whole.

This report is intended solely for the information and use of management, members of the legislature, and federal awarding agencies and pass-through entities, and is not intended to be and should not be used by anyone other than these specified parties.

Respectfully submitted,

A handwritten signature in black ink, appearing to read "Crit Luallen".

Crit Luallen
Auditor of Public Accounts

December 17, 2010



SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS

COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Agriculture					
Direct Programs:					
10.025	Plant and Animal Disease, Pest Control, and Animal Care (Note 7)	AGR	\$ 552,381	\$	\$
		F&W	40,539		
10.028	Wildlife Services (Note 7)	F&W	15,086		
10.066	Livestock Assistance Program (Note 15)	AGR			
10.069	Conservation Reserve Program	EEC	16,234		
10.086	ARRA-Aquaculture Grants Program (AGP) (Note 14)	ADB	53,261		
10.153	Market News	AGR	9,387		
10.156	Federal-State Marketing Improvement Program	AGR	135		
10.163	Market Protection and Promotion	AGR	74,002		
10.169	Specialty Crop Block Grant Program	AGR	84,883		
10.170	Specialty Crop Block Grant Program-Farm Bill	AGR	97,610		
Supplemental Nutrition Assistance Program Cluster:					
10.551	Supplemental Nutrition Assistance Program (Note 2) (Note 11) (Note 16)	CHFS		1,164,591,491	
10.561	State Administrative Matching Grants for the Supplemental Nutrition Assistance Program (Note 2)	CHFS	43,123,864		7,813,168
10.561	ARRA-State Administrative Matching Grants for the Supplemental Nutrition Assistance Program (Note 2) (Note 14)	CHFS	5,313,750		187,352
Child Nutrition Cluster:					
10.553	School Breakfast Program (Note 2)	EDU	59,206,813		59,121,200
		JUV	474,072		
10.555	National School Lunch Program (Note 2) (Note 11)	EDU	165,822,650		165,657,063
		AGR		20,296,803	
		JUV	848,782		
10.556	Special Milk Program for Children (Note 2)	EDU	82,376		82,376
10.559	Summer Food Service Program for Children (Note 2)	EDU	7,269,789		7,214,968
10.557	Special Supplemental Nutrition Program for Women, Infants, and Children (Note 2)	CHFS	125,228,544		22,748,532
10.558	Child and Adult Care Food Program (Note 2)	EDU	31,125,962		30,788,439
10.560	State Administrative Expenses for Child Nutrition	EDU	2,071,378		20,770
		AGR	298,714		
10.565	Commodity Supplemental Food Program (Note 11) (Note 12)	AGR	982,211	3,254,679	
Emergency Food Assistance Cluster:					
10.568	Emergency Food Assistance Program (Administrative Costs)	AGR	1,340,386		
10.568	ARRA-Emergency Food Assistance Program (Administrative Costs) (Note 14)	AGR	826,903		
10.569	Emergency Food Assistance Program (Food Commodities) (Note 11)	AGR		8,983,247	
10.572	WIC Farmers' Market Nutrition Program (FMNP)	CHFS	120,055		
		AGR	147		
10.574	Team Nutrition Grants (Note 15)	EDU			
10.576	Senior Farmers Market Nutrition Program	AGR	306,454		
10.579	ARRA-Child Nutrition Discretionary Grants Limited Availability (Note 14)	EDU	1,769,340		
10.582	Fresh Fruit and Vegetable Program	EDU	1,002,480		994,834
10.652	Forestry Research	EEC	454,204		
10.664	Cooperative Forestry Assistance (Note 11)	EEC	3,125,541	47,799	828,336
10.676	Forest Legacy Program	EEC	32,722		
10.678	Forest Stewardship Program	EEC	118,924		
10.680	Forest Health Protection	EEC	66,342		58,258
10.769	Rural Business Enterprise Grants (Note 15)	AGR			

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. Department of Agriculture (Continued)</u>					
Direct Programs (Continued):					
10.771	Rural Cooperative Development Grants (Note 15)	AGR			
10.902	Soil and Water Conservation	EEC	612,071		3,601
		F&W	429,308		
10.913	Farm and Ranch Lands Protection Program	AGR	830,939		
10.914	Wildlife Habitat Incentive Program (Note 15)	EEC			
		F&W			
10.NA(1)	Rural Rehabilitation Student Loan Program (Note 3)	AGR	145,426		
Total U.S. Department of Agriculture			\$ 453,973,665	\$ 1,197,174,019	\$ 295,518,896
<u>U.S. Department of Commerce</u>					
Direct Programs:					
Public Works and Economic Development Cluster:					
11.307	Economic Adjustment Assistance (Note 15)	DLG	\$	\$	\$
11.469	Congressionally Identified Awards and Projects (Note 15)	PARKS			
11.555	Public Safety Interoperable Communications Grant Program	KSP	5,263,575		
		KOHS	1,843,719		1,821,523
11.558	State Broadband Data and Development Grant Program	COT	490,538		
Total U.S. Department of Commerce			\$ 7,597,832	\$ 0	\$ 1,821,523
<u>U.S. Department of Defense</u>					
Direct Programs:					
12.002	Procurement Technical Assistance For Business Firms	CED	\$ 131,020	\$	\$
12.113	State Memorandum of Agreement Program for the Reimbursement of Technical Services	EEC	125,615		
12.400	Military Construction, National Guard	MIL	3,098,869		
12.401	National Guard Military Operations and Maintenance (O & M) Projects	MIL	19,594,387		
12.401	ARRA-National Guard Military Operations and Maintenance (O & M) Projects (Note 14)	MIL	3,258,736		
12.404	National Guard Challenge Program	MIL	1,968,617		
12.607	Community Economic Adjustment for Establishment, Expansion, Realignment, or Closure of a Military Installation	CMA	285,700		
12.700	Donations/Loans of Obsolete DOD Property (Note 11)	KSP		267,437	
12.NA(1)	Chemical Demilitarization and Remediation Activity for Hazardous Waste Activities at Chemical Demilitarization Facilities	EEC	390,160		14,769
12.NA(2)	Monitoring of Wildlife	F&W	693,887		
12.NA(3)	Teacher and Teacher's Aide Placement Assistance Program	EPSB	81,176		
Total U.S. Department of Defense			\$ 29,628,167	\$ 267,437	\$ 14,769
<u>U.S. Department of Housing and Urban Development</u>					
Direct Programs:					
Community Development Block Grants-State-Administered Small Cities Program					
14.228	Community Development Block Grants/State's Program and Non-Entitlement Grants in Hawaii (Note 2) (Note 8)	DLG	\$ 40,116,857	\$	\$ 38,556,573
14.255	ARRA-Community Development Block Grants/State's program and Non-Entitlement Grants in Hawaii (Note 14)	DLG	1,567,844		1,561,107
14.401	Fair Housing Assistance Program-State and Local	HRC	128,021		
14.408	Fair Housing Initiatives Program	HRC	12,746		
14.251	Economic Development Initiative-Special Project, Neighborhood Initiative and Miscellaneous Grants	PARKS	21,774		
Total U.S. Department of Housing and Urban Development			\$ 41,847,242	\$ 0	\$ 40,117,680
<u>U.S. Department of the Interior</u>					
Direct Programs:					
15.250	Regulation of Surface Coal Mining and Surface Effects of Underground Coal Mining (Note 11)	EEC	\$ 11,041,810	\$ 26,193	\$ 49,859

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of the Interior (Continued)					
Direct Programs (Continued):					
15.252	Abandoned Mine Land Reclamation (AMLR) Program	EEC	26,466,848		10,723,985
15.255	Applied Science Program Cooperative Agreements Related to Coal Mining and Reclamation	EEC	28,682		
Fish and Wildlife Cluster:					
15.605	Sport Fish Restoration Program (Note 7)	F&W	5,068,221		
15.611	Wildlife Restoration (Note 9)	F&W	6,683,505		
15.614	Coastal Wetlands Planning, Protection and Restoration Act	F&W	16,684		
15.615	Cooperative Endangered Species Conservation Fund (Note 7)	F&W	308,410		
		EEC	55,637		
15.616	Clean Vessel Act	F&W	85,320		
15.622	Sportfishing and Boating Safety Act	F&W	124,975		
15.623	North American Wetlands Conservation Fund	EEC	9,000		
15.632	Conservation Grants Private Stewardship for Imperiled Species (Note 15)	F&W	62,064		
		EEC			
15.633	Landowner Incentive Program	F&W	229,117		
15.634	State Wildlife Grants (Note 7)	F&W	1,173,994		
15.657	Endangered Species Conservation-Recovery Implementation Funds (Note 11)	EEC		3,276	
15.656	ARRA-Recovery Act-Habitat Enhancement, Restoration and Improvement (Note 14)	F&W	1,904		
15.808	U.S. Geological Survey-Research and Data Collection (Note 15)	EEC	1,088		
		COT			
15.809	National Spatial Data Infrastructure Cooperative Agreements Program	COT	4,152		
15.904	Historic Preservation Fund Grants-In-Aid	KHC	851,850		81,596
15.916	Outdoor Recreation-Acquisition, Development and Planning (Note 10) (Note 6)	DLG	544,951		543,081
		PARKS	964		
Total U.S. Department of the Interior			<u>\$ 52,759,176</u>	<u>\$ 29,469</u>	<u>\$ 11,398,521</u>
U.S. Department of Justice					
Direct Programs:					
16.003	Law Enforcement Assistance-Narcotics and Dangerous Drugs Technical Laboratory Publications (Note 15)	COT	\$	\$	\$
16.202	Prisoner Reentry Initiative Demonstration	CORR	97,239		
16.203	Comprehensive Approaches to Sex Offender Management Discretionary Grant (Note 15)	JUV	85,552		
		CORR			
		JUST			
16.523	Juvenile Accountability Block Grants (Note 15)	JUV	499,397		42,097
		AOC	54,862		
		UPS	33,798		
		PUBAD			
16.540	Juvenile Justice and Delinquency Prevention-Allocation to States	JUV	909,046		629,972
16.543	Missing Children's Assistance	KSP	389,838		
16.548	Title V-Delinquency-Prevention Program	JUV	155,506		155,337
16.549	Part E-State Challenge Activities (Note 15)	JUV			
16.550	State Justice Statistics Program for Statistical Analysis Centers	JUST	65,117		
16.554	National Criminal History Improvement Program (NCHIP) (Note 15)	KSP	274,778		
		KOHS			
		JUST			
16.560	National Institute of Justice Research, Evaluation, and Development Project Grants	KSP	380,848		
		JUST	81,085		
16.575	Crime Victim Assistance	JUST	5,030,906		4,806,189
		UPS	331,406		
16.576	Crime Victim Compensation	PPC	180,335		
16.579	Edward Byrne Memorial Formula Grant Program (Note 15)	JUST	427,883		349,638
		CORR	15,219		
		KSP			
		JUV			
		PUBAD			

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Justice (Continued)					
Direct Programs (Continued):					
16.580	Edward Byrne Memorial State and Local Law Enforcement Assistance Discretionary Grants Program (Note 15)	CHFS KSP JUST PUBAD	330,609		
16.585	Drug Court Discretionary Grant Program (Note 15)	AOC CHFS	193,884		
16.586	Violent Offender Incarceration and Truth in Sentencing Incentive Grants (Note 15)	JUST			
16.588	Violence Against Women Formula Grants	JUST UPS OAG CHFS	1,585,169 139,508 11,681 5,023		1,345,196
16.588	ARRA-Violence Against Women Formula Grants (Note 14)	JUST	180,152		180,152
16.589	Rural Domestic Violence, Dating Violence, Sexual Assault, and Stalking Assistance Program (Note 15)	JUST			
16.592	Local Law Enforcement Block Grants Program (Note 15)	KSP JUST			
16.593	Residential Substance Abuse Treatment for State Prisoners (Note 15)	CORR JUST	155,232		
16.606	State Criminal Alien Assistance Program	CORR	58,995		
16.607	Bulletproof Vest Partnership Program (Note 15)	KSP CORR JUST	23,447 12,736		
16.609	Community Prosecution and Project Safe Neighborhoods (Note 15)	UPS			
16.610	Regional Information Sharing Systems (Note 15)	COT			
16.710	Public Safety Partnership and Community Policing Grants	JUST KSP	165,402 134,740		
16.727	Enforcing Underage Drinking Laws Program	KSP	377,443		203,505
16.728	Drug Prevention Program (Note 15)	TC			
16.735	Protecting Inmates and Safeguarding Communities Discretionary Grant Program	CORR	4,257		
16.738	Edward Byrne Memorial Justice Assistance Grant Program	JUST KSP CORR AOC JUV UPS	2,458,033 465,721 200,988 78,367 27,815 23,541		2,120,060
16.738	ARRA-Edward Byrne Memorial Justice Assistance Grant Program (Note 14)	CORR DCJT	918,946 30,007		13,568
16.740	Statewide Automated Victim Information Notification (SAVIN) Program	CORR	288,627		
16.741	Forensic DNA Backlog Reduction Program	KSP	431,555		
16.748	Convicted Offended and/or Arrestee DNA Backlog Reduction Program (In-House Analysis and Data Review) (Note 15)	JUST			
16.743	Forensic Casework DNA Backlog Reduction Program	PUBAD JUST	475,248 89,245		
16.744	Anti-Gang Initiative	KSP	49,762		
16.745	Criminal and Juvenile Justice and Mental Health Collaboration Program (Note 7)	AOC	19,568		
16.746	Capital Case Litigation	JUST OAG PUBAD	49,950 10,197 5,883		
16.750	Support for Adam Walsh Act Implementation Grant Program	KSP	69,817		
16.800	ARRA-Recovery Act-Internet Crimes Against Children Task Force Program (ICAC) (Note 14)	KSP	19,908		
16.801	ARRA-Recovery Act-State Victim Assistance Formula Grant Program (Note 14)	JUST	93,489		93,489
16.802	ARRA-Recovery Act-State Victim Compensation Formula Grant Program (Note 14)	PPC	89,537		

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Justice (Continued)					
Direct Programs (Continued)					
16.803	ARRA-Recovery Act-Edward Byrne Memorial Justice Assistance Grant (JAG) Program/Grants to States and Territories (Note 14)	KSP	3,294,266		
		JUST	1,555,218		1,085,711
		UPS	137,315		
		F&W	136,492		
		AOC	34,088		
		PUBAD	9,305		
		JUV	122		
16.804	ARRA-Recovery Act-Edward Byrne Memorial Justice Assistance Grant(JAG) Program/Grants to Units of Local Government (Note 14)	OAG	12,493		
16.808	ARRA-Recovery Act-Edward Byrne Memorial Competitive Grant Program (Note 14)	KSP	161,904		
16.810	ARRA-Recovery Act-Assistance to Rural Law Enforcement to Combat Crime and Drugs Competitive Grant Program (Note 14)	OAG	214,961		
		UPS	62,408		
16.NA(1)	Drug Enforcement Administration	KSP	1,101,565		
16.NA(2)	Federal Bureau of Investigation	KSP	154,648		
16.NA(3)	Federal Methamphetamine Initiative (Note 15)	KSP			
16.NA(4)	Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF) Program	KSP	20,178		
16.NA(5)	Prescription Drug Monitoring Program (Note15)	CHFS			
16.NA(6)	District Fugitive Task Force	KSP	12,501		
Total U.S. Department of Justice			\$ 25,194,761	\$ 0	\$ 11,024,914
U.S. Department of Labor					
Direct Programs:					
17.002	Labor Force Statistics	DWI	\$ 1,034,065	\$	\$
17.005	Compensation and Working Conditions	LABOR	165,054		
Employment Services Cluster:					
17.207	Employment Service/Wagner-Peyser Funded Activities	DWI	6,079,231		
17.207	ARRA-Employment Service/Wagner-Peyser Funded Activities (Note 14)	DWI	2,802,147		
17.801	Disabled Veterans' Outreach Program (DVOP)	DWI	698,182		
17.804	Local Veterans' Employment Representative Program	DWI	1,811,005		
17.225	Unemployment Insurance (Note 2)(Note 4)	DWI	921,020,873		40,017
17.225	ARRA-Unemployment Insurance (Note 2) (Note 4) (Note 14)	DWI	1,075,269,000		
17.235	Senior Community Service Employment Program	CHFS	2,145,651		2,102,125
17.235	ARRA-Senior Community Service Employment Program (Note 14)	CHFS	435,387		421,989
17.245	Trade Adjustment Assistance	DWI	12,793,338		12,310,416
Workforce Investment Act Cluster:					
17.258	WIA Adult Program (Note 2)	DWI	14,008,723		12,950,156
17.258	ARRA-WIA Adult Program (Note 2) (Note 14)	DWI	5,882,719		5,867,354
17.259	WIA Youth Activities (Note 2)	DWI	16,038,744		14,731,707
		EDU	62		
17.259	ARRA-WIA Youth Activities (Note 2) (Note 14)	DWI	12,001,715		11,666,028
17.260	WIA Dislocated Workers (Note 2)	DWI	28,089,476		26,472,392
		EDU	787,358		722,421
		LABOR	2,012		
17.260	ARRA-WIA Dislocated Workers (Note 2) (Note 14)	DWI	10,168,716		10,168,716
17.261	WIA Pilots, Demonstrations, and Research Projects (Note 15)	DWI			
17.267	Incentive Grants-WIA Section 503 (Note 15)	DWI			
17.268	H-1B Job Training Grants	DWI	2,958,658		2,922,732
17.271	Worker Opportunity Tax Credit Program (WOTC)	DWI	387,451		
17.272	Permanent Labor Certification for Foreign Workers (Note 15)	DWI			
17.273	Temporary Labor Certification For Foreign Workers	DWI	298,335		
17.275	ARRA-Program of Competitive Grants for Worker Training and Placement in High Growth and Emerging Industry Sectors	DWI	26,230		
17.276	ARRA-Health Coverage Tax Credit (HCTC) (Note 14)	DWI	1,536,653		
17.503	Occupational Safety and Health-State Program (Note 4)	LABOR	3,743,207		113,400
17.504	Consultation Agreements (Note 4) (Note 15)	LABOR			
17.505	OSHA Data Initiative (Note 15)	LABOR			

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Labor (Continued)					
Direct Programs (Continued)					
17.600	Mine Health and Safety Grants	EEC	649,127		
17.603	Brookwood-Sago Grant (Note 15)	EEC			
Total U.S. Department of Labor			<u>\$ 2,120,833,119</u>	<u>\$ 0</u>	<u>\$ 100,489,454</u>
U.S. Department of Transportation					
Direct Programs:					
20.106	Airport Improvement Program	TC PARKS	\$ 1,261 6,340	\$	\$
Highway Planning and Construction Cluster:					
20.205	Highway Planning and Construction (Note 2) (Note 5) (Note 15)	TC PARKS	522,339,327		59,878,739
20.205	ARRA-Highway Planning and Construction (Note 2) (Note 14) (Note 15)	KSP TC	185,458,469		
20.219	Recreational Trails Program (Note 2) (Note 6) (Note 15)	KHP DLG PARKS	743,311		640,736
20.218	National Motor Carrier Safety	KSP	4,589,852		245,257
20.232	Commercial Driver License Programs Improvement Grant (Note 15)	TC	675,041		
20.238	Commercial Drivers License Information System (CDLIS) Modernization Grant	TC	178,636		
20.505	Metropolitan Transportation Planning	TC	660,829		660,829
Federal Transit Cluster:					
20.500	Federal Transit-Capital Investment Grants	TC	4,286,579		4,286,579
20.507	Federal Transit-Formula Grants	TC	2,082,662		2,082,662
20.507	ARRA-Federal Transit-Formula Grants (Note 14)	TC	2,106,849		2,106,849
20.509	Formula Grants for Other Than Urbanized Areas	TC	12,341,098		11,831,187
20.509	ARRA-Formula Grants for Other Than Urbanized Areas (Note 14)	TC	18,574,062		18,574,062
Transit Services Programs Cluster:					
20.513	Capital Assistance Program for Elderly Persons and Persons with Disabilities	TC	2,064,550		2,014,550
20.516	Job Access-Reverse Commute	TC	1,493,367		1,493,367
20.521	New Freedom Program	TC	987,143		987,143
20.514	Public Transportation Research	TC	1,154,509		1,154,509
Highway Safety Cluster:					
20.600	State and Community Highway Safety (Note 15)	TC KSP OAG AOC DCJT	2,580,609 634,212 164,771 57,340		2,076,870
20.601	Alcohol Impaired Driving Countermeasures Incentive Grants I	KSP TC	252,996 63,774		
20.602	Occupant Protection Incentive Grants	TC KSP	710,081 144,615		136,987
20.604	Safety Incentive Grants for Use of Seatbelts (Note 15)	KSP			
20.605	Safety Incentives to Prevent Operation of Motor Vehicles by Intoxicated Persons (Note 15)	TC			
20.609	Safety Belt Performance Grants	TC	271,922		47,780
20.610	State Traffic Safety Information System Improvement Grants	KSP TC	273,500 193,505		
20.612	Incentive Grant Program to Increase Motorcyclist Safety	TC	119,774		
20.700	Pipeline Safety Program Base Grants	EEC	255,276		
20.703	Interagency Hazardous Materials Public Sector Training and Planning Grants	MIL	284,818		
Total U.S. Department of Transportation			<u>\$ 765,751,078</u>	<u>\$ 0</u>	<u>\$ 108,218,106</u>

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. Department of Treasury</u>					
Direct Programs:					
21.NA(1)	Internal Revenue Service	KSP	\$ 6,443	\$	\$
Total U.S. Department of Treasury			\$ 6,443	\$ 0	\$ 0
<u>U.S. Appalachian Regional Commission</u>					
Direct Programs:					
23.002	Appalachian Area Development (Note 15)	DLG TAH	\$	\$	\$
23.011	Appalachian Research, Technical Assistance, and Demonstration Projects	DLG AOC	1,109,052 13,281		984,646
Total U.S. Appalachian Regional Commission			\$ 1,122,333	\$ 0	\$ 984,646
<u>U.S. Equal Employment Opportunity Commission</u>					
Direct Programs:					
30.002	Employment Discrimination-State and Local Fair Employment Practices Agency Contracts	HRC	\$ 156,520	\$	\$
Total U.S. Equal Employment Opportunity Commission			\$ 156,520	\$ 0	\$ 0
<u>U.S. General Services Administration</u>					
Direct Programs:					
39.003	Donation of Federal Surplus Personal Property (Note 11)	FAC	\$	\$ 478,254	\$
39.011	Election Reform Payments (Note 13)	KBE	454,560		
Total U.S. General Services Administration			\$ 454,560	\$ 478,254	\$ 0
<u>National Aeronautics and Space Administration</u>					
Direct Programs:					
43.002	Aeronautics (Note 15)	COT	\$	\$	\$
Total National Aeronautics and Space Administration			\$ 0	\$ 0	\$ 0
<u>U.S. National Foundation on the Arts and the Humanities</u>					
Direct Programs:					
45.024	Promotion of the Arts-Grants to Organizations and Individuals	KHS	\$ 35,000	\$	\$
45.025	Promotion of the Arts-Partnership Agreements	KAC	930,689		832,562
		KHS	25,000		
45.025	ARRA-Promotion of the Arts-Partnership Agreements (Note 14)	KAC	306,933		306,776
45.161	Promotion of the Humanities-Research (Note 15)	HRC			
45.310	Grants to States	DLA	1,870,192		458,858
Total U.S. National Foundation on the Arts and Humanities			\$ 3,167,814	\$ 0	\$ 1,598,196
<u>U.S. Department of Veterans Affairs</u>					
Direct Programs:					
64.005	Grants to States for Construction of State Home Facilities (Note 15)	VA	\$	\$	\$
64.203	State Cemetery Grants (Note 15)	VA			
Total U.S. Department of Veterans Affairs			\$ 0	\$ 0	\$ 0
<u>U.S. Environmental Protection Agency</u>					
Direct Programs:					
66.001	Air Pollution Control Program Support (Note 4)	EEC	\$ 1,116,443	\$	\$
66.032	State Indoor Radon Grants	CHFS	363,551		313,665
66.034	Surveys, Studies, Investigations, Demonstrations and Special Purpose Activities Relating to the Clean Air Act (Note 4) (Note 11)	EEC	653,736	142,053	

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Environmental Protection Agency (Continued)					
Direct Programs (Continued):					
66.040	State Clean Diesel Grant Program (Note 4) (Note 19)	EEC	155,505		155,505
66.040	ARRA-State Clean Diesel Grant Program (Note 14)	EEC	850,484		760,952
66.418	Construction Grants for Wastewater Treatment Works	EEC	43,208		
66.419	Water Pollution Control State, Interstate, and Tribal Program Support	EEC	2,469,457		89,689
66.432	State Public Water System Supervision	EEC	254,379		
66.436	Surveys, Studies, Investigations, Demonstrations, and Training Grants and Cooperative Agreements-Section 104(B)(3) of the Clean Water Act (Note 4) (Note 15)	EEC			
66.454	Water Quality Management Planning	EEC	74,744		67,687
66.454	ARRA-Water Quality Management Planning (Note 14)	EEC	330,952		28,804
66.458	Capitalization Grants for Clean Water State Revolving Funds	EEC	207,387		
		PARKS	550,391		
66.458	ARRA-Capitalization Grants for Clean Water State Revolving Funds (Note 14) (Note 15)	EEC	231,416		
		KHP			
66.460	Nonpoint Source Implementation Grants	EEC	4,116,510		3,059,000
66.461	Regional Wetland Program Development Grants	EEC	223,341		
66.463	Water Quality Cooperative Agreements (Note 15)	EEC			
66.467	Wastewater Operator Training Grant Program (Technical Assistance) (Note 15)	EEC			
66.468	Capitalization Grants for Drinking Water State Revolving Funds	EEC	2,361,877		
66.468	ARRA-Capitalization Grants for Drinking Water State Revolving Funds (Note 14)	EEC	318,550		
66.471	State Grants to Reimburse Operators of Small Water Systems for Training and Certification Costs	EEC	70,582		
66.474	Water Protection Grants to the States	EEC	45,376		23,402
66.608	Environmental Information Exchange Network Grant Program and Related Assistance (Note 15)	EEC	31,194		
		COT			
66.605	Performance Partnership Grants	AGR	598,759		
66.701	Toxic Substances Compliance Monitoring Cooperative Agreements	EEC	99,533		
66.707	TSCA Title IV State Lead Grants Certification of Lead-Based Paint Professionals	CHFS	216,677		29,308
66.708	Pollution Prevention Grants Program	EEC	80,890		37,750
66.709	Multi-Media Capacity Building Grants for States and Tribes	EEC	18,171		
66.717	Source Reduction Assistance (Note 15)	EEC			
66.801	Hazardous Waste Management State Program Support	EEC	1,720,075		
66.802	Superfund State, Political Subdivision, and Indian Tribe Site-Specific Cooperative Agreements	EEC	188,503		
66.804	Underground Storage Tank Prevention, Detection and Compliance Program	EEC	279,039		
66.805	Leaking Underground Storage Tank Trust Fund Corrective Action Program	EEC	1,644,183		
66.805	ARRA-Leaking Underground Storage Tank Trust Fund Corrective Action Program (Note 14)	EEC	307,468		
66.809	Superfund State and Indian Tribe Core Program-Cooperative Agreements	EEC	77,130		
66.817	State and Tribal Response Program Grants	EEC	440,704		
66.940	Environmental Policy and State Sustainability Grants	EEC	43,058		
66.951	Environmental Educational Grants	EEC	4,891		
Total U.S. Environmental Protection Agency			\$ 20,188,164	\$ 142,053	\$ 4,565,762
U.S. Department of Energy					
Direct Programs:					
81.039	National Energy Information Center	EEC	\$ 6,937	\$	\$
81.041	State Energy Program	EEC	626,750		193,178
81.041	ARRA-State Energy Program (Note 14)	EEC	3,033,274		962,449
		FAC	75,564		
		EDU	27,800		
		ADB	16,856		
		CED	11,297		
81.042	Weatherization Assistance for Low-Income Persons (Note 15)	FAC	5,935,356		5,935,356
		CHFS			
81.042	ARRA-Weatherization Assistance for Low-Income Persons (Note 14)	FAC	13,792,599		13,792,599
81.086	ARRA-Conservation Research and Development (Note 14)	EDU	34,942		

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Energy (Continued)					
Direct Programs (Continued):					
81.104	Office of Environmental Waste Processing (Note 4)	EEC	1,125,382		288,830
		CHFS	851,927		380,535
81.119	ARRA-State Energy Program Special Projects (Note 14)	EEC	44,835		44,330
81.122	ARRA-Electricity Delivery and Energy Reliability, Research, Development and Analysis (Note 14)	EEC	164,273		
81.127	ARRA-Energy Efficient Appliance Rebate Program (EEARP) (Note 14)	EEC	1,780,778		1,749,121
81.128	ARRA-Energy Efficiency and Conservation Block Grant Program (EECBG) (Note 14)	DLG	38,070		
		EEC	85,201		
		PPC	89,967		
81.502	Paducah Gaseous Diffusion Plant Environmental Monitoring and Oversight (Note 15)	CHFS			
81.NA(1)	Department of Energy (Note 15)	F&W			
Total U.S. Department of Energy			<u>\$ 27,741,808</u>	<u>\$ 0</u>	<u>\$ 23,346,398</u>
U.S. Department of Education					
Direct Programs:					
Title I, Part A Cluster:					
84.010	Title I Grants to Local Educational Agencies (Note 2)	EDU	\$ 226,055,723	\$	\$ 225,133,857
84.389	ARRA-Title I Grants to Local Educational Agencies, Recovery Act (Note 14) (Note 2)	EDU	82,194,502		
84.011	Migrant Education-State Grant Program	EDU	8,197,113		8,073,145
84.013	Title I Program for Neglected and Delinquent Children	JUV	918,693		787,101
		CORR	22,775		
		EDU	6,495		
Special Education Cluster:					
84.027	Special Education - Grants to States (Note 2)	EDU	151,805,010		149,690,535
84.173	Special Education - Preschool Grants (Note 2)	EDU	9,752,321		9,520,769
84.391	ARRA-Special Education Grants to States, Recovery Act (Note 2) (Note 14)	EDU	81,325,320		
84.392	ARRA-Special Education-Preschool Grants, Recovery Act (Note 2) (Note 14)	EDU	4,370,843		
84.048	Career and Technical Education-Basic Grants to States	DWI	9,371,175		7,041,497
		EDU	7,063,390		6,813,992
		EPSB	172,802		
Vocational Rehabilitation Services Cluster:					
84.126	Rehabilitation Services-Vocational Rehabilitation Grants to States (Note 2)	DWI	48,441,534		2,021,195
84.390	ARRA-Rehabilitation Services-Vocational Rehabilitation Grants to States, Recovery Act (Note 2) (Note 14)	DWI	2,738,478		
84.128	Rehabilitation Services-Service Projects	DWI	225,112		221,625
84.144	Migrant Education-Coordination Program	EDU	8,882		
84.161	Rehabilitation Services-Client Assistance Program	DWI	144,680		
84.169	Independent Living-State Grants	DWI	277,097		208,021
84.177	Rehabilitation Services-Independent Living Services for Older Individuals Who are Blind	DWI	522,980		
84.181	Special Education-Grants for Infants and Families	CHFS	4,729,448		
84.181	ARRA-Special Education-Grants for Infants and Families (Note 14)	CHFS			
84.393	ARRA-Special Education-Grants for Infants and Families, Recovery Act (Note 14)	CHFS	1,267,330		484,401
84.186	Safe and Drug-Free Schools and Communities-State Grants	EDU	3,171,599		2,960,440
		JUST	561,095		
		CHFS	40,895		40,895
84.187	Supported Employment Services for Individuals with the Most Significant Disabilities	DWI	337,107		
Education of Homeless Children and Youth Cluster:					
84.196	Education for Homeless Children and Youth	EDU	1,029,489		586,289
84.387	ARRA-Education for Homeless Children and Youth, Recovery Act (Note 14)	EDU	519,922		
84.213	Even Start-State Educational Agencies	EDU	1,010,363		937,096
84.215	Fund for the Improvement of Education (Note 10) (Note 15)	KHS	191,305		
		EDU			
84.224	Assistive Technology	DWI	464,920		224,051
84.240	Program of Protection and Advocacy of Individual Rights	PUBAD	312,680		

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Education (Continued)					
Direct Programs (Continued):					
84.243	Tech-Prep Education	DWI	1,576,425		762,699
		EDU	209,661		134,743
84.265	Rehabilitation Training-State Vocational Rehabilitation Unit In-Service Training	DWI	296,345		
84.287	Twenty-First Century Community Learning Centers	EDU	11,561,331		11,452,485
84.298	State Grants for Innovative Programs	EDU	106,647		106,643
Educational Technology State Grants Cluster:					
84.318	Education Technology State Grants	EDU	3,954,737		3,703,034
84.386	ARRA-Education Technology State Grants, Recovery Act	EDU	1,222,939		
84.323	Special Education-State Personnel Development	EDU	1,198,272		1,194,220
84.326	Special Education-Technical Assistance and Dissemination to Improve Services and Results for Children with Disabilities	EDU	197,990		197,990
84.330	Advanced Placement Program (Advanced Placement Test Fee; Advanced Placement Incentive Program Grants)	EDU	741,123		547,946
84.331	Grants to States for Workplace and Community Transition Training for Incarcerated Individuals	CORR	293,235		
84.336	Teacher Quality Partnership Grants (Note 15)	EPSB			
84.343	Assistive Technology - State Grants for Protection and Advocacy	PUBAD	56,517		
84.350	Transition to Teaching	EDU	202,517		155,456
84.357	Reading First State Grants	EDU	10,033,462		9,397,491
84.358	Rural Education	EDU	5,587,520		5,587,520
84.365	English Language Acquisition Grants	EDU	3,116,519		3,008,459
84.366	Mathematics and Science Partnerships	EDU	3,670,582		3,608,361
84.367	Improving Teacher Quality State Grants (Note 2)	EDU	45,465,656		44,699,023
84.369	Grants for State Assessments and Related Activities	EDU	4,620,651		25,555
84.371	Striving Readers	EDU	124,251		75,515
84.372	Statewide Data Systems	EDU	416,274		
		EPSB	87,205		
School Improvements Grants Cluster:					
84.377	School Improvement Grants	EDU	5,630,040		5,414,888
84.388	ARRA-School Improvement Grants, Recovery Act (Note 14) (Note 15)	EDU			
State Fiscal Stabilization Fund Cluster:					
84.394	ARRA-State Fiscal Stabilization Fund (SFSF)-Education State Grants, Recovery Act (Note 14) (Note 2)	FAC	70,000,000		70,000,000
		EDU	223,038,700		
84.397	ARRA-State Fiscal Stabilization Fund (SFSF)-Government Services, Recovery Act (Note 14) (Note 15) (Note 2)	CORR	75,367,600		
		KSP	14,831,700		
		FAC			
84.398	ARRA-Independent Living State Grants, Recovery Act (Note 14)	DWI	36,895		
84.399	ARRA-Independent Living Services for Older Individuals Who Are Blind, Recovery Act (Note 14)	DWI	59,384		
Passed Through From the Powell County Board of Education:					
84.215	Fund for the Improvement of Education Pass Through Grantor-Variou (Note 15)	KHS			
Passed Through From the Letcher County Board of Education:					
84.215	Fund for the Improvement of Education Pass Through Grantor-Variou (Note 15)	KHS			
Passed Through From the Civic Education Center:					
84.304	Civic Education- We the People and the Cooperative Education Exchange Program Pass Through Grantor-Variou (Note 10)	AOC	108,516		
Passed Through From the Center for Civic Education:					
84.929	We the People Pass Through Grantor-Variou (Note 10)	AOC			
Total U.S. Department of Education			<u>\$ 1,131,063,771</u>	<u>\$ 0</u>	<u>\$ 574,816,936</u>

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. National Archives and Records Administration					
Direct Programs:					
89.003	National Historical Publications and Records Grants	DLA	\$ 21,288	\$	\$
Total U.S. National Archives and Records Administration			\$ 21,288	\$ 0	\$ 0
U.S. Election Assistance Commission					
Direct Programs:					
90.401	Help America Vote Act Requirements Payments	KBE	\$ 1,871,414	\$	\$ 1,871,414
90.402	Help America Vote Mock Election Program (Note 15)	SOS			
Total U.S. Election Assistance Commission			\$ 1,871,414	\$ 0	\$ 1,871,414
U.S. Department of Health and Human Services					
Direct Programs:					
93.003	Public Health and Social Services Emergency Fund (Note 15)	CHFS	\$	\$	\$
93.041	Special Programs for the Aging-Title VII, Chapter 3-Programs for Prevention of Elder Abuse, Neglect, and Exploitation	CHFS	69,154		69,154
93.042	Special Programs for the Aging-Title VII, Chapter 2-Long Term Care Ombudsman Services for Older Individuals	CHFS	160,910		148,064
93.043	Special Programs for the Aging-Title III, Part D-Disease Prevention and Health Promotion Services	CHFS	283,550		283,550
Aging Cluster:					
93.044	Special Programs for the Aging-Title III, Part B-Grants for Supportive Services and Senior Centers	CHFS	5,740,255		5,058,859
93.045	Special Programs for the Aging-Title III, Part C-Nutrition Services	CHFS	8,241,707		7,721,787
93.053	Nutrition Services Incentive Program	CHFS	1,816,133		1,816,133
93.705	ARRA-Aging Home-Delivered Nutrition Services for States (Note 14)	CHFS	416,888		381,798
93.707	ARRA-Aging Congregate Nutrition Services for States (Note 14)	CHFS	831,775		772,725
93.048	Special Programs for the Aging-Title IV-and Title II-Discretionary Projects	CHFS	245,934		228,368
93.051	Alzheimer's Disease Demonstration Grants to States	CHFS	111,881		72,954
93.052	National Family Caregiver Support, Title III,Part E	CHFS	2,102,255		2,079,049
93.069	Public Health Emergency Preparedness (Note 2) (Note 11)	CHFS	24,357,870	10,444,736	18,034,289
93.070	Environmental Public Health and Emergency Response	CHFS	132,215		60,058
93.071	Medicare Enrollment Assistance Program	CHFS	152,682		152,682
93.087	Enhance the Safety of Children Affected by Parental Methamphetamine or Other Substance Abuse	CHFS	610,340		274,255
93.089	Emergency System for Advance Registration of Volunteer Health Professionals	CHFS	15,854		
93.103	Food and Drug Administration-Research	CHFS	8,484		
93.104	Comprehensive Community Mental Health Services for Children with Serious Emotional Disturbances (SED)	CHFS	2,688,536		2,397,485
93.110	Maternal and Child Health Federal Consolidated Programs	CHFS	275,631		69,687
93.116	Project Grants and Cooperative Agreements for Tuberculosis Control Programs (Note 11)	CHFS	826,666	79,796	529,982
93.130	Cooperative Agreements to States/Territories for the Coordination and Development of Primary Care Offices	CHFS	101,216		32,246
93.134	Grants to Increase Organ Donations (Note 15)	CHFS			
93.136	Injury Prevention and Control Research and State and Community Based Programs	CHFS	651,216		651,216
93.138	Protection and Advocacy for Individuals with Mental Illness	PUBAD	418,453		
93.150	Projects for Assistance In Transition from Homelessness (PATH)	CHFS	432,001		432,001
93.197	Childhood Lead Poisoning Prevention Projects - State and Local Childhood Lead Poisoning Prevention and Surveillance of Blood Lead Levels in Children	CHFS	482,429		323,040
93.217	Family Planning - Services	CHFS	5,729,621		5,097,676
93.230	Consolidated Knowledge Development and Application (KD&A) Program (Note 15)	CHFS			
93.234	Traumatic Brain Injury State Demonstration Grant Program	CHFS	43,102		
93.235	Abstinence Education Program	CHFS	395,755		382,046
93.236	Grants for Dental Health Residency Training	CHFS	1,041		
93.242	Mental Health Research Grants (Note 15)	CHFS			

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Health and Human Services (Continued)					
Direct Programs (Continued):					
93.243	Substance Abuse and Mental Health Services-Projects of Regional and National Significance (Note 15) (Note 7)	CHFS AOC JUV JUST	2,868,170 1,257,721		2,608,643
93.251	Universal Newborn Hearing Screening	CHFS	451,421		
93.262	Occupational Safety and Health Program (Note 15)	CHFS			
93.267	State Grants for Protection and Advocacy Services	PUBAD	45,102		
Immunization Cluster:					
93.268	Immunization Grants (Note 11) (Note 2)	CHFS	3,064,297	34,912,487	1,482,412
93.712	ARRA-Immunization (Note 14) (Note 2)	CHFS	99,254	1,550,567	
93.276	Drug-Free Communities Support Program Grants (Note 15)	KVE			
93.414	ARRA-State Primary Care Offices (Note 14)	CHFS	30,121		30,121
93.283	Centers for Disease Control and Prevention-Investigations and Technical Assistance	CHFS	5,005,001		4,126,422
93.556	Promoting Safe and Stable Families	CHFS	6,734,795		6,493,077
Temporary Assistance for Needy Families Cluster:					
93.558	Temporary Assistance for Needy Families (Note 2)	CHFS	147,928,175		23,764,491
93.714	ARRA-Emergency Contingency Fund for Temporary Assistance for Needy Families (TANF) State Program (Note 14) (Note 15)	DWI CHFS	3,825,203		3,825,203
93.563	Child Support Enforcement (Note 15) (Note 2)	CHFS OAG	14,245,360		147,824
93.563	ARRA-Child Support Enforcement (Note 2) (Note 14)	CHFS	30,290,029		25,202,702
93.568	Low-Income Home Energy Assistance (Note 2)	CHFS	66,792,655		66,660,766
Community Services Block Grant Cluster:					
93.569	Community Services Block Grant	CHFS	10,922,004		10,682,066
93.710	ARRA-Community Services Block Grant (Note 14)	CHFS	10,501,439		10,501,439
93.571	Community Services Block Grant Formula and Discretionary Awards Community Food and Nutrition Programs (Note 15)	CHFS			
93.585	Empowerment Zones Program	OC	1,350,000		1,350,000
Child Care and Development Block Grant Cluster:					
93.575	Child Care and Development Block Grant (Note 2)	CHFS	85,131,885		3,425,606
93.596	Child Care Mandatory and Matching Funds of the Child Care and Development Fund (Note 2)	CHFS	24,564,662		9,142,104
93.713	ARRA-Child Care and Development Block Grant (Note 2) (Note 14)	CHFS	32,260,858		1,805,281
93.586	State Court Improvement Program (Note 7)	AOC	427,586		
93.590	Community-Based Child Abuse Prevention Grants	CHFS	2,851,166		2,739,596
93.597	Grants to States for Access and Visitation Programs	CHFS	122,440		122,440
93.599	Chafee Education and Training Vouchers Program (ETV)	CHFS	571,388		
Head Start Cluster:					
93.600	Head Start	EDU	133,637		
93.603	Adoption Incentive Payments	CHFS	764,000		764,000
93.617	Voting Access for Individuals with Disabilities-Grants To States	KBE	164,702		88,912
93.618	Voting Access for Individuals with Disabilities-Grants for Protection and Advocacy Systems	PUBAD	41,403		
93.630	Developmental Disabilities Basic Support and Advocacy Grants	CHFS PUBAD	2,060,800 547,055		791,912
93.643	Children's Justice Grants to States	CHFS AOC OAG	150,179 82,175 55,000		
93.645	Child Welfare Services-State Grants	CHFS	4,212,770		
93.647	Social Services Research and Demonstration (Note 15)	CHFS			
93.652	Adoption Opportunities	CHFS	418,441		415,965
93.658	Foster Care-Title IV-E (Note 2)	CHFS JUV AOC	41,896,044 2,796,202 293,616		2,698,355
93.658	ARRA-Foster Care-Title IV-E (Note 2) (Note 14)	CHFS	2,432,663		
93.659	Adoption Assistance (Note 2)	CHFS	38,532,212		
93.659	ARRA-Adoption Assistance (Note 2) (Note 14)	CHFS	3,320,988		

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Health and Human Services (Continued)					
Direct Programs (Continued):					
93.667	Social Services Block Grant (Note 15)	CHFS	23,534,845		56,388
		JUV	5,624,386		
		FAC			
93.667	ARRA-Social Services Block Grant (Note 14)	CHFS	20,092		
93.669	Child Abuse and Neglect State Grants	CHFS	342,869		267,433
93.671	Family Violence Prevention and Services/Grants for Battered Women's Shelters-Grants to State and Indian Tribes	CHFS	1,137,773		1,129,375
93.674	Chafee Foster Care Independence Program	CHFS	1,930,830		1,172,458
93.717	ARRA-Preventing Healthcare-Associated Infections (Note 14)	CHFS	43,897		40,626
93.719	ARRA- State Grants to Promote Health Information Technology (Note 14)	CHFS	35,356		
93.720	ARRA-Survey and Certification Ambulatory Surgical Center Healthcare-Associated Infection (ASC-HAI) Prevention Initiative (Note 14)	CHFS	14,495		
93.725	ARRA-Communities Putting Prevention to Work: Chronic Disease Self-Management Program (Note 14)	CHFS	2,019		
93.723	ARRA-Prevention and Wellness-State, Territories and Pacific Islands (Note 14)	CHFS	5,062		
93.767	Children's Health Insurance Program (Note 2)	CHFS	123,192,943		158,684
Medicaid Cluster:					
93.775	State Medicaid Fraud Control Units (Note 2)	OAG	2,090,299		
93.777	State Survey and Certification of Health Care Providers and Suppliers (Note 2)	CHFS	5,784,172		
93.778	Medical Assistance Program (Note 2)	CHFS	4,087,341,324		2,659,913
93.778	ARRA-Medical Assistance Program (Note 2)(Note 14)	CHFS	505,415,419		
93.779	Centers for Medicare and Medicaid Services (CMS) Research, Demonstrations and Evaluations	CHFS	1,987,592		1,032,135
93.780	Grants to States for Qualified High-Risk Pools (Note 15)	PPC			
93.793	Medicaid Transformation Grants	CHFS	329,458		
93.889	National Bioterrorism Hospital Preparedness Program	CHFS	6,518,012		5,720,213
		MIL	137,777		
93.917	HIV Care Formula Grants	CHFS	7,357,481		3,180,193
93.938	Cooperative Agreements to Support Comprehensive School Health Programs to Prevent the Spread of HIV and Other Important Health Problems	EDU	636,840		176,653
		CHFS	129,295		29,358
93.940	HIV Prevention Activities - Health Department Based	CHFS	1,825,271		1,367,123
93.941	HIV Demonstration, Research, Public and Professional Education Projects	CHFS	221,211		68,221
93.944	Human Immunodeficiency Virus (HIV)/Acquired Immunodeficiency Virus Syndrome (AIDS) Surveillance (Note 15)	CHFS			
93.945	Assistance Programs for Chronic Disease Prevention and Control	CHFS	415,712		331,431
93.958	Block Grants for Community Mental Health Services	CHFS	5,359,628		4,951,716
		DWI	75,000		
		CORR	45,500		
93.959	Block Grants for Prevention and Treatment of Substance Abuse (Note 15)	CHFS	20,027,580		19,631,262
		KSP	43,786		
		JUST			
93.977	Preventive Health Services - Sexually Transmitted Diseases Control Grants (Note 11)	CHFS	649,035	234,247	43,384
93.988	Cooperative Agreements for State-Based Diabetes Control Programs and Evaluation of Surveillance Systems	CHFS	83		
93.991	Preventive Health and Health Services Block Grant	CHFS	1,122,889		849,976
93.994	Maternal and Child Health Services Block Grant to the States	CHFS	9,814,383		7,309,777
93.NA(1)	Other Federal Assistance	CHFS	244,284		
Total U.S. Department of Health and Human Services			\$ 5,420,042,771	\$ 47,221,833	\$ 276,114,761
U.S. Corporation for National and Community Service					
Direct Programs:					
94.003	State Commissions	CHFS	\$ 195,259	\$	\$
94.004	Learn and Serve America-School and Community Based Programs	EDU	245,103		230,020

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. Corporation for National and Community Service (Continued)</u>					
Direct Programs (Continued):					
94.006	AmeriCorps	CHFS	3,184,001		2,991,293
		CORR	47,019		
94.006	ARRA-AmeriCorps (Note 14)	CHFS	622,810		609,414
94.007	Program Development and Innovation Grants	CHFS	67,505		
94.009	Training and Technical Assistance	CHFS	90,870		
Foster Grandparents/Senior Companion Cluster:					
94.011	Foster Grandparent Program	CHFS	557,077		9,000
94.NA(1)	Clinical Laboratory Improvement Act (Note 15)	CHFS			
Total U.S. Corporation for National and Community Service			<u>\$ 5,009,644</u>	<u>\$ 0</u>	<u>\$ 3,839,727</u>
<u>U.S. Office of National Drug Control Policy</u>					
Direct Program:					
95.001	High Intensity Drug Trafficking Areas Program	KSP	\$ 997,033	\$	\$
Total U.S. Office of National Drug Control Policy			<u>\$ 997,033</u>	<u>\$ 0</u>	<u>\$ 0</u>
<u>U.S. Social Security Administration</u>					
Direct Programs:					
Disability Insurance/Supplemental Security Income Cluster:					
96.001	Social Security-Disability Insurance (Note 2)	CHFS	\$ 45,931,639	\$	\$
96.009	Social Security State Grants for Work Incentives Assistance to Disabled Beneficiaries	PUBAD	34,044		
Total U.S. Social Security Administration			<u>\$ 45,965,683</u>	<u>\$ 0</u>	<u>\$ 0</u>
<u>U. S. Department of Homeland Security</u>					
Direct Programs:					
Homeland Security Cluster:					
97.004	Homeland Security Grant Program (Note 15)	KOHS	\$	\$	\$
		DCJT			
		MIL			
		KSP			
		EPPC			
97.067	Homeland Security Grant Program (Note 15)	KOHS	12,269,603		11,068,374
		DCJT			
		TC	14,577		
		F&W	8,663		
		KSP	6,668		
		MIL			
		KVE			
		COT			
		AGR			
		JUST			
		EPPC			
97.001	Pilot Demonstration or Earmarked Projects	KOHS	204,072		202,462
97.012	Boating Safety Financial Assistance	F&W	1,334,018		
97.017	Pre-Disaster Mitigation (PDM) Competitive Grants	MIL	750,288		750,288
97.023	Community Assistance Program State Support Services Element (CAP-SSSE) (Note 4)	EEC	133,777		
97.029	Flood Mitigation Assistance (Note 15)	MIL	946,860		946,860
		TC			
97.032	Crisis Counseling	MIL	36,630		
97.036	Disaster Grants-Public Assistance (Presidentially Declared Disasters) (Note 2)	MIL	186,532,761		178,409,197
		TC	15,881,929		
		PARKS	265,662		
		KSP	234,924		

See accompanying Notes to the Schedule of Expenditures of Federal Awards

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U. S. Department of Homeland Security (Continued)</u>					
Direct Programs (Continued):					
97.039	Hazardous Mitigation Grant	MIL	681,925		461,440
97.040	Chemical Stockpile Emergency Preparedness Program (Note 15)	MIL	14,480,920		12,956,528
		CHFS			
97.041	National Dam Safety Program	EEC	46,100		
97.042	Emergency Management Performance Grants (Note 15)	MIL	4,611,537		2,990,573
		KOHS			
97.045	Cooperating Technical Partners	EEC	3,734,265		
97.047	Pre Disaster Mitigation	MIL	1,056,120		893,374
97.056	Port Security Grant Program	F&W	1,223		
97.070	Map Modernization Management Support	EEC	113,816		
97.076	National Center for Missing and Exploited Children (NCMEC) (Note 19)	KSP			
97.077	Homeland Security Research Testing, Evaluation, and Demonstration of Technologies Related to Nuclear Detection	TC	79,587		
97.078	Buffer Zone Protection Program (BZPP)	KOHS	269,804		240,692
		F&W	312,661		
		KSP	91,825		
97.082	Earthquake Consortium	MIL	24,324		
97.089	Driver's License Security Grant Program	TC	1,493,242		
97.116	ARRA-Port Security Grant Program (ARRA) (Note 14) (Note15)	KSP			
Total U.S. Department of Homeland Security			\$ 245,617,781	\$ 0	\$ 208,919,788
<u>Other Federal Assistance</u>					
Direct Programs:					
NA(1)	Tennessee Vally Authority (Note 15)	F&W	\$	\$	\$
Total Other Federal Assistance			\$ 0	\$ 0	\$ 0
Total All State Agencies			\$ 10,401,012,066	\$ 1,245,313,065	\$ 1,664,661,491

See accompanying Notes to the Schedule of Expenditures of Federal Awards

COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010

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 other discretely presented component units, 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 and other discretely presented component units 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.

Noncash assistance programs are not reported in the basic financial statements of the Commonwealth for FY 2010. The noncash expenditures presented on this schedule represent the noncash assistance expended using the method or basis of valuation described in Note 11.

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.

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

Note 1 - Purpose of the Schedule and Significant Accounting Policies (Continued)

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:

- (a) Federal funds 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 and discretely presented component units 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 and discretely presented component units report those amounts as expenditures.

- (b) Federal funds 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 \$34.9 million for FY 2010. The Commonwealth had the following programs (cash and noncash) that met the Type A program definition for FY 10, 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. Programs with both ARRA and non-ARRA funding sharing the same CFDA number and not included as part of a cluster are presented as a combined amount, in this note and denoted with an asterisk (*). These Type A programs and clusters were:

CFDA	Program Title	Expenditures
Supplemental Nutrition Assistance Program Cluster:		
10.551	Supplemental Nutrition Assistance Program	\$ 1,164,591,491
10.561	State Administrative Matching Grants for the Supplemental Nutrition Assistance Program	43,123,864
10.561	ARRA-State Administrative Matching Grants for the Supplemental Nutrition Assistance Program	5,313,750
Child Nutrition Cluster:		
10.553	School Breakfast Program	59,680,885
10.555	National School Lunch Program	186,968,235
10.556	Special Milk Program for Children	82,376
10.559	Summer Food Service Program for Children	7,269,789
10.557	Special Supplemental Nutrition Program for Women, Infants, and Children	125,228,544

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

Note 2 - Type A Programs (Continued)

CFDA	Program Title	Expenditures
Community Development Block Grant-State-Administered Small Cities Program		
Cluster:		
14.228	Community Development Block Grants/States Programs and Non-Entitlement Grants in Hawaii	40,116,857
14.255	ARRA-Community Development Block Grants/States Programs and Non-Entitlement Grants in Hawaii	1,567,844
17.225	Unemployment Insurance	921,020,873
17.225	ARRA-Unemployment Insurance	1,075,269,000
Workforce Investment Act Cluster:		
17.258	WIA Adult Program	14,008,723
17.258	ARRA-WIA Adult Program	5,882,719
17.259	WIA Youth Activities	16,038,806
17.259	ARRA-WIA Youth Activities	12,001,715
17.260	WIA Dislocated Workers	28,878,846
17.260	ARRA-WIA Dislocated Workers	10,168,716
Highway Planning and Construction Cluster:		
20.205	Highway Planning and Construction	522,339,327
20.205	ARRA-Highway Planning and Construction	185,458,469
20.219	Recreational Trails Program	743,311
Title I, Part A Cluster:		
84.010	Title I Grants to Local Educational Agencies	226,055,723
84.389	ARRA-Title I ARRA Grants to Local Education Agencies, Recovery Act	82,194,502
Special Education Cluster:		
84.027	Special Education - Grants to States	151,805,010
84.173	Special Education - Preschool Grants	9,752,321
84.391	ARRA-Special Education - Grants to States	81,325,320
84.392	ARRA-Special Education - Preschool Grants	4,370,843
Vocational Rehabilitation Services Cluster:		
84.126	Rehabilitation Services - Vocational Rehabilitation Grants to States	48,441,534
84.390	ARRA-Rehabilitation Services - Vocational Rehabilitation Grants to States, Recovery Act	2,738,478

COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)

Note 2 - Type A Programs (Continued)

CFDA	Program Title	Expenditures
84.367	Improving Teacher Quality State Grants	45,465,656
State Fiscal Stabilization Fund Cluster:		
84.394	ARRA-State Fiscal Stabilization Fund (SFSF)- Education State Grants, Recovery Act	293,038,700
84.397	ARRA-State Fiscal Stabilization Fund (SFSF)- Government Services, Recovery Act	90,199,300
Immunization Cluster:		
93.268	Immunization Grants	37,976,784
93.712	ARRA-Immunization	1,649,821
Temporary Assistance for Needy Families Cluster:		
93.558	Temporary Assistance for Needy Families	147,928,175
93.714	ARRA-Emergency Contingency Fund for Temporary Assistance for Needy Families (TANF) State Program	3,825,203
93.563*	Child Support Enforcement	44,535,389
93.568	Low-Income Home Energy Assistance	66,792,655
Child Care Cluster:		
93.575	Child Care and Development Block Grant	85,131,885
93.596	Child Care Mandatory and Matching Funds of the Child Care and Development Fund	24,564,662
93.713	ARRA- Child Care and Development Block Grant	32,260,858
93.658*	Foster Care-Title IV-E	47,418,525
93.659*	Adoption Assistance	41,853,200
93.767	Children's Health Insurance Program	123,192,943

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

Note 2 - Type A Programs (Continued)

CFDA	Program Title	Expenditures
Medicaid Cluster:		
93.775	State Medicaid Fraud Control Units	2,090,299
93.777	State Survey and Certification of Health Care Providers and Suppliers	5,784,172
93.778	Medical Assistance Program	4,087,341,324
93.778	ARRA-Medical Assistance Program	505,415,419
Disability Insurance/Supplemental Security Income Cluster:		
96.001	Social Security - Disability Insurance	45,931,639
97.036	Disaster Grants-Public Assistance (Presidentially Declared Disasters)	202,915,276
	Total Type A Programs	\$ 10,967,749,756

Note 3 - Rural Rehabilitation Student Loan Program (CFDA 10.NA (1))

The Kentucky Rural Rehabilitation Student Loan Program was initially awarded \$672,629 in 1970 by the U. S. Farmers Home Administration. Since 1970, the program has operated on interest from student loans outstanding and on income from investments administered by the Office of Financial Management. The Department of Agriculture is no longer in the business of making student loans and reassigned all loans in payment compliance to the Kentucky Higher Education Assistance Authority (KHEAA). The Department of Agriculture retained only those loans that had a delinquent payment history. This program is currently in phase-out status, with authorization from the U. S. Department of Agriculture (USDA) to eliminate the principal through issuance of specific grants and scholarships. Most outstanding loans have been classified as contingent uncollectible liabilities; however, if loan payments are received, they are directly deposited into the principal account. The total amount of money in the investment account as of June 30, 2010 was \$92,251. Student loans and investment earned interest of \$6,072. Outstanding student loans totaled \$64,466. The total grants and scholarships authorized by the USDA in FY 10 totaled \$145,426.

Note 4 - Unemployment Insurance (CFDA 17.225)

The Commonwealth paid out \$1,955,285,075 in benefits in FY 2010. The amounts shown on the accompanying schedule reflect both the amount expended for benefits from the Trust Fund and an additional \$41,004,798 of federal funds expended for administration of the program, resulting in a combined total of \$1,996,289,873 in federal expenditures. Included in this amount is \$1,075,269,000 in benefit payments funded by the American Recovery and Reinvestment Act (ARRA).

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

Note 5 - Highway Planning and Construction (CFDA 20.205)

The information reported for CFDA 20.205 Highway Planning and Construction program represents the activity of all open projects during FY 2010. These projects were funded from several apportionments. Apportionments refer to a federal, statutorily prescribed division or assignment of funds. The expenditures reflected on the schedule include expenditures for advance construction projects, which are not yet under agreements with the Federal Highway Administration.

Program Income - The Highway Planning and Construction Program earned program income of \$17,551,409 in FY 2010. This income is comprised of program income (interest) attributable to the Garvee Bonds.

Refunds - Expenditures for the Highway Planning and Construction Program were shown net of any refunds, resulting from a reimbursement of prior or current year expenditures. Refunds totaled \$2,386,468 for FY 2010.

Note 6 - Outdoor Recreation - Acquisition, Development and Planning (CFDA 15.916) and Recreational Trails Program (CFDA 20.219)

Administrative costs are shown as expended when received from the federal government. These costs are recovered through a negotiated, fixed indirect cost rate. Any over or under recovery will be recouped in the future.

Note 7 - Research and Development Expenditures

OMB Circular A-133 Section 105 states, "Research and development (R&D) means all research activities, both basic and applied, and all development activities that are performed by a non-federal entity."

The expenditures presented in the SEFA include R&D expenditures. The R&D portion of the expenditures for each program is listed below.

CFDA	Program Title	State Agency	Expenditures
10.025	Plant and Animal Disease, Pest Control, and Animal Care	F&W	\$ 40,539
10.028	Wildlife Services	F&W	15,806
15.605	Sport Fish Restoration	F&W	389,670
15.615	Cooperative Endangered Species Conservation Fund	F&W	109,667
15.634	State Wildlife Grants	F&W	1,019,270
16.745	Criminal and Juvenile Justice and Mental Health Collaboration Program	AOC	16,874
93.243	Substance Abuse and Mental Health Services-Projects of Regional and National Significance	AOC	221,826
93.586	State Court Improvement Program	AOC	29,516
Total Research and Development Expenditures			\$ 1,843,168

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

Note 8 - Community Development Block Grants/State's Program and Non-Entitlement Grants in Hawaii (CFDA 14.228)

The Commonwealth matches the federal portion of administration dollar for dollar. Cash expenditures include the federal portion of administration.

Note 9 - Wildlife Restoration (CFDA 15.611)

The Department of Fish and Wildlife Resources leases properties from the U.S. Army Corp of Engineers for Condition Three and Condition Five Projects. These projects stipulate that the properties leased be managed for wildlife purposes and may produce income. The leases for wildlife management rights on these properties are non-monetary. The Department of Fish and Wildlife Resources currently leases the following properties:

- Barren River
- Green River
- Dewey Lake
- Fishtrap Lake
- Barlow Bottoms-Olmstead
- Birdsville Island
- Lake Cumberland
- Paintsville Lake
- Sloughs-Grassy Pond

Any expenditure in excess of revenue from each property listed above will be eligible for reimbursement under the Wildlife Restoration (CFDA 15.611) grant from the U.S. Department of the Interior. The properties listed above are not reimbursed with federal funds if the grant has already been expended to manage other wildlife properties.

Note 10 - 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.

Received From	Direct/Pass Through (Grantor)	State Agency	Amount
<u>Fund for the Improvement of Education (CFDA 84.215)</u>			
Powell County Board of Education	Pass Through (Various)	KHS	\$ 213,855
Total Fund for the Improvement of Education			\$ 213,855

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

Note 11 - Noncash Expenditure Programs

The Commonwealth's noncash programs and a description of the method/basis of valuation follows:

CFDA	Program Title	Amount	Method/Basis of Valuation
10.551	Supplemental Nutrition Assistance Program	\$ 1,164,591,491	EBT Issuance.
10.555	National School Lunch Program	20,296,803	Commodities issued for FY 2010 per ECOS report.
10.565	Commodity Supplemental Food Program	3,254,679	Quantity issued to recipients valued using May 2010 Commodity File.
10.569	Emergency Food Assistance Program (Food Commodities)	8,983,247	Quantity issued to recipients valued using FY2010 ECOS Report.
10.664	Cooperative Forestry Assistance	47,799	Acquisition Cost as indicated by Government Services Administration (GSA).
12.700	Donations/Loans of Obsolete DOD Property	267,437	Depreciated value.
15.250	Regulation of Surface Coal Mining and Surface Effects of Underground Coal Mining	26,193	Inventory of Controlled Property.
15.657	Endangered Species Recovery Program	3,276	Invoice Copy.
39.003	Donation of Federal Surplus Personal Property	478,254	23.3% of federal acquisition cost (\$2,052,593).
66.034	Surveys, Studies, Investigations, Demonstrations and Special Purpose Activities Relating to the Clean Air Act	142,053	EPA contracts with Research Triangle Institute for sample analysis.
93.069	Public Health Emergency Preparedness	10,444,736	Grant Award Document.

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

Note 11 - Noncash Expenditure Programs (Continued)

CFDA	Program Title	Amount	Method/Basis of Valuation
93.116	Project Grants and Cooperative Agreements for Tuberculosis Control Programs	79,796	Grant Award Document.
93.268	Immunization Grants	34,912,487	Grant Award Document.
93.712	ARRA-Immunization Grants	1,550,567	
93.977	Preventive Health Services-Sexually Transmitted Diseases Control Grants	234,247	Grant Award Document.
	Total Noncash Expenditures	\$ 1,245,313,065	

Note 12 - Activity Occurring in Programs with Inventoriable Items

The Department of Agriculture operates a statewide Commodity Supplemental Food Program (CFDA 10.565). The dollar value of the inventory, based on the 2010 USDA Commodity File is as follows:

Commodity Supplemental Food Program CFDA 10.565

Beginning Inventory, July 1, 2009	\$ 861,864
Price Adjustments	114,742
Adjusted Inventory, July 1, 2009	976,606
Received Commodities	3,748,769
Issued to Recipients	(3,254,679)
Net Value of Inventory Adjustments, June 30, 2010	3,064
Ending Inventory, June 30, 2010	\$ 1,473,760

Note 13 - Election Reform Payments (CFDA 39.011)

Interest earned must be used for additional program expenditures.

Note 14 - Pertaining to ARRA Designation

In order to identify ARRA funds on the Schedule of Expenditures of Federal Awards, the ARRA- prefix will precede the Program Title on the Grantor Schedule.

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2010
(CONTINUED)**

Note 15 - Zero Expenditure Programs

These programs had no expenditures related to the respective state agency during FY 10. 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. For CFDA numbers with multiple state agencies listed, the schedule is presented in descending expenditure amount order.

Note 16 - Supplemental Nutrition Assistance Program and ARRA (CFDA 10.551)

The reported expenditures for benefits under the Supplemental Nutrition Assistance Program (SNAP) (CFDA 10.551) are supported by both regularly appropriated funds and incremental funding made available under section 101 of the American Recovery and Reinvestment Act of 2009. The portion of total expenditures for SNAP benefits that is supported by Recovery Act funds varies according to fluctuations in the cost of the Thrifty Food Plan, and to changes in participating households' income, deductions, and assets. This condition prevents USDA from obtaining the regular and Recovery Act components of SNAP benefits expenditures through normal program reporting processes. As an alternative, USDA has computed a weighted average percentage to be applied to the national aggregate SNAP benefits provided to households in order to allocate an appropriate portion thereof to Recovery Act funds. This methodology generates valid results at the national aggregate level but not at the individual State level. Therefore, we cannot validly disaggregate the regular and Recovery Act components of our reported expenditures for SNAP benefits. At the national aggregate level, however, Recovery Act funds account for approximately 15 percent of USDA's total expenditures for SNAP benefits in the Federal fiscal year ended September 30, 2009.

THIS PAGE LEFT BLANK INTENTIONALLY

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



CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

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

Honorable Steven L. Beshear, Governor
Cabinet Secretaries and Agency Heads
Members of the Commonwealth of Kentucky Legislature

We have audited the governmental activities, the business-type activities, the aggregate discretely presented component units, each major fund and the aggregate remaining fund information of the Commonwealth of Kentucky as of and for the year ended June 30, 2010, and have issued our report thereon dated December 17, 2010. We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards applicable to financial audits contained in *Government Auditing Standards* issued by the Comptroller General of the United States.

Internal Control Over Financial Reporting

In planning and performing our audit, we considered the Commonwealth's internal control over financial reporting as a basis for designing our auditing procedures for the purpose of expressing our opinion on the financial statements, but not for the purpose of expressing an opinion on the effectiveness of the Commonwealth's internal control over financial reporting. Accordingly, we do not express an opinion on the effectiveness of the Commonwealth's internal control over financial reporting.

Our consideration of internal control over financial reporting was for the limited purpose described in the preceding paragraph and was not designed to identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses and therefore, there can be no assurance that all deficiencies, significant deficiencies, or material weaknesses have been identified. However, as described in the accompanying schedule of financial statement findings we identified certain deficiencies in internal control over financial reporting that we consider to be material weakness and other deficiencies that we consider to be significant deficiencies.

A *deficiency in internal control* exists when the design or operation of a control does not allow management or employees, in the normal course of performing their assigned functions, to prevent, or detect and correct misstatements on a timely basis. A *material weakness* is a deficiency, or a combination of deficiencies, in internal control such that there is a reasonable possibility that a material misstatement of the entity's financial statements will not be prevented, or detected and corrected on a timely basis. We consider the deficiency described in the accompanying schedule of financial statement findings to be a material weakness, which is identified as finding 10-KST-1.

A *significant deficiency* is a deficiency or a combination of deficiencies in internal control that is less severe than a material weakness, yet important enough to merit attention by those charged with governance.



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

We consider the deficiencies described in the accompanying schedule of financial statement findings to be significant deficiencies, which are identified as findings; 10-KST-1, 10-CHFS-2, 10-CHFS-3, 10-CHFS-4, 10-CHFS-5, 10-CHFS-6, 10-CHFS-7, 10-DOC-8, 10-DOC-9, 10-DOC-10, 10-DOC-11, 10-DOC-12, 10-DOC-13, 10-DOC-14, 10-DWI-15, 10-DWI-16, 10-DWI-17, 10-DWI-18, 10-DWI-19, 10-FAC-20, 10-FAC-21, 10-FAC-22, 10-FAC-23, 10-FAC-24, 10-FAC-25, 10-KDE-26, 10-KDE-27, 10-KDE-28, 10-KDE-29, 10-KDE-30, 10-KDE-31, 10-KDE-32, 10-KDE-33, 10-KDE-34, 10-KHP-35, 10-KHP-36, 10-KSP-37, 10-KST-38, 10-KST-39, 10-KST-40, 10-KST-41, 10-KST-42, 10-KST-43, 10-KST-44, 10-KST-45, 10-PARKS-46, 10-PARKS-47, 10-PC-48, 10-PC-49, 10-REV-50, 10-TC-51, 10-TC-52, and 10-TC-53.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Commonwealth's financial statement for the year ended June 30, 2010, is free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts, and grant agreements, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. However, providing an opinion on compliance with those provisions was not an objective of our audit, and accordingly, we do not express such an opinion. The results of our tests disclosed no instances of noncompliance or other matters that are required to be reported under *Government Auditing Standards*.

Management's response to the findings identified in our audit is described in the accompanying comments and recommendations. We did not audit management's response and, accordingly, we express no opinion on it.

We noted certain matters that we reported to management in separate letters.

This report is intended solely for the information and use of management, of the Commonwealth of Kentucky, others within the entity, and the General Assembly and is not intended to be and should not be used by anyone other than these specified parties.

Respectfully submitted,



Crit Luallen

Auditor of Public Accounts

December 17, 2010

FINANCIAL STATEMENT FINDINGS

FINANCIAL STATEMENT FINDINGS

Material Weaknesses Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-1: The Kentucky State Treasury Should Reconcile The Commonwealth's Bank Accounts To eMARS In A Timely Manner

Historically, the Kentucky State Treasury has performed a reconciliation of the Commonwealth's bank accounts to the accounting system on a daily and monthly basis. Largely due to the implementation of a new financial accounting system, eMARS, Treasury had been unable to reconcile bank accounts to the accounting system in a timely manner for FY 07, FY 08 and FY 09. Treasury has worked with the Finance and Administration Cabinet to develop new reconciliation procedures and to create a more efficient and effective process. However, these problems persisted into FY 10 and as of June 30, 2010, the most recent reconciliation completed was for May 2009.

Although Treasury has made progress in FY 10 the reconciliation process is still behind. The reconciliation process had to be modified due to the implementation of the eMARS accounting system, and new, customized reports had to be developed, which are time-consuming processes and contributed to the delay in reconciliations.

Bank accounts that are not reconciled could result in oversights, errors, and miscalculations that misstate account balances for financial reporting purposes. Given the volume and the size of receipts and disbursements processed by Treasury, these reconciling items could potentially materially misstate the cash and other account balances reported in the CAFR.

Good internal controls dictate that bank accounts be reconciled in a timely manner. Daily reconciliations should be performed within a few days of the actual occurrence and monthly account reconciliations should be performed within a few weeks after the necessary system reports are run at the end of the month.

Recommendation

Treasury should continue to take appropriate steps to ensure monthly bank reconciliations are performed timely. We understand the Commonwealth's change in financial accounting systems was beyond Treasury's control and that this has made the reconciliation process more difficult. However, every effort should be made between Treasury and the Finance and Administration Cabinet (FAC) to complete the FY 10 reconciliations as soon as possible. Going forward, as future accounting system changes occur, we recommend FAC and Treasury address the impact of those changes on Treasury processes as early in the implementation as possible to avoid significant and prolonged gaps in internal controls.

Management's Response and Corrective Action Plan

The Treasury Department is very pleased that the Auditor acknowledges that the reconciliation backlog was beyond the Treasury's Control. The eMARS accounting system, when implemented by the Finance Cabinet, did not have a workable bank reconciliation system. In recent months the Treasury Department has created a reconciliation system, worked to identify and correct data weaknesses in eMARS, and cut the reconciliation backlog by two-thirds. Because of the diligence and determination of current Treasury Department staff, the accounts should be totally balanced within this fiscal year.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-CHFS-2: The Cabinet For Health And Family Services Should Develop Procedures To Ensure Accuracy And Completeness Of Non-Cash Expenditures Reported In The SEFA

The Cabinet for Health and Family Services (CHFS) does not have a reliable system in place for ensuring that accurate and complete financial information is reported for the Immunizations Grants and ARRA-Immunization programs (CFDA 93.268 and 93.712) on the Schedule of Expenditures of Federal Awards - Non-Cash Programs. During our audit of the SEFA, we identified the following problems with the SEFA 3 report:

- The initial non-cash expenditures of \$40,552,567 reported to the Finance and Administration Cabinet (FAC) on the SEFA 3 for the Immunization Grants program (CFDA 93.268) was an estimate and not based on the actual Immunizations supplied to Kentucky, during state fiscal year 2010. OMB Circular A-133 requires states to report the actual value of the immunizations used by the state during the period under audit. CHFS provided the auditor with a “replenishment report” from the Centers for Disease Control that showed actual non-cash expenditures of \$34,912,487 after a verbal audit finding was issued. Had the original estimate been used, the program’s non-cash expenditures would have been misstated by \$5,640,080. CHFS should not be using an estimate when the actual expenditures are available.
- CHFS did not report non-cash ARRA expenditures of \$1,550,567 for the ARRA-Immunizations program (CFDA 93.712) on the initial SEFA 3 schedule that was submitted to the Finance and Administration Cabinet (FAC). And, the initial documentation that was provided to the Auditor as support for the non-cash expenditures reported on the SEFA 3 schedule did not include the non-cash ARRA expenditures for the ARRA-Immunization program. Federal guidelines specify that all ARRA expenditures should be separately accounted for and disclosed on the SEFA.

CHFS lacks adequate controls to ensure the accuracy and completeness of the information that is reported in the SEFA 3 for the Immunizations programs. The likely cause is a lack of written procedures for requesting information from the various departments overseeing the Immunizations programs.

CHFS is not complying with Federal requirements in using an estimate when the actual expenditures are available and by not separately reporting the ARRA non-cash expenditures in the SEFA 3.

OMB Circular A-133 Audits states:

7.22 - The Special Tests and Provisions section of the 2010 *OMB Circular A-133, Compliance Supplement (Compliance Supplement)*‡ (Part 3, Section N) and appendix 7, “Other Circular A-133 Advisories,” describe the compliance requirements for separate accountability of Recovery Act funding Recipients of Recovery Act awards agree (as a condition of accepting the award) to maintain records that identify adequately the source and application of Recovery Act awards. In addition, recipients agree to identify the expenditure of Recovery Act awards separately on the SEFA and the data collection form....

§____.205 - Basis for determining Federal awards expended.

(a) Determining Federal awards expended. The determination of when an award is expended should be based on when the activity related to the award occurs.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-CHFS-2: The Cabinet For Health And Family Services Should Develop Procedures To Ensure Accuracy And Completeness Of Non-Cash Expenditures Reported In The SEFA (Continued)

Additionally, page 3 of the SEFA instructions from FAC states:

On all schedules indicate on the schedule if the information on that schedule is from an ARRA award (i.e. on schedule 6 if there is ARRA funds going to a sub-recipient note on the schedule that this pertains to ARRA funds). Also when there is a CFDA that has both regular and ARRA funds you must identify the regular and ARRA funds separately.

Recommendation

We recommend CHFS develop procedures to ensure accurate accounting and reporting of Immunizations Grants and ARRA-Immunizations program non-cash expenditures in the SEFA. For the non-cash expenditures, the Division of General Accounting personnel who prepare the agency's SEFA should ask for supporting documentation to confirm the non-cash expenditures that are reported in the SEFA.

Management's Response and Corrective Action Plan

In response to the findings during the audit of the SEFA 3 Schedule, the Kentucky Immunization Program (KIP) as a part of the Infectious Disease Branch of the Division of Epidemiology and Health Planning, Department for Public Health, has developed the following written procedures for ensuring the accuracy and completeness of non-cash expenditures reported in the SEFA 3.

An estimate of non-cash expenditures for CFDA 93.268 will not continue to be part of the process of calculating these totals in the future. KIP receives quarterly notices of award for the vaccine budget, which is the main source of non-cash expenditures. The Vaccines for Children (VFC) Coordinator manages this budget in conjunction with Centers for Disease Control (CDC) and the Immunization Program Manager. However, as additional funds become available on a federal level, the actual non-cash expenditure of these funds may increase for Kentucky Vaccine Program (KVP) for vaccine purchase. In this case, CDC does not issue an additional notice of award and often times the notice that the program will receive additional non-cash funds for vaccine purchase is done by e-mail. In the future, the report of SEFA 3 non-cash expenditures will include copies of the quarterly notice of awards for the vaccine budget as well as CDC produced monitoring reports of vaccine non-cash expenditure. This will provide a more accurate account of the funds awarded by formal notice of award as well as additional non-cash funds provided.

As an additional note, CDC has plans to place a Public Health Advisor (PHA) in KIP. When this person is placed, the program will have an increase in non-cash expenditures as PHA's are documented in the federal immunization grant as non-cash expenditures.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-CHFS-3: The Cabinet For Health And Family Services Should Have Controls In Place To Ensure Financial Reports Are Complete And Accurate

During testing of accounts payable, a review of the 2009 Medicaid Benefit Payments was conducted. Upon review of the 2009 Medicaid Benefits Payment, it was determined that the American Recovery and Reinvestment Act (ARRA) funds were not included in the final SFY 09 Medicaid Benefit amount utilized in calculating the accounts payable estimate for FY 10. The Medicaid Benefit amount was understated, causing the percentage of accounts payable for Medicaid to be incorrect.

Reports maintained by agency personnel failed to include ARRA funds for FY 10. This omission of funds caused the accounts payable for FY 10 to be understated. Controls were not in place to ensure that all funds were reported in the closing package, which reports accounts payable to the Finance and Administration Cabinet for reporting in the Commonwealth's Comprehensive Annual Financial Report. The miscalculation of the percentage caused the Medicaid portion of accounts payable estimate to be understated by \$54,652,088, for FY 10.

Good internal controls dictate procedures be in place to ensure that all reports used for financial reporting are complete and accurate. It also requires that personnel be up to date on reporting regulations and requirements, to ensure that all funds are being recorded correctly to limit misstatements.

Recommendation

We recommend CHFS incorporate the following procedures to ensure accurate and complete reporting.

- Require all reporting personnel to be up to date on reporting requirements for all funds.
- Implement procedures to verify that the information is complete and accurate, including agency reports.

Management's Response and Corrective Action Plan

We agree. The accounts payable estimate for FY 2010 has been corrected. DMS staff in the Division of Administration and Financial Management no longer rely solely on the accuracy of the CHFS agency reports in eMARS. Staff now run custom reports and compare the results in order to determine variances and improve accuracy.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-CHFS-4: The Cabinet For Health And Family Services Hazelwood Facility Should Ensure Invoices Are Paid In A Timely Manner

During our FY 10 audit of the Cabinet for Health and Family Services (CHFS) expenditures, we tested forty invoices at Hazelwood Intermediate Care Facility for timeliness of payment. We noted the following exceptions:

- Two invoices totaling \$870 with two different invoice dates for July 2009 and November 2009 were paid seven and eleven months late.
- One invoice totaling \$395 was paid three days late.
- One invoice totaling \$242 was paid two weeks late.

This continues to be a problem. This is a repeat finding from the FY 09 audit noted in Finding 09-CHFS-2.

Payments are not being processed and paid within the specified thirty (30) working days in accordance with KRS 45.453.

Vendors were not paid in a timely manner. Payments may be assessed a 1% late penalty.

KRS 45.453 states, "All bills shall be paid within thirty (30) working days of receipt of goods and services or a vendor's invoice except when the purchasing agent has transmitted a rejection notice to the vendor."

Recommendation

We recommend Hazelwood review and improve the invoice payment process to ensure payments on invoices are made within the prescribed timeframes as set forth in KRS 45.453 and not incur a 1% late penalty as set forth in KRS 45.454.

Management's Response and Corrective Action Plan

The Business Office Staff developed and is implementing new written Accounts Payable processes in order to avoid similar issues in the future. All invoices are date stamped and matched with the correct purchase order. Invoices will be processed immediately if there are no issues with the goods or services procured. Weekly audits of pending invoices by the Business Office Manager are now done to ensure that all invoices are paid within a timely manner or that appropriate follow up actions are taken to resolve any outstanding issues. Executive Staff from each department have been instructed by written memo that no orders shall be placed without prior approval from the Business Office. When orders are placed, vendor information will be secured and verified in the eMARS system to ensure payments are made timely and that multiple vendor names for the same vendor are not being utilized that would create confusion.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-CHFS-4: The Cabinet For Health And Family Services Hazelwood Facility Should Ensure Invoices Are Paid In A Timely Manner (Continued)**

Management's Response and Corrective Action Plan (Continued)

This will help eliminate issues of having to add a vendor to the system after the purchase has already been made. It will also enable the business office to be aware of all purchases that are made within the facility. A new Business Office manager with an accounting degree and a background in health care is being recruited to begin work at the facility January 2011. In the interim, a central office employee from the Division of Administration and Financial Management has been detailed to oversee daily operations of the business office. This individual reports daily to the Department's Director of Administration and Financial Management.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-CHFS-5: The Cabinet For Health And Family Services Should Provide Additional Guidance And Oversight At The Hazelwood Facility

Testing of expenditure procedures at Hazelwood Intermediate Care Facility identified that the business office lacked proper segregation of duties for expenditures in FY 2010. Auditors tested the Imprest Cash Fund for the facility and determined there were many instances of purchases being made without purchase order requests, supporting documentation for the purchase (receipts), or purchases were made lacking approval from appropriate facility personnel. The auditors also noted the facility lacks segregation of duties over purchases. The business office manager was documented requesting and approving the purchase order documents that were available, as well as one instance of a program director requesting and approving the purchase of tickets to a wrestling event, as referred to in finding 10-CHFS-7. The business manager is also responsible for writing checks and requesting reimbursements for those checks, without anyone else in the office verifying who the check was written to, or that it was processed through the bank.

There is a lack of effective oversight by the Cabinet for Health and Family Services, specifically Behavioral Health, Developmental and Intellectual Disabilities (BHDID). Internal controls at the facility are weak; employees of Hazelwood are able to request checks for events or programs without any type of tracking document for the purchase. When those employees return from the event or program, they are not required to provide any type of supporting documentation, such as travel logs, receipts or employee and patient lists for attendees.

The lack of internal controls allowed \$11,574 in purchases to be made by the Hazelwood Intermediate Care Facility with little to no supporting documentation for purchases from the Imprest Cash Fund Account.

Good internal controls dictate that controls be in place to monitor expenditures being made by the facility and personnel. These controls include monitoring of purchases to ensure they are allowable, reasonable, and follow standard purchasing procedures as outlined by Finance in FAP 111-55-00.

- An agency shall maintain a small purchase order file containing the price quotations requested, quotations received, a tabulation of prices offered, and comments by the agency handling the small purchase concerning the basis for placing the order. The agency shall retain these records for audit and review purposes.

Recommendation

We recommend CHFS implement more stringent internal controls:

- Require purchase orders be signed and approved by appropriate business office personnel for any purchase.
- Require all personnel return receipts, travel logs, personnel and patient logs, as supporting documentation for purchases made.
- Purchase orders with invoices should be maintained in accordance with Finance policy.
- Purchasing personnel should be trained and up to date on Finance requirements for purchases made.
- Provide guidance and oversight at the Hazelwood Intermediate Care Facility.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-CHFS-5: The Cabinet For Health And Family Services Should Provide Additional Guidance And Oversight At The Hazelwood Facility (Continued)**

Management's Response and Corrective Action Plan

The auditors noted that the Business Office did not have proper segregation of duties for expenditures during the FY 2010 year. This was due to short staffing resulting from several extended medical leaves. Accordingly, the Business Office has now put policies in place that will assure proper separation of duties, notwithstanding any employee absences or turnover. The list of duties is in writing and in the process of being incorporated into formal facility policy (after review by governing board).

It was also noted that there were imprest cash purchases made without proper purchase requests and signatures. In order to minimize the opportunity for similar occurrences, the Department is revoking Hazelwood's imprest cash authority and closing the account. While imprest cash will no longer be used, the Hazelwood Business Office is updating purchasing processes and will make written policies available to staff. Purchase requests exceeding \$500 will require sign off by both the Fiscal/Business Office manager and the facility director; with purchases less than \$500 requiring approval of the Fiscal/Business Office manager. A new Business Office manager with an accounting degree and a background in health care is being recruited to begin work January 2011. In the interim, a central office employee from the Division of Administration and Financial Management has been detailed to oversee daily operations of the business office. This individual reports daily to the Department's Director of Administration and Financial Management.

All recommendations by the auditor's office are being incorporated into current practice including requiring receipts, travel logs, personnel and patient logs as supporting documentation. Practices will be in writing and will be consistent with the Finance and Administration Cabinet's FAP's and any other requirements. Updates to procedures will be presented to the Facility Director by December 15, 2010. The Facility Director will review and forward them to the Commissioner for the Department's review with an anticipated effective date of January 1, 2011. This will ensure future transactions have necessary documentation and approvals.

Additionally, the Cabinet's Division of Procurement Services is scheduling on-site Procurement training for staff. Anticipated completion of the on-site training is not later than January 31, 2011.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-CHFS-6: The Cabinet For Health And Family Services Should Improve Policies And Procedures Over Its Imprest Cash Accounts

In testing expenditures of the Hazelwood Intermediate Care Facility, we reviewed the Imprest Cash Account utilized by the facility. Review of this account revealed that bank reconciliations were not being performed by the business office in a timely manner. During the audit the following problems were noted:

- Eleven months (July, August, September, October, November, December, January, February, March, April, and May) had reconciliations that were not performed until September 2010. June's reconciliation was not available to auditors for review.
- One instance of conflicting dates noted on reconciliation supplied to the auditors. The date on the first page of the reconciliation was dated eleven (11) months prior to the actual month end of the account.
- Reconciliations were being signed off as complete, but were missing supporting documentation marked as reviewed per the Imprest Cash Internal Audit checklist (such as purchase orders, receipts, manager approvals)
- One instances of missing reconciliations, and associated account information.
- Two instances in which the Imprest Cash Fund Account was overdrawn. Auditors noted that NSF fees were being paid from the account in the amount of \$60.
- Reimbursements to the facility for expenses paid from the Imprest Cash Account ceased in December 2009. Claims are not being submitted to CHFS.
- Based upon review of available reconciliations, there were twenty eight (28) instances of checks being voided after reimbursement, reimbursed twice, or requesting reimbursement for wrong amount.

There is a lack of effective oversight by the Cabinet for Health and Family Services, specifically Behavioral Health, Developmental and Intellectual Disabilities (BHDID). Business office personnel of Hazelwood Intermediate Care Facility were not performing reconciliations or monthly reimbursements as required. Personnel at the facility informed audit staff that there was a high turnover in staff at the beginning of the fiscal year, causing required business office functions to not be performed in a timely manner.

Monthly bank reconciliations must be performed to ensure that accounts are up to date and that all amounts withdrawn have been accounted for and to verify the accuracy of bank statements and ledger balances. This will ensure that all recorded expenditures are accounted for. Proper reconciliation procedures should also help ensure that the facility is performing requests for reimbursement in a timely manner and not overdrawing the account, thereby avoiding unnecessary NSF charges.

Per the Finance and Administration Cabinet, the following recommendations are made concerning reconciliations of cash accounts:

- Someone independent of the cash receipt process should summarize cash receipts. This summary should be compared to the State Treasury deposits to ensure that all collections are deposited intact. Reconciliation of cash receipts into eMARS against an agency's internal accounting system should also be performed.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-CHFS-6: The Cabinet For Health And Family Services Should Improve Policies And Procedures Over Its Imprest Cash Accounts (Continued)

- Someone independent of the cash receipt function should reconcile the mail log where cash and receipts are initially received, to the daily cash and receipts activity. Subsequently, a comparison of actual currency and coins deposited with actual currency and coins received should be conducted.
- Monies received on prepaid accounts should be reconciled with deposits and posting to the accounting records.

Per FAP 111-56-00 IMPREST CASH FUNDS:

- **PROPER USE OF IMPREST CASH FUNDS:** The preferred methods of payment for all expenses are the state's procurement and accounting systems and the state procurement card. An agency shall use imprest cash funds only if it is impractical or impossible to make payments through one of the preferred methods.
- **HOW TO ESTABLISH IMPREST CASH FUNDS:** (d) The agency custodian shall establish a bank account for the Imprest Cash Fund at the Commonwealth's depository bank and order checks. The custodian shall write checks to make payments authorized by the authority and prepare an agency imprest cash voucher. The custodian shall also prepare a summary of disbursements and requests for reimbursement per instructions of the Division of Statewide Accounting Services.

Recommendation

The following are recommendations for bank reconciliations of the Hazelwood Imprest Cash Account:

- Accounts should be reconciled within 30 days of the month end for cash accounts.
- Reconciliations should agree the bank balance and the ledger balance, and those balances should be readily traceable to the bank statement and ledger.
- Reconciliations should be performed by someone not directly involved with recording transactions in the Imprest Cash Account.
- The preparer and reviewer (preferably the finance director) sign and date the reconciliations indicating they are complete and have been reviewed.
- Reconciliations, supporting bank statements and ledger balances should be maintained on file in accordance with the facilities' and CHFS' record retention policy.

Management's Response and Corrective Action Plan

The Department is revoking Hazelwood's imprest cash authority and closing the account.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-CHFS-7: The Cabinet For Health And Family Services Should Strengthen Policies And Procedures To Ensure That Appropriate Documentation And Authorization For Expenditures Are Maintained At The Hazelwood Facility

During our review of the Hazelwood Intermediate Care Facility imprest cash account, we found a lack of appropriate documentation and proper authorization for expenditures from the account, including:

- One expense in the amount of \$469 for the replacement of a patient's chair that disappeared. No documentation of complaint filed by parent or police report was on file to justify the purchase.
- One expense for lodging in the amount of \$150 had no supporting documentation.
- Expenses for program entertainment trips totaling \$3,939 with no documentation logging the patients and staff attending events. These trips were to movie theaters, wrestling events and other activities that could easily be used by non-authorized individuals.
- Several expenses totaling \$470 for local wrestling events with circumstances suggesting the purchase of these tickets benefited a staff member, who wrestled in the wrestling association. Auditors learned that the association selects the main event based on tickets sold, giving the employee a possible incentive to inflate sales. This is a conflict of interest.
- Ten checks totaling \$1,121 were reimbursed twice.
- Seventeen checks totaling \$724 were voided after being reimbursed.
- Imprest Cash Account documentation at the Finance and Administration Cabinet does not list the correct bank account information and appears to not be updated.

The facility is using Imprest Cash Account rather than eMARS to process many programmatic and operating expenditures which obscures the details of the expenses and keeps all controls and monitoring at a local level. Also, the agency lacks proper controls over maintaining appropriate supporting documentation to justify expenditures and authorizations for purchases.

Failure to maintain appropriate supporting documentation and evidence of authorizations increases risk that expenditures could be made that are not necessary or reasonable for the program's operations, and also increases the risk of fraud.

Good internal controls dictate maintenance of adequate supporting documentation of expenditures and proper authorization documentation.

Per the Finance and Administration Cabinet Policy FAP 111-56-00:

Proper Use of Imprest Cash Funds: The preferred methods of payment for all expenses are the state's procurement and accounting systems and the state procurement cards. An agency shall use imprest cash funds only if it is impractical or impossible to make payments through one of the preferred methods.

Per KRS 11A.020, Public servant prohibited from certain conduct - Exception - Disclosure of personal or private interest.

- (2) If a public servant appears before a state agency, he shall avoid all conduct which might in any way lead members of the general public to conclude that he is using his official position to further his professional or private interest.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-CHFS-7: The Cabinet For Health And Family Services Should Strengthen Policies And Procedures To Ensure That Appropriate Documentation And Authorization For Expenditures Are Maintained At The Hazelwood Facility (Continued)

Recommendation

We recommend the CHFS Behavioral Health, Developmental and Intellectual Disabilities (BHDID) implement policies to:

- Document the types of expenditures permissible to run through Imprest Cash Account, and file this with CHFS and FAC for Imprest Cash Account documentation. This policy should be in line with FAP 111-56-00.
- Update imprest cash bank account documentation with Finance and Administration Cabinet.
- Maintain all documentation supporting expenditures, their authorization and justification.
- Educate employees about the Executive Branch Code of Ethics Conflict of Interest policy and have employees sign a statement of awareness and understanding of the policy and implications of violating the policy. Refrain from expenditures that present conflicts of interest for staff. When unavoidable, ensure the appropriate justification and authorization is documented and require employee to recuse him/herself from decisions regarding the matter and from initiating, processing, or authorizing transactions related to it.

Management's Response and Corrective Action Plan

Effective immediately any client-owned items found missing will be investigated by Hazelwood's facility security before the item is replaced. A report from Security and/or the Police will be included with the request for replacement.

The facility's imprest cash account is being closed. The individual involved in this purchase of tickets for resident activities is no longer employed by this facility.

All Executive Staff, Business Office staff, and Human Resources staff will attend mandatory in-service training on the Executive Branch Code of Ethics Conflict of Interest within the next six months with the first training session being conducted December 17, 2010. Training will be conducted annually thereafter.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DOC-8: The Department Of Corrections Should Expand, Finalize, And Implement A System Development Life Cycle Policy To Govern System Development, Testing, Modifications And Implementation

As noted during three previous audits, the Department of Corrections (DOC) has not finalized or implemented formal System Development Life Cycle (SDLC) procedures governing controls for system development, testing, modifications, and implementation in relation to the Kentucky Offender Management System (KOMS). DOC drafted an SDLC policy based upon the Microsoft Solutions Framework (MSF); however, completion and distribution of the policy was not anticipated until the end of June 2010.

DOC chose to use the Governance Model to direct their SDLC process. This model utilizes the following five stages: envisioning, planning, developing, stabilizing, and deploying. DOC has also adopted a modified version of the Royce Waterfall Model as their preferred method for developing software solutions. This model follows a sequential software development process and includes the following seven phases: requirements gathering, design/develop, implementation, integration, testing, installation, and maintenance.

KOMS has been divided into three phases for complete statewide implementation. DOC is in the process of completing the third phase to implement KOMS statewide. For KOMS, the vendor is only responsible for performing the initial system qualification testing using test scripts developed by the vendor. Following successful completion of this test, the scripts are turned over to DOC who is responsible for functional testing and for making any modifications to the system.

The vendor has provided DOC with a Software Test Plan, which guides the testing before implementation. According to this process, appointed individuals, called Subject Matter Experts (SMEs), review the software and system to ensure that the proper functionalities are included, according to the External Design Functions. This process is performed each time a system is replaced by a function of KOMS. Documentation of the testing is retained by DOC through HelpBox tickets and release notes. Any changes or enhancements that are made to the system require Executive Staff approval. After each KOMS module is tested, the Commonwealth Office of Technology (COT) is responsible for moving the modules into the production environment. It appears this process will be adequate, once formally implemented and if properly followed.

Without formalized SDLC procedures, management increases the risk of implementing ineffective and inefficient systems and the risk of entering inaccurate or incomplete data within the production environment, thereby adversely affecting system processing results.

SDLC procedures should be developed and distributed to all key personnel to ensure consistent implementation of new systems. The SDLC procedures should address all key steps comprising the software development process. SDLC procedures require that formal test plans be adequately developed and documented, that testing be performed within a test environment separate from production environments, and that test results and resolutions be documented. All testing documentation should be reasonably retained for future reference. Further, SDLC procedures must be consistently applied.

FINANCIAL STATEMENT FINDINGS*Significant Deficiencies Relating to Internal Controls and/or Noncompliances***FINDING 10-DOC-8: The Department Of Corrections Should Expand, Finalize, And Implement A System Development Life Cycle Policy To Govern System Development, Testing, Modifications And Implementation (Continued)**

Recommendation

We recommend DOC expand, finalize, and implement adequate formal SDLC control policies and procedures to govern all DOC systems currently under development and to be used for all future software development projects. These policies and procedures should outline all stages of the SDLC process and should include testing strategies and methodologies, control and maintenance of test and production environments, testing documentation and retention requirements, and procedures for migration of system changes to the production environment. Further, these formal procedures should be developed centrally and distributed to all divisions within DOC for compliance.

Management's Response and Corrective Action Plan

DOC has finalized the Software Development Life Cycle documents and has posted them to our intranet. The document templates can be found on the intranet site.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DOC-9: The Department Of Corrections Should Strengthen And More Closely Adhere To The Kentucky Offender Management System (KOMS) Defect Management Process

As noted in the prior two audits, review of program modification controls for the Department of Corrections (DOC) Kentucky Offender Management System (KOMS) identified multiple instances where the existing program change control procedures were not being consistently followed.

The KOMS Defect Management Process describes the procedures for requesting and completing modifications to KOMS. DOC Information Technology (IT) staff and KOMS trainers may request changes to KOMS using tickets within the in-house HelpBox application. Issues are prioritized, and either DOC or the vendors develop a solution. The vendors view the KOMS requests and address any software defects; defects are resolved by the creation of new KOMS releases or patches. All defects are logged and tracked in the vendor-maintained KOMS Defect Tracking Tool. If the issue does not require a programming solution, it is deemed to be a technical assistance request and is assigned to DOC IT staff for completion.

Releases or patches developed by the vendors are sent to DOC for approval and testing, and then the testing documentation is sent back to the vendors to review. The KOMS Defect Management Process developed by DOC states DOC Executive Staff is to provide written approval to the vendors for releases or patches; however, DOC management indicated they do not adhere to this approval procedure. Once the release, patch, or DOC-developed change is tested and approved by the appropriate parties, DOC IT staff makes an email request to the Commonwealth Office of Technology (COT) Service Desk for movement of the change into production. Once the change has been implemented and the associated ticket has been closed by COT, a notification email is sent to DOC IT staff.

Our review of 126 unique logged KOMS software issues and associated release notes since the prior year fieldwork revealed:

- Forty-four issues (approximately 34.9 percent) had a priority level of '0'. This is not a valid priority level based on the KOMS Defect Management Process and discussions with agency staff.
- Nineteen issues (approximately 15.1 percent) lacked a priority level.
- Twenty issues (approximately 15.9 percent) did not have the tester, testing date or results recorded.
- One issue (approximately 0.80 percent) omitted the Issue Identification (ID).

To further test the controls surrounding KOMS program modifications, a sample of eleven completed KOMS issues was reviewed to ensure all supporting documentation for testing and approvals were appropriately developed and maintained. This examination revealed the following exceptions:

- Three issues (approximately 27.3 percent) did not have an associated HelpBox ticket on file to justify the initial defect notification.
- Seven issues (approximately 63.6 percent) for which the release notes and HelpBox ticket reflected differing priority levels.
- Four issues (approximately 36.4 percent) for which documentation could not be provided to show the approval was sent to COT prior to being placed into production.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DOC-9: The Department Of Corrections Should Strengthen And More Closely Adhere To The Kentucky Offender Management System (KOMS) Defect Management Process (Continued)

DOC is currently in the process of implementing a new tracking system, Trac. The first phase of converting HelpBox tickets to Trac has been completed. Trac will allow KOMS software errors and fixes to be connected to the various milestones within the change process. Trac will also work in conjunction with the current HelpBox application to enhance the ability to determine the type and status of changes to KOMS. The migration to Trac means that tickets will still go to HelpBox initially and will be classified as either functional, defect, or enhancement. Functional issues will remain within HelpBox until closure. Defects and enhancements, however, will be migrated from HelpBox to Trac for further tracking.

Failure to properly apply and monitor change control procedures increases the risk that incorrect or unauthorized changes could be made to critical applications and, potentially, be moved into the live production environment. Further, this failure in process increases the risk that changes will not be prioritized appropriately, which could untimely affect the progress of changes to implementation.

Program modification control procedures should be consistently applied in order to ensure that only appropriately authorized changes to critical applications are made and implemented within the production environment in a timely fashion. Consistent monitoring of the change control process helps ensure adequate documentation exists for all changes and that the changes made are acceptable to the user business areas prior to implementation.

Recommendation

We recommend DOC take the following actions to strengthen the controls of the KOMS program modification process:

- Review the current KOMS Defect Management Process document to ensure the established procedures are appropriate and acceptable to all parties. Revisions should be made where necessary.
- Ensure all KOMS software issues are logged within the HelpBox tracking system and assigned an accurate priority level and issue ID.
- Proceed with the implementation of Trac system. Within the new system, all defect and enhancement details should be retained, as well as the associated authorization, testing, and promotion documentation.
- Once the Trac system is formally implemented, procedures in the KOMS Defect Management Process document should be updated to reflect appropriate changes in the program change tracking process.
- Ensure the KOMS release notes are thoroughly completed to reflect all issue details and testing documentation.
- Consistently apply all established procedures within the KOMS Defect Management Process document.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances***

FINDING 10-DOC-9: The Department Of Corrections Should Strengthen And More Closely Adhere To The Kentucky Offender Management System (KOMS) Defect Management Process (Continued)

Management's Response and Corrective Action Plan

DOC has been working actively to migrate from the HelpBox system into the new defect tracking system. DOC will migrate to the new tracking system by August 15, 2010. All KOMS software defects that are identified will be assigned a ticket number for tracking. All changes to the KOMS workflow will be documented and posted to the project website by the end of September 2010.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DOC-10: The Department Of Corrections Should Formalize And Consistently Apply Logical Security Controls Over KRONOS

As noted in the two previous audits, the Department of Corrections (DOC) did not have formal written security policies and procedures related to the KRONOS payroll system. Therefore, DOC did not have a KRONOS security manual to address management, user, and administrator responsibilities concerning the system. An informal procedure was used for requesting, approving, and granting access to KRONOS for applicable users. However, discussions with DOC management indicated they anticipate formal procedures will be drafted by the end of June 2010.

The current informal procedures dictate elevated permissions provided through the Project View and Super access levels is only granted to managers with a direct supervisory relationship to the employees whose payroll records they have the ability to update. Managers requiring access to view payroll records corresponding to employees not under their direct supervision must complete the KRONOS Access Request form to justify the reason for the additional access. After completion, the request form must be emailed to the manager's immediate supervisor. The request form instructions require the supervisor to sign off and submit the request form to the payroll staff. Once received by the Payroll Branch Manager, the form will be marked approved, denied, or will be returned for additional information. No supervisor or Payroll Branch Manager approval sign off fields were available on the request form.

Of 14 users currently requiring access to view the payroll data of employees outside their direct supervision, we noted the following:

- Six users, or approximately 42.9 percent, had the KRONOS Access Request form on file; however, it lacked a supervisor sign off.
- Four users, or approximately 28.6 percent, had the KRONOS Access Request form on file; however, it was completed and submitted by the user requesting access and not their immediate supervisors as required by the form instructions.
- One user, or approximately 7.1 percent, had no KRONOS Access Request form on file. According to agency management, this user no longer performs timekeeping responsibilities for the group to which she was originally assigned. Her access was removed during our audit fieldwork.

Allowing users the ability to access information without proper authorization may subject the processing of data to errors and/or omissions and may compromise the integrity of data processed through the KRONOS system.

The foundation of logical security is access control, which refers to how system access is determined and granted to users. Formal policies provide a security framework to educate management and users of their security responsibilities. Consistent application of formalized security policies and procedures provides continuity for implementation and sets the tone of management concern for strong system controls. Further, the level of system access granted to users should be restricted to only areas necessary for an employee to perform assigned job duties.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DOC-10: The Department Of Corrections Should Formalize And Consistently Apply Logical Security Controls Over KRONOS (Continued)

Recommendation

We recommend DOC proceed with drafting, formalizing, and implementing a KRONOS security manual. Included in this manual should be descriptions of the processes and procedures for requesting, approving, and granting appropriate system access to all users requiring KRONOS access. The procedures should, at a minimum, achieve the following:

- Provide guidance for the authorization and establishment of general user accounts and manager accounts granted Read access.
- Detail the use of organizational structure in the authorization and setup of manager accounts granted elevated permissions through Super and Project View access.
- Stipulate a requirement for the submission of a KRONOS Access Request form where a manager is required to read the payroll data for employees not falling under the direct chain of command.
- Specify steps to be taken in the event an account requires an amendment to the granted access level or revocation.

Further, we recommend the KRONOS Access Request form be revised to include an authorization sign off field for the supervisor and Payroll Branch Manager. Due to there being a relatively small number of users with access to view other employee's data not under their direct supervision, we suggest the revised request form be completed for all of these users and the form be consistently used in the future.

Management's Response and Corrective Action Plan

KRONOS Security Manual will be drafted, revised and finalized by the end of October 2010. KRONOS Access Request form will be revised to incorporate changes recommended by the audit team. A new access form was created by Payroll Manager on July 14, 2010. This form will be sent out to all payroll liaisons with specific instructions to detail who needs to request the access, with manager approval as well as Payroll Manager approval prior to access being granted. The form is to be disseminated by close of business on July 31, 2010.

All manager access/super access authorities will be audited in house monthly to ensure proper procedures are being followed.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DOC-11: The Department Of Corrections Should Complete Implementation Of Information Technology Security Policies

As noted since our Fiscal Year (FY) 2006 audit, the Department of Corrections (DOC) has not implemented formalized security policies. Though the DOC Information Technology Branch drafted a security policy entitled Individual User Access to Computer Information and Resources as early as December 2005 and updated the draft policy as recently as December 2006, it was not formally adopted and implemented. Since that time, additional draft policies were created, but were not formalized and implemented.

Specifically, the following DOC policies have been developed, but not finalized:

- Individual User Access to Computer Information and Resources;
- DOCIT-010 User ID and Password Protocol;
- DOCIT-011 Anti-Virus Protocol;
- DOCIT-012 Internet and Acceptable Use Code of Conduct;
- DOCIT-013 Password Auditing and Protocol Enforcement for Network Domains;
- DOCIT-014 Securing Unattended Workstations Protocol;
- DOC Standard Application User Profiles; and
- Information Technology Appropriate Use Protocol.

In discussions with agency personnel during the FY 2010 audit, it was noted the completion and distribution of the DOC security policy was scheduled for the end of June 2010. Once completed and distributed, these policies are to include policies relating to security passwords, userids, user access, regular review of unauthorized login attempts and disaster recovery procedures. All applications and systems are to be covered by the policy.

Failure to implement formal information system security policies increases the risk of unauthorized access or modification to computer programs and data, destruction of assets, and interruption of services.

Development and consistent application of information system security policies and procedures provides continuity for policy implementation and sets the tone of management concern for securing information system assets and resources. To strengthen security over the DOC computing resources, a formal security policy that addresses all applications must be centrally and formally developed, implemented, distributed and enforced.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-DOC-11: The Department Of Corrections Should Complete Implementation Of Information Technology Security Policies (Continued)**

Recommendation

We recommend DOC ensure currently developed information security policies are updated to reflect management's decisions related to the security procedures, officially adopted, implemented and distributed to all DOC personnel. Further, DOC should ensure compliance with all security policies is enforced on a consistent basis.

Management's Response and Corrective Action Plan

DOC has updated the protocols and formalized them and posted them to the DOC intranet.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DOC-12: The Department Of Corrections Should Ensure All Agency Machines Are Properly Configured To Include Only Necessary Services

As noted in the prior year, our FY 2010 security vulnerability assessment on machines owned by the Kentucky Department of Corrections (DOC) revealed 29 of 115 scanned machines, or approximately 25.2 percent, could potentially be mis-configured. A mis-configured machine could waste resources, entice an attack using ports that are unnecessarily open, or allow excessive hypertext transfer protocol (HTTP) methods. The ports open on each of these machines should be reviewed to ensure they have a specific business purpose and that the services are properly authorized. Fifteen of these machines contained open ports reported during the prior year audit. Of the 29 potentially mis-configured machines, two machines reported the potential use of a remote shell suite of programs.

For security purposes, detailed information that would identify the specific machines contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

System misconfigurations that allow unnecessary services can negate other security configurations established on the machine, increase potential security vulnerabilities, and provide enticements for intruders to enter the system. Further, improperly secured services could allow unauthorized access to sensitive or critical system resources. Specific to web servers, excessive HTTP methods provide additional avenues for system intrusion. The use of unsecured transmission programs also increases the risk of compromised data transmissions.

To assist in securing a network adequately, it is necessary to ensure all machines and web services are configured to only allow necessary services to operate. Only necessary business-related ports should be open and anonymous or default profiles should be avoided. Only the necessary HTTP methods (such as POST, HEAD, and GET) should be supported on agency web servers.

Recommendation

We recommend DOC take the necessary actions to ensure the noted services on each machine have a specific business purpose and are properly authorized. If the service is necessary, it should be reviewed to ensure it is properly authorized, licensed, and configured as well as adequately secured. Any unnecessary services should be disabled or the associated ports should be closed. HTTP methods not required for the operation and maintenance of a web server should be disabled. If the remote shell suite of programs is being utilized, it should be replaced by a more secured shell suite.

Management's Response and Corrective Action Plan

DOC will investigate all listed devices and reported vulnerabilities within the report. DOC will compile all actions taken for each IP address that was provided and will complete this task by the end of September 2010. The DOC would like to note that access to the devices that were provided is only accessible from within the DOC network because of the firewall that we have in place.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-DOC-13: The Department Of Corrections Should Ensure Sufficient Authentication Is Required To Access Potentially Sensitive Information**

As noted in the prior year, during the FY 2010 audit of the Kentucky Department of Corrections (DOC), instances were discovered where no authentication was required to allow an outside user to gain access either to information about the machine or to the service running on a designated port. We determined 12 out of the 115 machines scanned, or approximately 10.4 percent of the population, did not have sufficient authentication. Ten of these machines were reported to the agency during the prior year audit.

For security purposes, detailed information that would identify the specific machines contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

If a machine is allowed to provide excessive information associated with the machine to an anonymous user, then an intruder could potentially use this information to attempt to gain access to the machine or network.

Only necessary and required users should have access to services, particularly those services containing potentially sensitive information.

Recommendation

We recommend DOC restrict the level of information provided by their network machines to public or anonymous users. If a service is not necessary, required, and properly configured, it should be disabled. For appropriate services, authentication should be configured, and only users who have a need for services should be given user IDs and passwords for access.

Management's Response and Corrective Action Plan

DOC will investigate all devices listed and disable anonymous/public access where permissible. The DOC would like to note that access to the devices that were provided is only accessible from within the DOC network because of the firewall that we have in place. Documentation and configuration of this will be completed by the end of August 2010.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-DOC-14: The Department Of Corrections Should Ensure Necessary Steps Are Taken To Mitigate Identified Vulnerabilities On Agency Machines**

While performing the FY 2010 security vulnerability assessment for the Kentucky Department of Corrections (DOC) machines, we determined 1 out of 115 scanned machines, or approximately 0.9 percent, contained a user login webpage that was susceptible to authentication parameter manipulation. Specifically, the user ID and password length restrictions could be manipulated at the client side before being exchanged with the server.

For security purposes, detailed information that would identify the specific machines contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

The ability to circumvent established input restrictions at the client could allow the submission of malicious code or superfluous information. These could then result in potential buffer overflows, Denial of Service (DoS) attacks, or Cross Site Scripting (XSS).

Client communication should be appropriately sanitized at the server to ensure that only appropriate responses are submitted to the server.

Recommendation

We recommend DOC ensure all client communication with the noted machine is appropriately sanitized to comply with all input restrictions. All client communication in non-compliance should be rejected.

Management's Response and Corrective Action Plan

DOC will investigate the device that was detected and document any configuration changes made to the device to comply with the recommendation. This will be completed by August 15, 2010. The DOC would like to note that access to the devices that were provided is only accessible from within the DOC network because of the firewall that we have in place.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DWI-15: Unemployment Insurance Should Implement Procedures To Ensure Its Accounts Payable Estimate Is Accurate And Complete

During the Department for Workforce Investment (DWI) Accounts Payable audit, the auditor was unable to verify some of the check registers provided as support for the estimated accounts payable to claimants and to the IRS. Based on our review, two errors were discovered that would amount to \$14,435,835 if not corrected.

The first error was a check register being omitted from their closing package preparation process. The amount omitted that should have been included in the accounts payable was \$2,734,702.

The second error was more complex and amounted to \$11,701,133. Each of DWI's check registers is generated for a two week pay period without consideration of the different fiscal years. The UI check registers show totals for each week of the two week period. Their process only picked up the full weeks which ended on or before June 30. When the fiscal year end falls on Friday or Saturday, their process gives the correct results. When the fiscal year falls on Sunday through Thursday, their process did not give the correct results.

After the auditors explained the errors, DWI took pro-active steps to correct the errors. The AFR-70 accounts payable was updated by DWI. A revised closing package was re-issued and submitted to FAC to reflect the adjusted amount for inclusion in the CAFR.

One check register was omitted from the closing package preparation process causing an understatement in accounts payable. The other check registers were included, but the days were not properly prorated among fiscal years. Such mistakes lead to misstating the UI accounts payable and subsequently misstating the closing package AFR-70 amounts.

Good internal controls over the accounts payable function require that all check register transactions be captured and allocated where appropriate. Proper internal controls are needed in order to ensure the appropriate AFR-70 closing package amount is reported. These measures are necessary to ensure the completeness of UI accounts payables, facilitate the reconciliation to accounting records, and ensure accurate financial reporting.

Recommendation

We recommend DWI-UI take steps each year to review the fiscal year end check registers and the accounts payable allocation process to ensure accuracy and completeness

Management's Response and Corrective Action Plan

We agree with the auditor's finding and have taken corrective action to prevent this issue in the future.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DWI-16: The Department For Workforce Investment Should Strengthen The Disaster Recovery Plan

As noted during the last six audits, our assessment of the Department For Workforce Investment (DWI) business continuity planning revealed that, although planning documents have been created, some information was either not sufficiently detailed or required clarification.

The DWI has created and formalized the following documents regarding disaster recovery:

- The Kentucky Unemployment Insurance (UI) Disaster Recovery Plan (DRP);
- EDU-06 Backup Procedures Policy;
- Division of Technology Services (DTS) Business Contingency Plan (BCP); and,
- DWI DTS DRP.

Review of the UI DRP revealed a lack of information for the back-up schedule and off-site storage location, details about the pyramid notification system used by supervisors in case of an emergency, details surrounding cooperative efforts with the Department of Revenue to back up quarterly reports and payments, information regarding employee awareness and training related to the DRP, and documentation concerning how alternate work sites would be determined in the case of an emergency.

The EDU-06 Backup Procedures Policy provides details concerning back up strategies, schedules and requirements for the entire Education Cabinet. Discussions with agency personnel revealed DTS is responsible for back-ups at the central level; however, the policy does not specifically state this responsibility.

A review of the DTS DRP revealed there was no specific information presented for recovery procedures related to the Unemployment Insurance Accounts (UIA) and the Unemployment Insurance Benefits (UIB) system. Further, there is no documentation within the DTS DRP related to employee awareness and training or disaster recovery testing procedures, results, or future testing plans.

The Commonwealth Office of Technology (COT) performs annual Disaster Recovery tests for select systems. Discussions with DWI personnel revealed that UIA, UIB, and Wage Records Systems (WRX) were last tested successfully in 2004. The UIA and UIB systems were included in a 2009 test; however, due to problems with two critical databases, system recovery was unable to be completed. According to agency management, budgetary constraints were the reason for the length of time between tests.

We are aware additional funding has been requested from the Federal government to assist in the updating of DWI disaster recovery plans.

Failure to maintain a complete and current 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.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DWI-16: The Department For Workforce Investment Should Strengthen The Disaster Recovery Plan (Continued)

Good management practices minimize risks through planning. The goal of a DRP or BCP is to improve preparedness at minimal cost using available resources. Accordingly, proper documentation, knowledge, and periodic training for the DRP assures that DWI's IT systems can be recovered in cases of emergency, and that critical processes are not hindered by lengthy system down time. An effective DRP should document the most current critical personnel and contact information, critical systems and related data files with specific backup and recovery procedures, training and testing requirements, and update procedures intended for the DRP. In addition, assurance of adequate asset management and insurance coverage should be considered as part of the DRP.

Recommendation

We recommend DWI update current documentation related to the agency overall DRP. Specifically, we recommend the UI DRP be updated to include details regarding:

- the back-up schedule and where the off-site storage is located,
- the pyramid notification system,
- the back-up of quarterly reports and payments at the Department of Revenue,
- how employees are educated or trained concerning the procedures in case of an emergency,
- documentation of how alternate work sites are determined in case of an emergency, and
- an incorporation, by reference, of the EDU-06 Backup Procedures Policy.

We recommend DWI update the EDU-06 Backup Procedures Policy to reflect agency staff responsible for performing back-up procedures at the central and field level.

Updated copies of these documents should be distributed to key personnel and a copy be maintained centrally and within an appropriate off-site storage area.

In addition, we encourage DWI to continue working with the Department of Revenue on creating electronic images of hard copy forms to allow all critical data to be backed-up electronically.

Finally, DWI should continue discussions with COT to allow for scheduling of Disaster Recovery testing for the UIA/UIB and WRX systems as soon as funding is available.

Management's Response and Corrective Action Plan

The Division of Technology Services agrees with this finding. An independent vendor is currently doing an evaluation of the Business Continuity Policy including the Disaster Recovery Plan, upon completion recommendations will be evaluated and implemented. We have and will continue to evaluate and update the current policies in place making them more comprehensive in their scope, to include but not limited to back-up schedules, off-site storage location, and notification system.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-DWI-17: The Office Of Employment And Training Should Develop Formal System Documentation To Support Processing Performed By The Workforce Investment Act Online Reporting Of Kentucky System**

Our FY 2010 audit of the Office of Employment and Training's (OET) Workforce Investment Act (WIA) Online Reporting of Kentucky (WORK) system revealed OET did not maintain basic documentation of the overall functionality or specific processing of the WORK system.

The WORK system was based on a vendor-developed application customized for the Commonwealth of Kentucky. It was designed to manage the process of initiating, reviewing, and awarding grant monies offered by the State Pass-Through Entity for WIA, the Department for Workforce Investment (DWI), to the Local Workforce Investment Area (LWIA) offices. WORK also manages the processes of reimbursement, financial reporting, and progress reporting. The original contract with the application vendor required a user manual be created for use at the LWIAs and training be provided for the central level staff. The vendor did not provide specific user or technical manuals to OET for use by the central level staff. Further, no user or technical documentation has been developed and finalized internally at OET for central level staff. OET recently drafted a manual for central level staff; however, the draft manual is limited in scope and does not cover administrative or other grant or reporting functions for central level staff.

We are aware the contract with the application vendor for the WORK system expires on May 31, 2010, and OET is looking at potential options for either replacing or upgrading the current system.

Lack of documentation increases the likelihood of erroneous or incomplete processing. It further increases the likelihood of unauthorized data modification, destruction of assets, and interruption of services.

Proper documentation should be maintained for each critical system in production to, at a minimum, identify the purpose of the system, what procedures can be performed within the system, how the system will interact with other systems, and what output of data or reports are anticipated.

Recommendation

We recommend OET work with the application vendor to develop an overview of the specific procedures currently available within the WORK system. Due to the fact the WORK system may be replaced or upgraded within the next year, we further recommend OET include a requirement within the next contract to provide a technical manual for the new system. This manual should specifically cover the overall functionality of the system, the administration of the system, and the processing of transactions at the central and LWIA levels. Finally, going forward, OET should specifically monitor the adherence of the vendor to all contractual obligations.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-DWI-17: The Office Of Employment And Training Should Develop Formal System Documentation To Support Processing Performed By The Workforce Investment Act Online Reporting Of Kentucky System (Continued)**

Management's Response and Corrective Action Plan

DTS Security will be working with OET to implement the policies and procedures manual for the WORK system. We will work with the vendor to obtain the scope of this application and will create procedures for granting access, creating and assigning passwords, resetting passwords, the different levels of access and develop the guidelines for who gets the different levels of access.

We will develop a policy manual with following information:

- *The scope of the project.*
- *Procedures for granting access*
- *Documentation of how the program works.*
- *Training of staff - how to use the program.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DWI-18: The Office Of Employment And Training Should Strengthen And Consistently Apply Administrative Logical Security Procedures Over The Workforce Investment Act Online Reporting Of Kentucky System

Our FY 2010 audit of the Office of Employment and Training's (OET) Workforce Investment Act (WIA) Online Reporting of Kentucky (WORK) system revealed the informal administrative logical security controls over the WORK system were lax. This lack of formal documentation of controls for the system has allowed a situation where staff were provided excessive rights based on current job duties and a lack of understanding on the requirements for administering the system.

Six levels of access were allowed to the WORK system. Three of these levels were explicitly defined within the Grantee Help Manual and are being used by staff at the Local Workforce Investment Area (LWIA) offices. The remaining three levels of access are being used by central level Department of Workforce Investment (DWI) staff; however, there is no documentation of the exact functionality established for each of these central access levels. The auditor was able to glean from discussion with staff and inference of functional characteristics within the Grantee Help Manual, that these three central access levels allow administration of user accounts, development of allocation for grants, and approval of applications from LWIAs for grant funding. The only specific difference identified by OET management between these access levels is one access level has the ability to create a new grant within WORK. Therefore, all central level staff, no matter individual job duties within the system, have been provided both administrative and operational functionality, which creates a segregation of duties situation.

During discussions with OET staff related to the WORK system, it was determined there is currently no access level established within the system that would allow "read" only access to data and reports. If someone needs information from WORK and does not have access, an authorized WORK user will publish reports for the individual. However, our review identified an instance where this process was not followed. Specifically, as part of the review process for the Financial portion of the DWI audit, an auditor requested access to the WORK system. OET provided this auditor with the same access level as a central level employee; thereby, providing the user with both administrative and operational functionality, which is excessive based on the auditor's needs and request.

Our review of the Grantee Help Manual, which is provided to LWIA staff for processing at the LWIA level within the WORK system, identified the process to be followed by LWIA staff to request, delete, or change access for users, was no longer accurate. According to Section 1.1.6 of the Grantee Help Manual, DWI requires that the Chief Executive Officer of a LWIA write a letter to the DWI Budget and Support Branch Manager requesting access for each member of the LWIA that will be accessing WORK. This process was followed when WORK was first implemented; however, has since been changed. Currently, requests for new access, deletion, or changes in status require a written request from either the LWIA Fiscal Officer or Authorized Signatory. A written request is the only requirement for Level 2 (LWIA Staff Member) or Level 4 (Fiscal Officer) access. A Level 5 (Authorized Signature) access request requires both a written request and a signed OET Authorized Signature Form.

We examined supporting documentation for 12 new user accounts to determine compliance with the established informal procedures currently in use for granting access.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-DWI-18: The Office Of Employment And Training Should Strengthen And Consistently Apply Administrative Logical Security Procedures Over The Workforce Investment Act Online Reporting Of Kentucky System (Continued)**

Our examination revealed that only 2 users had sufficient documentation on file to support all access levels granted. The remaining 10 users, or 83.3 percent of new user accounts, did not have documentation on file supporting all or part of their granted access levels to the WORK system.

As was noted in the prior year, the OET Authorized Signature Form only authorizes a user to apply for signatory authority access within WORK. There is currently no way to designate on this form any other type of access level for the WORK system, nor has there been a separate request form developed and used for the other access levels. The auditor is aware of a new access form being developed for use at the central level to request access to the WORK system. However, at this point, no specific access form has been developed for use with LWIA staff.

During the FY 2009 audit of the WORK system, we identified several accounts that appeared no longer to be needed. For FY 2010, we found that all but two of the unnecessary accounts were made inactive as had been indicated by OET at the end of the prior audit. These two accounts are associated with the same user. It was explained that this individual left the agency in December 2008, but had returned to the agency in May 2009. One of the accounts was currently being used by the individual and was required for his job; the other account was no longer needed, but had been inadvertently allowed to remain active after the prior year.

Additionally, within the FY 2009 audit, we questioned the need for individual users to be established with both Fiscal Officer and Authorized Signatory rights at the LWIAs. Due to staffing resources at some LWIAs, OET management decided to allow this dual function for users if the LWIA Director provided approval through a formal request for the access. During the FY 2010 review of users, there were nine users identified with both Fiscal Officer and Authorized Signatory rights. We examined supporting documentation for all nine user accounts to determine compliance with the established informal procedure. Our examination revealed that only one user had sufficient documentation on file. The remaining 8 users, or 88.9 percent of users, did not have documentation on file supporting all or part of their granted access levels to the WORK system. In one case where there was insufficient support, the individual provided the Fiscal Officer and Authorized Signatory rights is the LWIA Director.

We are aware the contract with the application vendor for the WORK system expires on May 31, 2010, and OET is looking at potential options for either replacing or upgrading the current system.

Failure to develop and implement administrative logical security controls could lead to a lack of understanding by management and users of specific roles and responsibilities, which could result in a failure to comply with security policies, a failure to perform assigned security responsibilities, or inappropriate and inefficient use of system resources. If the developed controls are not sufficiently strong, this situation increases the risk of unauthorized data modification, destruction of assets, interruption of services, and inappropriate or illegal use of system resources.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DWI-18: The Office Of Employment And Training Should Strengthen And Consistently Apply Administrative Logical Security Procedures Over The Workforce Investment Act Online Reporting Of Kentucky System (Continued)

The foundation of logical security is access control, which refers to how system access is determined and granted to users. Formal policies provide a security framework to educate management and users of their security responsibilities. Consistent application of formalized security policies and procedures provides continuity for implementation and sets the tone of management concern for strong system controls. Further, the level of system access granted to users should be restricted to only areas necessary for an employee to perform assigned job duties.

Recommendation

We recommend OET create, formalize, and implement a WORK security manual. This manual should include the procedures for requesting, approving, and granting system access to all users requiring WORK access. The Grantee Help Manual should be updated to reflect the current access request process. Additionally, a new WORK access request form should be developed for central level and LWIA staff. This form should include a listing of the available access levels, a description of the access levels, and space for all appropriate management approvals. Access request forms should be completed and maintained for all users.

We recommend OET work with the application vendor to determine whether a security access level is currently available which would allow only read access to the system. If this is currently available, then OET should alter the auditor's access to this access level.

For those LWIA staff provided both Level 4 (Fiscal Officer) and Level 5 (Authorized Signatory) access, OET should require authorization from the current LWIA Director confirming the necessity of both levels of access. OET should define an alternative procedure for approval for those instances where the staff requiring the Fiscal Officer and Authorized Signatory access is the LWIA Director. This authorization should be maintained for audit purposes.

Due to the fact the WORK system may be replaced or upgraded within the next year, we are recommending OET include the following items within the next contract:

- The next vendor should provide a security manual for the new system. This manual should, at a minimum, specifically cover all access levels available in the system; the process for requesting access to the system; the process for establishing, altering, revoking, and deleting access to the system for users; and appropriate use guidelines for all users.
- All available access levels should be identified and associated access rights for each level should be explicitly described.
- A read-only access level should be available for use.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-DWI-18: The Office Of Employment And Training Should Strengthen And Consistently Apply Administrative Logical Security Procedures Over The Workforce Investment Act Online Reporting Of Kentucky System (Continued)**

Recommendation (Continued)

In anticipated of the new or upgraded system,

- OET should provide a listing of all currently active users to the individual LWIAs to be reviewed and validated for appropriateness.
- OET should review the currently active central level staff to ensure access is still necessary.
- Any user accounts identified as no longer necessary should be changed to inactive status.
- OET should specifically identify the functionality needed within the system for each central level staff. Using this information, functional groups should be identified, such as administration, grant review, and allocation. These functional groups should be provided as defined access levels to the vendor for inclusion in the new system.

Management's Response and Corrective Action Plan

DTS will work with OET and the vendor on the different levels of access and develop the guidelines for who gets what level. We will also have the levels of access on the request form and have a designator requestor from OET send us requests after their approval.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DWI-19: The Office Of Employment And Training Should Ensure Programmatic Logical Security Controls Are Properly Designed And Configured

Our FY 2010 audit of the Office of Employment and Training's (OET) Workforce Investment Act (WIA) Online Reporting of Kentucky (WORK) system revealed programmatic logical security controls were not designed or properly configured to ensure only authorized users interact with the system.

User accounts can be established by users granted one of three central access levels. When a new user account is created, the user will be provided a user name and initial password. The password must be changed by the user on first login. The criteria established for the syntax of a valid password are very minimal:

- Password must be at 7-12 characters in length.
- Password must not be "password."
- The same password may not be used twice in a row.

However, there is not a password lockout threshold and passwords do not expire.

Additionally, OET staff is unaware of a function within the WORK system that would allow a password for a current user account to be reset. According to OET, if a user is unable to remember his or her password, then an authorized member of OET may either create a new account for the user or look up the current account's password. It was determined the password is shown in clear text within the source code of the user information screen in the WORK system.

Finally, it was noted that user accounts within the WORK system are numeric and issued sequentially. There were three user accounts identified during review of user accounts within the system that did not follow this anticipated syntax. OET management was unaware of why these accounts were established differently from the other accounts, nor how the account names were established with a different syntax.

We are aware the contract with the application vendor for the WORK system expires on May 31, 2010, and OET is looking at potential options for either replacing or upgrading the current system.

The existence of non-expiring passwords, the lack of a lockout threshold, and the sequentially numbered user names increase the risk that an unauthorized user could attempt to access the system and would not be identified. A password cracking tool could be run against a known user account without causing a disruption in service to the user, since the account would never be locked out, even if a large number of incorrect passwords were attempted. Since the tendency of most users with non-expiring passwords is to keep the same password indefinitely, a potential intruder has the advantage of an unlimited amount of time to work with an account to determine the correct password.

Further, the fact passwords are viewable in clear text increases the risk a current user of the system with access to this information might impersonate another valid user. Because a legitimate user account name and password would be used, there would be no direct indication of inappropriate use.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-DWI-19: The Office Of Employment And Training Should Ensure Programmatic Logical Security Controls Are Properly Designed And Configured (Continued)

The Commonwealth Office of Technology (COT) has issued an Enterprise Policy related to logical security controls over user accounts and passwords, CIO-072, UserID and Password Policy. This policy was originally established in 2002 and most recently updated in May 2007. Within this policy, COT establishes specific expectations for user IDs and password controls.

Passwords must be:

- Kept confidential;
- Changed at least every 31 days unless otherwise approved (non-expiring passwords must be approved on an exception basis);
- Changed whenever there is a chance that the password or the system could be compromised;
- Encrypted when held in storage or when transmitted across the network when the path is connected to an external network.

Passwords must:

- Be eight (8) or more characters;
- Contain uppercase letter(s);
- Contain lowercase letter(s);
- Contain a number;
- Contain a special character.

Password History

Individuals must not reuse previously used passwords. To prevent this, a password history of 12 or more previous passwords must be kept.

Password Change

Passwords must be changed by the user at least every 31 days. If inadvertent disclosure is known or suspected, the passwords must be changed immediately. NOTE: In the event misuse is suspected, do NOT change the password; IMMEDIATELY notify the System/Network Administrator and/or the agency's security office. A security incident must be documented. Subsequent password change shall be made by the System/Network Administrator's and/or agency's security office direction only.

Minimum Password Age

Where supported, the minimum password age must be set to one day. This will help prevent users from "cycling" through passwords, thus bypassing the password history list. However, if inadvertent disclosure is known or suspected, the password must be changed immediately. In such instances, notify the systems administrator immediately.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-DWI-19: The Office Of Employment And Training Should Ensure Programmatic Logical Security Controls Are Properly Designed And Configured (Continued)**

Password and UserID Lockout

To prevent individuals from attempting to log-in with UserIDs by guessing passwords, accounts will be locked after three (3) consecutive invalid log-in attempts. Password resets must follow the policy stated herein for password length/composition.

Further, it is good business practice to develop a system that would allow a password to be reset, if there is an occasion where a user has forgotten his or her password. This control should be maintained at an appropriately high level of management and requests for password resets should be documented and maintained for review.

Recommendation

We recommend OET work with the application vendor to alter the password control configurations within the system to comply with the CIO-072, UserID and Password Policy. These control configurations should include, at a minimum,

- Passwords should be at least 8 characters.
- Passwords should contain at least one upper case letter, lower case letter, number, and special character.
- Passwords should be changed every 31 days.
- Passwords should have a minimum age value of 1 day.
- A password history of the last 12 passwords should be maintained.
- Accounts should be locked out of the application after three consecutive invalid log-in attempts.

OET should request the application vendor to restrict access to the underlying source code of the user information page, if possible. If that is not possible, the password information should be removed from the source code and stored only in an encrypted format to be used within the password validation process.

Further, OET should work with the application vendor to determine if a password reset function is available within the current system. If so, this process should be formally documented, distributed to all appropriate staff, and immediately implemented.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-DWI-19: The Office Of Employment And Training Should Ensure Programmatic Logical Security Controls Are Properly Designed And Configured (Continued)**

Recommendation (Continued)

Due to the fact the WORK system may be replaced or upgraded within the next year, we are recommending OET include the following items within the next contract:

- The password control configurations must adhere to the CIO-072, UserID and Password Policy settings.
- Any instance of the password being stored within or transmitted from the application should be appropriately encrypted.
- A password reset function should be available within the system.

Management's Response and Corrective Action Plan

DTS will work with the vendor to determine if a password reset function is available and a password lockout threshold. DTS will also work with the vendor to remove the password information from the source code.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-FAC-20: The Finance And Administration Cabinet Should Ensure Formalized Policies Are Developed And Implemented Governing Security Over Microsoft Outlook Public Folders

During the fiscal year (FY) 2010 audit of the Finance and Administration Cabinet (Finance), we discovered the Commonwealth Office of Technology (COT) had not developed formalized policies or consistently provided other guidance to agency staff related to the Microsoft Outlook Public Folders.

A concern was brought to our attention from another audit conducted by this office where agency staff responsible for Public Folders was not provided guidance on how to properly administer the folders leading several folders to be open for viewing and modification by anonymous users. Discussions with COT staff in charge of the Public Folders revealed that once the top level folder was established, the administration of this top level folder and any sub-folders will be the responsibility of agency staff. The COT staff confirmed no policies, procedures, or guidance were provided to agency staff explicitly defining their responsibilities related to the security of these Public Folders.

While researching this issue, on March 9, 2010, we found a video on the COT website discussing how to establish and secure Public Folders. According to this video, COT establishes top level Public Folders at the request of the agency's COT Technical Contact. The top level folder will be established with security role for the Default and Anonymous Permissions set to "None," thereby restricting access to the folder to all users. The security of the folder and any sub-folders are then turned over to the agency to administer. Further, examples were provided on how to secure the folders.

On March 22, 2010, we found the COT website had been updated and redesigned. During the website change, the Public Folders video had been removed from the COT website. At this time, there is no plan for COT to return this video to the website.

As noted during the prior year audit, we discovered the Finance Cabinet and the Information Systems Public Folders were not secured adequately. Our review of the Finance Cabinet Public Folder identified two calendars viewable by an anonymous user. Appointments were viewable for agency-use vehicles containing information related to the vehicle use such as requesting employee, reasons for use, and destinations. Further, our review of the Information Systems Public Folder identified one calendar and one email folder viewable by an anonymous user. The calendar appears to be used for scheduling of program changes and outages for State systems. The Role was set to "Author" for the email folder, which allows access to not only view contents, but also add and modify the contents. The issues associated with the calendars in each folder were identified during the prior year audit.

Failure to document in writing formalized policies and procedures that affect all state agencies increases the risk that users will be unaware of critical business processes and allow sensitive information to be viewable to all state employees. The permissions granted to the 'Finance Cabinet' and 'Information Systems' Public Folders could allow an individual to potentially gain or change useful information concerning staff movements and schedules.

Development and consistent application of formalized policies and procedures provides continuity for policy implementation and sets the tone of management concern for ensuring the appropriate usage of information system assets and resources.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-FAC-20: The Finance And Administration Cabinet Should Ensure Formalized Policies Are Developed And Implemented Governing Security Over Microsoft Outlook Public Folders (Continued)

Upon agency request, COT creates the top level Public Folder in Outlook for use by the agency. Agency representatives control permission rights to files and folders as determined by each agency's business requirements.

According to the Office of the Chief Information Officer (CIO), Enterprise Policy CIO-060, Internet and Electronic Mail Acceptable Use Policy, "Agencies that permit the use of E-mail to transmit sensitive or confidential information should be aware of the potential risks of sending unsecured transmissions. E-mail of this nature should, at a minimum, contain a confidentiality statement. E-mail content and file attachments considered highly sensitive or confidential must be encrypted using the Enterprise Standards (X.509 certificates) and approved product for secure electronic messaging services. To protect confidential data, some federal laws require the use of encrypted transmission to ensure regulatory compliance."

Recommendation

We recommend the following actions be implemented by Finance to ensure confidential information is properly secured:

- Formalized policies and procedures should be developed and communicated to agency personnel to ensure all appropriate staff is aware of how to use, setup, and maintain Microsoft Outlook Public Folders.
- COT should return the instructional video related to Public Folders to the website and reference the video to all new agency staff working with Public Folders.
- The user permissions established for the calendars and email folder discussed within this comment should be changed to "None," thereby eliminating the ability of unauthorized users to view entries within the calendars or email folders.
- Specified Finance staff should periodically review the security control permissions applied to all agency Public Folders and subfolders to ensure secure roles restrict anonymous access.

Management's Response and Corrective Action Plan

Permissions assigned to Outlook Public Folders are highly dependent on agency business needs. Individual agencies are responsible for assigning the permissions to their Outlook Public Folders and assessing the appropriateness of this access. To offer guidance in this area, COT is working to place the instructional video in an appropriate location on the COT website to be referenced by all agencies that utilize Outlook Public Folders.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-FAC-21: The Finance And Administration Cabinet Should Ensure Anonymous Access Is Limited Through Network Neighborhood

Based on an issue originally identified during the fiscal year (FY) 2009 audit of the Office of Financial Management (OFM) related to the ability to access a machine housing the Complete Asset Management, Reporting, and Accounting (CAMRA) application, it was determined the Finance and Administration Cabinet (Finance) did not properly restrict access to machines on one of its domains. As noted during the prior year audit, review of this Finance domain through Network Neighborhood revealed 206 out of 253 machines within the oversight responsibility of the Commonwealth Office of Kentucky (COT) allowed access without authentication of the requesting user. Of the 206 machines, 143 machines had files or folders that were accessible. Also, the auditor was able to access into sub-folders within 71 machines. Of the machines holding sub-folders, 38 machines contained files or documents in which the auditor could view. The information found on the accessible machines included databases, reports, resource drivers, messaging logs, image files, and various executable files.

Additionally, further review of the machine housing the CAMRA application identified an anonymous user had the ability to access files within a production data directory and download them to an external location.

For security purposes, detailed information concerning the specific machines contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

Sensitive or inappropriate material that is placed in a shared file can be obtained by unauthorized users if not properly secured. Further, if a machine is not configured to prohibit anonymous access, then an intruder could potentially use this available resource to attempt to gain access to the network.

Security measures should be in place to adequately secure files on local workstations. Access to an agency's domain machines should be restricted to only users requiring access related to a valid business purpose. All anonymous access should be prohibited.

Recommendation

We recommend Finance work with COT to review all machines within the domain discussed above to ensure resources are adequately secured. Security on all network machines should be configured to prohibit anonymous access, unless a valid business purpose is determined and specifically documented. Periodic reviews of domain machines should be performed to ensure anonymous access is not allowed.

Management's Response and Corrective Action Plan

COT is in the process of reviewing the detail findings provided by the auditors. All network machines included in the detail findings will be reviewed to ensure that they are adequately secured. Access that does not have a specific business need will be removed.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-FAC-22: The Finance And Administration Cabinet Should Expand Logical Security Over The UNIX Servers

As noted during the prior three audits of the Finance and Administration Cabinet (Finance), logical security controls should be strengthened over enhanced Management Administrative and Reporting System (eMARS) UNIX servers. We tested the security controls established for three UNIX servers determined to be critical to eMARS processing. Various security related control weaknesses were noted during the audit as detailed below.

Security Policy and Procedures Documentation

For fiscal year (FY) 2010, the Commonwealth Office of Technology (COT) stated UNIX servers are managed in accordance with COT-067, Security Standard Procedure Manual, and CIO-072, User ID and Password Policy. These two documents adequately address logical security. However, they do not discuss on-going monitoring of access to ensure users continue to have a valid business purpose for retaining access to the servers.

It was documented during the FY 2007 review that user audits were being performed periodically to ensure only authorized users have access to the three UNIX servers. Discussion with COT personnel revealed user audits have not been performed since FY 2007. Current plans are in place for COT to develop a procedure for the auditing and monitoring of UNIX accounts; however, this was not completed during FY 2010.

User Access Accountability and Authorization

An examination of new UNIX server accounts revealed user access authorization was inadequate for one user on all three servers under review. An authorization form was provided for this user; however, it did not specify the machines for which the user was shown as having access. This user was also a member of a group on all three servers, but the group profile was not identified on the access authorization form.

Additionally, five users continue to have access to one of the servers reviewed despite COT stating the access was unnecessary in the prior year's review.

Default Security Options

The last password change date was reviewed for all user and system accounts with access to the three UNIX servers to determine if the password had been changed according to policy. A comparison between the last password change date and the last time a user logged in resulted in the following issues:

- One account with access to one or more of the servers had changed its password according to policy, however, the account had not been used to login to the server recently. Due to inactivity, this account should be reviewed to ensure access is necessary.
- Two accounts with access to one or more of the servers had not changed their password recently, but the last login attempt was made prior to the date in which the password was changed. Due to inactivity, these accounts should be reviewed to ensure access is necessary.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-FAC-22: The Finance And Administration Cabinet Should Expand Logical Security Over The UNIX Servers (Continued)

- Thirteen accounts with access to one or more of the servers were found to have been last changed prior to the date expected for our testing and the last login attempt was within 35 days of the last changed date. Due to password age, these accounts should be reviewed to ensure access is necessary.
- One account with access to one or more of the servers was found to have been last changed prior to the date expected for our testing; however, the last login time stamp was over 35 days past the last changed date. This account appears to violate the password policy of requiring a password reset after 35 days.

COT had established default security options for their UNIX servers, as well as user account password restriction defaults. We tested the actual settings of the three critical eMARS UNIX servers and the active users to ensure the settings agreed with the established defaults. Our testing revealed the following:

- One account on one server where the password setting was weaker than both the COT policy and industry recommended setting.

For security purposes, detailed information that would identify the specific servers or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

Failure to implement and consistently apply logical security controls could lead to a lack of understanding by management and users that could result in a failure to comply with security policies, failure to perform assigned security responsibilities, or inappropriate and inefficient use of system resources. This situation increases the risk of unauthorized data modification, destruction of assets, interruption of services, or inappropriate or illegal use of system resources. The existence of unnecessary accounts is inviting to intruders and can lead to those accounts being utilized by unauthorized users.

Adequate security policies and procedures should be implemented, properly maintained, and consistently applied to provide continuity for policy implementation and set the tone of management concern for a strong system to secure assets and resources.

Recommendation

We recommend Finance management work with COT to expand UNIX logical security policies and procedures to include a procedure for the auditing and monitoring of UNIX accounts. Further, UNIX server settings should be reviewed to ensure the established user security options conform to COT policy.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-FAC-22: The Finance And Administration Cabinet Should Expand Logical Security Over The UNIX Servers (Continued)**

Management's Response and Corrective Action Plan

COT has developed a process to conduct annual reviews of user access on the UNIX servers. This process is scheduled to be implemented by the end of the current calendar year. Once in place, this process will be evaluated to determine if all requirements within the findings have been met. COT will continue to work with the Finance Cabinet to address any concerns that are not resolved by this process.

COT has reviewed the detail findings provided by the auditors. Through this review, it has been determined that a significant number of the accounts identified in the findings as having active access to systems were in a state that prevented this access. Each finding has been reviewed and appropriate actions have been taken, or put in motion, to resolve items identified that do not have a documented valid business need. Some review and actions will require participation by the agency. COT will work with the Finance Cabinet to address these concerns.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-FAC-23: The Finance And Administration Cabinet Should Formalize And Consistently Apply A Policy To Govern The Security Of The eMARS Production Databases

During the fiscal year (FY) 2010 audit of the Finance and Administration Cabinet (Finance), it was determined informal logical security procedures existed for granting access to the Enhanced Management Administrative and Reporting System (eMARS) production databases and establishing non-expiring passwords for specific types of accounts; however, these procedures were neither formally documented nor consistently applied. This situation was also noted during the previous two audits.

In order to request access to the eMARS production databases, a COT-F181 form must be completed, authorized electronically, and emailed to the Commonwealth Service Desk for processing within the FrontRange Information Technology Service Management (ITSM) application. Of 2 new individual users with access to the eMARS production databases, 1 user, or 50 percent, did not have a COT-F181 form on file.

Additionally, nine instances were identified where database user accounts were active for employees who were either no longer employed by the state or associated agencies, or who transferred to positions that no longer required access to the production databases. Specifically noted:

- Two users with access to the infoAdvantage production database transferred to another agency and no longer required access to the database. One of these users was noted during the prior year's audit.
- Four users' eMARS access had been revoked, yet all four still retained access to the infoAdvantage production database. Two of these users were noted during the prior year's audit.
- Two former CGI employees retained access to the financial production database, one of which also had access to the Vendor Self Service database. Both of these users were noted during the prior year's audit.
- One user with access to the Advantage Financial production database, infoAdvantage production database, and ePayment Gateway (ePAY) production database transferred to another agency and no longer requires access to the ePAY or Advantage Financial production databases.

As a result of the inquiry into these accounts, Finance indicated all of the unnecessary database accounts would be removed.

There are three user profiles utilized for the eMARS production databases. Two of these profiles are for system accounts or by outside agency automated jobs to extract information from the data warehouse. The accounts within these profiles require non-expiring passwords. The final user profile is used for the remaining individual users who are required to change passwords. The current process related to establishing accounts with non-expiring passwords requires the submission of the COT-F085 Security Exemption Request Form to the COT Security Administration Branch. The agency director and executive director must sign the request, and COT must indicate approval.

There were a total of six accounts established since the previous audit granted one of the profiles allowing non-expiring passwords. A COT-F085 form was not on file for two of the six accounts.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-FAC-23: The Finance And Administration Cabinet Should Formalize And Consistently Apply A Policy To Govern The Security Of The eMARS Production Databases (Continued)

Failure to consistently apply logical security controls could lead to a lack of understanding by management and users that could result in a failure to comply with security policies, failure to perform assigned security responsibilities, or inappropriate and inefficient use of system resources. This situation increases the risk of unauthorized data modification, destruction of assets, interruption of services, or inappropriate or illegal use of system resources. In addition, whenever electronic signatures are accepted forms of authorization, there should be another form of documentation on file, such as emails, to substantiate those signatures. The existence of unnecessary accounts is inviting to intruders and can lead to those accounts being utilized by unauthorized users.

Established security policies and procedures should be formally documented and consistently applied to provide continuity for policy implementation and set the tone of management concern for a strong system to secure assets and resources. Access should only be granted to approved users, and access should be removed promptly upon termination of employment or when said access is no longer required.

Recommendation

We recommend Finance formally document and consistently apply logical security procedures to ensure only authorized access is granted to the ePayment Gateway, Finance and Administration, Vendor Self Service, and infoAdvantage production databases. These procedures should require the COT-F181 form for establishing or changing access for accounts and the COT-F085 forms for authorizing a non-expiring password. Furthermore, emails authorizing these forms should be retained for audit purposes. All user setup documentation should be retained in a central repository for audit purposes.

In addition, Finance should develop procedures related to state employees, CGI employees, and agency contractors to ensure Finance Controller's Office is informed of terminations. Upon notification, Finance should ensure access to the eMARS application and underlying databases is promptly removed or revoked, depending upon whether historical account maintenance is required. Further, all production database accounts should be monitored at least bi-annually to ensure inactive or unnecessary accounts are removed or revoked.

Management's Response and Corrective Action Plan

COT has logical security procedures in place for the addition, modification, or removal of access to production databases. These procedures require that access be appropriately documented and authorized with a completed COT-F181 form. In addition, any account that requires a non-expiring password must be documented with an authorized and approved COT-F085 Security Exemption Request form. This documentation is to be retained within the COT service ticket system. The COT Security Administration Branch will work with the COT Data Management Branch to ensure that they are fully aware of the existing procedures.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances***

FINDING 10-FAC-23: The Finance And Administration Cabinet Should Formalize And Consistently Apply A Policy To Govern The Security Of The eMARS Production Databases (Continued)

Management's Response and Corrective Action Plan (Continued)

The Finance Cabinet has obtained a listing of existing accounts for the eMARS production databases from the COT Data Management Branch and is in the process of reviewing this information to remove unneeded or unnecessary accounts. The Finance Cabinet will establish a procedure to request a listing of production database accounts on a semi-annual basis to review this access. In addition, the Finance Cabinet will work to include language in the security documentation for eMARS that will require that they are notified of terminated employees to facilitate removal of unneeded or unnecessary accounts.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-FAC-24: The Finance And Administration Cabinet Should Develop And Implement A Formal Policy To Govern Security Of The eMARS Checkwriter Interface Process

As noted during the previous three audits, the Finance and Administration Cabinet (Finance) has yet to develop or implement a formal policy identifying responsibilities of those individuals involved with the Enhanced Management Administrative and Reporting System (eMARS) Checkwriter (CW) interface process. The Finance Statewide Accounting Services (SAS) is ultimately responsible for the processing of CW files. Further, SAS is responsible for ensuring access to CW files is reasonable. SAS should ensure a proper segregation of duties exists between the creator of the CW file and the person certifying the file for processing and check generation through eMARS. These duties are established through the use of eMARS security roles and a manual review process performed by SAS during the central level certification.

Our examination of the CW certification process revealed one CW file where the individual who loaded and certified at the department level was the same user.

Allowing users the ability to both create CW files and certify those files for processing and check generation increases the likelihood of unauthorized payments and may compromise the integrity of data processed through the system. A lack of formalized policy and procedures concerning the CW file access and processes can lead to inconsistent understandings between the agency, management, and users.

Formally implemented policy and procedures concerning CW access and established processes is necessary to allow both management and users to have a clear understanding of respective responsibilities. These controls are imperative to ensure the reasonableness of individual access as it relates to CW files and proper segregation of duties when processing CW files.

Recommendation

We recommend Finance establish formal policy and procedures to govern the security surrounding CW interface access and the submission and certification processes. This effort should include standardized procedures to ensure proper segregation of duties at the agency and central levels between the individuals creating and uploading the CW file and those individuals placing the certification on the CW file. This policy should explain the responsibilities associated with each of the CW interface security roles and discuss the need to assign these roles to different individuals, where possible, to ensure proper segregation of duties.

In the event that the same user is required to load and department certify a checkwriter file, the formalized CW interface security policy should require the department head or designee to request prior approval from SAS. Further, if the central level certifier determines that a checkwriter file has already been loaded and certified by the same user, SAS should elicit justification for these actions from the department. SAS should document the request and associated approval or refusal.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-FAC-24: The Finance And Administration Cabinet Should Develop And Implement A Formal Policy To Govern Security Of The eMARS Checkwriter Interface Process (Continued)****Management's Response and Corrective Action Plan**

Finance agrees that formal procedures should be established to govern the security surrounding the checkwriter submission/load and agency certification process. These procedures should explain the necessity to have a proper segregation of duties in regards to the checkwriter load and checkwriter certification process.

Finance also agrees that there should be procedures in place to sufficiently document those times when the segregation of duties cannot be met and the same person performs both functions. We are preparing for an upgrade to eMARS (implementation tentatively scheduled for March 2012). One of the goals of the upgrade is to focus on documentation of key business areas/processes. We want to provide sufficient documentation in areas where we feel documentation may not be where we would like it to be. Formalizing the security surrounding the eMARS checkwriter interface process would be a good example of the type of documentation we would like to develop as part of the upgrade.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-FAC-25: The Finance and Administration Cabinet Should Ensure All Reporting From infoAdvantage Is Accurate and Complete

As noted in the prior three audits, our fiscal year (FY) 2010 audit of the Finance and Administration Cabinet (Finance) revealed that infoAdvantage, the reporting solution used in conjunction with the Enhanced Management Administrative and Reporting System (eMARS) Advantage Financial application, could not be fully relied upon to provide the user with complete and accurate data. During the audit we found instances where reporting was not functioning as expected.

We identified instances where a data field related to a document was not available within the associated universe, but was required by the Document Control (DCTRL) table and available for use on the online version of the document.

- We noted that an active “Vendor” is required for the Solicitation Response (SR) and Solicitation Response Wizard (SRW) documents, and the “Commodity Line Description” field is required for the SR document, based on the DCTRL table; however there is not a “Vendor” code or “Commodity Line Description” field within the Solicitation Response class or linked to the document codes within the Procurement Awards Universe. These fields are available to be populated when the document is developed. When a user develops a report of SR and SRW documents from the infoAdvantage Procurement Awards universe including these fields, the values for the “Vendor” code and “Commodity Line Description” fields are coming from the Award Accounting Line. However, there is not a direct relationship between the Solicitation Response and the Award Accounting Line tables in the Procurement Awards universe. Therefore, the data values returned cannot be relied upon.
- We found that the “Cited Authority” field is required for the General Accounting Expense/Expenditure (GAX), Commodity Based Payment Requisition (PRC), and Commodity Based Internal Payment Requisition (PRCI) documents based on the DCTRL table; however the “Cited Authority” field is not available in the Accounting Journal class or linked to the document codes within the General Accounting Universe. The field, however, is available for use when the GAX, PRC, and PRCI documents are developed.

Additionally, we identified two instances where a data field related to a document is available within the anticipated universe, but the linking is not established to allow for reporting that will include the data field.

- We identified instances where the “Event Type” field is available, but not linked, to the Document Header within the Accounts Payable and Accounts Payable-Kentucky Universes. Without this linking to the “Event Type,” it is not possible for reporting to be developed to determine the appropriateness of coding for required and prohibited fields from the Event Requirements (ERQ) table on the Management Budget (OB1) or Check Writer Cancellation (CWC) documents.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-FAC-25: The Finance and Administration Cabinet Should Ensure All Reporting From infoAdvantage Is Accurate and Complete (Continued)

- We determined that it was not possible to create a report within infoAdvantage from the Procurement Awards Universe that would show all procurement awards associated with a specific federal program. Currently, a link does not exist between the Award Line information and Cost Accounting Chart of Accounts fields, which would allow this type of reporting.

The lack of a data dictionary in conjunction with the inability of a normal end-user to see the underlying database joins related to data elements increases the risk that a user will develop reports based on incorrect data elements, or inadvertently exclude data due to joins that the user is unaware of when developing the report.

For reports to be useful and valid for management decision-making purposes, the reporting solution used should be appropriately designed to allow users to view data and develop reports that are complete and accurate. A reporting solution must, therefore, be understandable by the end user in structure, content, and context. Further, the underlying structure of the data must be appropriate for the overall accounting regulations of the organization; otherwise, the solution may provide information that is not expected by the end user.

Recommendation

We recommend Finance continue work on the infoAdvantage reporting solution, in conjunction with the vendor, to ensure that all known reporting problems are corrected or properly addressed. Further, a review of the established joins within the universes should be performed to ensure they are functioning as intended for the Commonwealth of Kentucky.

To further assist end user reporting capabilities, Finance should develop a data dictionary that is available to all users. This data dictionary should include information concerning:

- The originating table location of the data element;
- A description of the data element;
- A description of all pertinent joins involving the data element; and,
- A listing of other data elements that the data element is dependent upon for reporting purposes.

FINANCIAL STATEMENT FINDINGS*Significant Deficiencies Relating to Internal Controls and/or Noncompliances***FINDING 10-FAC-25: The Finance and Administration Cabinet Should Ensure All Reporting From infoAdvantage Is Accurate and Complete (Continued)**

Management's Response and Corrective Action Plan

It is not feasible to create a "data dictionary" at this time. The eMARS team is currently reviewing the newest version of the Advantage software (Version 3.9) with the anticipation of going live March 2012. This version contains many Universe changes particularly within the Fixed Asset and Procurement areas. The team anticipates these updates will provide additional data elements that are not readily available today.

In addition, a new Kentucky specific universe is available. The KY-Contract Expenditure Summary Universe was made available in September 2010 to provide a summary of cash expenditures against all awards. This universe will provide expenditures against grants.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-26: The Kentucky Department Of Education Should Develop A Formal Disaster Recovery Plan And Formalize Backup Procedures

As noted within the past four audits of system controls for the Kentucky Department of Education (KDE), our FY 2010 audit found KDE had not developed or implemented a formalized Disaster Recovery Plan to address the backup and recovery of critical business servers, applications, and data in the case of a prolonged interruption. We are aware that a disaster recovery lead has been designated and a draft policy document related to the backup of information and data resources noted as critical has been developed. In addition, KDE is working to develop an Information Technology (IT) Disaster Recovery Plan; however, it is not expected to be completed until late December 2010.

An outside vendor has developed a Disaster Recovery Service for the MUNIS application. This service is available through the MUNIS contract and has currently been contracted by 28 districts, or 16.1 percent, of the 174 school districts. Because KDE does not have the authority over school district MUNIS servers to require participation, KDE encourages school district personnel to use this feature during training at the annual MUNIS User Conference, the Kentucky Association of School Business Officials (KASBO) conference, and the Kentucky Society for Technology in Education (KySTE) conference. Further, the Office of Education Technology (OET) has provided the Kentucky school districts with guidelines to assist with the backup of critical programs and data files.

To assist with the development of the IT Disaster Recovery Plan, KDE has purchased a planning system from a separate outside vendor. KDE began working with this vendor to start this project in March 2010. The anticipated completion date of this project is December 2010.

Further, KDE's Security Program Manager has drafted a data backup policy for critical systems and servers. All but one system requiring backup has been migrated to the Microsoft Data Protection Manager (DPM) backup system. An alternate backup solution is in place for the remaining system. KDE servers are reviewed regularly to determine whether it is necessary to backup the servers and new servers are added to the backup process as necessary. However, the KDE backup policy was not finalized during FY 2010.

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 Plans should be documented, approved, properly distributed, tested on a consistent basis, and updated as needed.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-26: The Kentucky Department Of Education Should Develop A Formal Disaster Recovery Plan And Formalize Backup Procedures (Continued)

Recommendation

We recommend KDE continue to work toward the development of a comprehensive Disaster Recovery Plan. This comprehensive plan should include an overall Disaster Recovery Plan for the cabinet, but also a specific plan for each of the KDE offices and departments. These individual plans should be reviewed and updated annually as necessary to reflect accurate information related to:

- emergency personnel contacts;
- potential alternative processing sites;
- system descriptions and process requirements;
- backup procedures;
- designation of on-site and off-site storage facilities;
- backup and retention schedules for electronic media;
- procedures to recover applications and data from backup media; and,
- planned testing procedures.

Once completed, the comprehensive plan should be distributed to key personnel. Training on the disaster recovery procedures should be provided to these key personnel. Further, annual testing should be performed to ensure that all necessary personnel are aware of their respective roles in the implementation of the plan.

We also recommend OET continue to encourage all Kentucky school districts to develop a Disaster Recovery Plan that, at a minimum, addresses the backup and recovery of their MUNIS server. A central level oversight authority or third party should review and approve all school district's contingency plans. OET should also continue to inform all school districts not currently using this service of the benefits of the Disaster Recovery Service for MUNIS.

Management's Response and Corrective Action Plan

As reported in past audit responses, KDE has various decentralized Disaster Recovery procedures for critical systems and services in place. With the hiring of a full-time Security Program Manager in 2008, KDE has focused on collecting this information in a centralized plan. KDE has a project underway to develop a documented plan that will ensure the continuity of operations and availability of critical resources and services in the event of a disaster. Initially, the KDE Enterprise Disaster Recovery Plan will include Crisis Management functions for business recovery. And, the bulk of the plan will address Recovery Functions for the enterprise IT services provided to the KDE Agency and K-12 School Districts. Before the project is completed, all necessary personnel will be notified of the location of the plan and the update process going forward. Once the project is completed, an on-going Disaster Recovery Program will include annual testing and other awareness activities.

School districts will continue to be informed of the Disaster Recovery services provided by the outside vendor for MUNIS (KDE's Financial Management system).

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-27: The Kentucky Department Of Education's Office Of Education Technology Should Expand And Consistently Apply Logical Security Policies For The KETS Network And MUNIS

As noted in our prior three audits of the Kentucky Department of Education (KDE) system controls, the Office of Education Technology (OET) has not formalized and implemented a security policy that identifies management and user responsibilities concerning security surrounding the Kentucky Education Technology System (KETS) network and MUNIS. Although KDE has developed an Acceptable Use Policy and Access Control Policy to address appropriate use of resources within KDE, these policies do not specifically address IT responsibilities associated with the KETS network and MUNIS.

OET management is responsible for central workstations and servers, as well as OET-related employee and contractor network access. Our audit revealed OET had not implemented a formalized security policy to control system access by these employees and contractors or access to OET-maintained servers by system users within other business units. Further, audit logging was enabled by OET for all UNIX and Windows-based servers; but, no security policy was formalized at the central level concerning procedures to periodically review the audit logs for users with high-level privileges.

All KDE users were granted Local Administrator rights on their workstations. This is considered unnecessary access for most KDE employees. 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.

In addition, an access request form was not developed for requesting and granting access to agency resources and applications. Currently, the OET Data Center Services team grants server access. The level of access is determined by the Division of Financial Data Management. Employees are required to sign Confidentiality Agreements upon hire. However, this form did not specifically identify the agency resources or applications to which the user requires access, did not list the level of access to be granted to the user, and was not required to be updated for changes in access. KDE intends to require access requests be processed through the KETS Service Desk in the future, although this is not currently a formalized procedure.

The school districts primarily use the MUNIS financial system to manage their 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 files to KDE, a transfer utility program transfers the file to a Gateway server maintained by OET, and then the files are transported daily to a File Transfer Protocol (FTP) server and temporarily stored for pickup by the Office of District Support Services (ODSS) staff. As MUNIS is a purchased system, specialized for Kentucky, select vendor staff also have access to the districts' MUNIS servers in the event that support is needed. Review of supporting documentation on file for a sample of five vendor staff with update access to district servers revealed none of the five users had a Confidentiality Agreement on file with KDE.

During FY 2010, five new user accounts were established on the Gateway server and three new user accounts were established on the FTP server.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KDE-27: The Kentucky Department Of Education's Office Of Education Technology Should Expand And Consistently Apply Logical Security Policies For The KETS Network And MUNIS (Continued)**

Based on our review, two of the new users on the Gateway server and one new user on the FTP server were considered testing exceptions due to the Confidentiality Agreement being signed at least seven months after access was granted. Further, one new user on the Gateway server for which we had requested supporting documentation, was determined by the agency to have left the employment of KDE; therefore, the access was deemed unnecessary and was revoked at that time. Information provided by the agency indicated this access was available for approximately 11 months after the employee's transfer.

Further, one new security group was established on the FTP server during FY 2010, but no supporting documentation for its creation was on file. Eight new users were added to groups on the Gateway server and five new users were added to groups on the FTP server; again there was no documentation supporting the access granted to these users. Additionally, we identified 11 disabled accounts on the Gateway server and 8 disabled accounts on the FTP server that remained members of one or more security groups on the respective servers.

Although no new Jefferson County school district employees had access to the servers reviewed for FY 2010, we determined KDE still does not request Confidentiality Agreements or other supporting documentation for Jefferson County employees. However, it was determined OET plans to establish an agreement with Jefferson County in the future to ensure all Jefferson County employees with MUNIS access agree to an appropriate level of confidentiality.

Although neither KDE nor OET had implemented a formal security policy related to specifically accessing MUNIS servers or software in the districts, an informal process was in place for KDE or OET staff to first obtain authorization from the school district before accessing the district's MUNIS server or software. A log was maintained at OET to track access to district servers by the root account. However, review of this log revealed that the activity being captured does not include the district server being accessed.

We are aware an overarching KDE Security Program exists including a Program Charter and Framework, governing technology policies, procedures, and initiatives. However, this group of documents was not finalized.

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. 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.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-27: The Kentucky Department Of Education's Office Of Education Technology Should Expand And Consistently Apply Logical Security Policies For The KETS Network And MUNIS (Continued)

System access should be limited to the level necessary for performing assigned duties, and system accounts should not be shared to ensure individual user activity could be tracked. Granting users system administration access to their computers increases the likelihood that unauthorized and unlicensed software could be installed and increases the chance of system attacks by viruses or other malware.

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 is not used within 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. Accounts that are not anticipated as being used in the future should be periodically purged. Finally, system user accounts and audit trails should be reviewed periodically in order to ensure identification and tracking of user activity.

Recommendation

We recommend OET standardize security responsibilities for all OET employees and ensure critical programs and data related to the KETS network and MUNIS, as well as the servers housing such data, are properly secured. The agency should, at a minimum:

- Formalize procedures related to the management of locked and disabled accounts on agency servers. These procedures should address the process of disabling or removing terminated employee accounts, as well as unnecessary generic accounts. Accordingly, a methodology should be developed so that a distinction can be made between accounts that can be safely removed versus accounts that must be retained on the server for performance reasons or audit trail history. These procedures should include the requirement for a periodic review of disabled and locked accounts to determine their necessity. If an account is deemed unnecessary, it should be permanently removed from the OET servers unless there is a pragmatic reason for maintaining the account, in which case it should be, at a minimum, disabled. All disabled accounts should be removed from current group membership on the OET servers.
- Evaluate all security group assignments on the OET servers to ensure that all assigned users require membership in the assigned groups. Implement procedures to periodically review security audit logs with special attention being given to users with high-level privileges so that inappropriate use of resources can be further investigated, if the need arises.
- Restrict Local Administrator rights to technical and support staff.
- Ensure all Confidentiality Agreements for sensitive information are completed, signed no later than the time access is granted, and retained by appropriate personnel.
- Finalize and implement plans to establish an agreement with Jefferson County to require a confidentiality agreement for all Jefferson County employees with access to OET servers.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-27: The Kentucky Department Of Education's Office Of Education Technology Should Expand And Consistently Apply Logical Security Policies For The KETS Network And MUNIS (Continued)

Recommendation (Continued)

- Develop and implement a user access request form. Users requesting access to KDE resources or applications should be required to complete this form. The completed forms should be approved by appropriate management and should be maintained in the user's file as supporting documentation for their access. Until an access request form is established, OET should continue to use KETS Service Desk tickets to establish or alter access. These tickets should be maintained for audit purposes.
- Ensure sufficient information is captured with the log used to track access to the district servers to allow the reviewer to determine the server on which the activity took place.

This comment is a result of our IT Audit fieldwork, which focused specifically on logical security policies governing MUNIS and the KETS Network. The same type of review was performed on specific critical applications for which the ODSS is responsible, which also resulted in a comment governing ODSS logical security policies, see 10-KDE-30. KDE should determine whether similar weaknesses exist in relation to other agency-identified critical applications. If so, then we recommend KDE ensure either a centralized or an individual security policy be developed and implemented to cover all critical applications owned by KDE.

Management's Response and Corrective Action Plan

- *KDE disagrees with the assessment that the Office of Knowledge, Information and Data Services (formerly OET) has not formalized and implemented a security policy that identifies management and user responsibilities surrounding the KETS and MUNIS and that the Acceptable Use Policy and Access Control Policies do not specifically address IT responsibilities. KDE has established an IT Security Program to introduce security control policies and processes and has a Security Program Manager. IT Security policies are being put forth and adopted for all of KDE. The existing policies broadly address management and user responsibilities and more work will come to further define the processes and procedures to support these policies as well as others.*
- *Due to the large number of services authenticated through Active Directory, KDE has started a formal process to review and remove accounts that have not been recently accessed. KDE plans to formalize additional processes to review enterprise accounts and sensitive servers administrated by KDE business owners thereby increasing current security controls.*
- *KDE plans to develop a process to review the security group assignments of sensitive servers. Currently KDE has limited resources, staff, and tools to regularly review security logs in an effective and efficient manner. Logs are retained short-term for review once an incident/issue is identified.*
- *KDE continues to investigate current methods available to reduce the number of KDE workstations with Local Administrator rights.*

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances***

FINDING 10-KDE-27: The Kentucky Department Of Education's Office Of Education Technology Should Expand And Consistently Apply Logical Security Policies For The KETS Network And MUNIS (Continued)

Management's Response and Corrective Action Plan (Continued)

- *KDE will improve the management of Confidentiality Agreements for sensitive information including Jefferson County agreements.*
- *KDE will introduce a common User Access Request process that will be used by all offices to administrate and track access to KDE Enterprise applications and other critical systems.*
- *KDE will investigate new methods to capture the district MUNIS server identification within the District server access log.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-28: The Kentucky Department Of Education's Office Of Education Technology Should Consistently Apply Program Modification Procedures

As noted during the prior four audits of the Kentucky Department of Education (KDE) system controls, the program modification process developed by the Office of Education Technology (OET) is not sufficient to ensure only authorized changes to the IT environment, which includes the Municipal Information System (MUNIS), are made.

OET developed and implemented a formalized Change Management Policy and Procedures Manual. This manual stipulates changes made to the IT environment must be documented on a properly completed and approved Request for Change (RFC) form. However, the manual does not specify the individuals responsible for performing testing of a proposed change or migration of a change to production. The current informal process has members of the MUNIS Support Team and one Tyler Corporation employee responsible for testing MUNIS-related changes. On the approval of the Project Manager, MUNIS-related changes are moved into production by a member of the MUNIS Support Team. This informal process could lead to a segregation of duties issue between the request for change, development of the change, testing of the change, and promotion to production. It could also lead to a failure to complete any one of these tasks.

Over the past four years, we have recommended the implementation of digital signatures on the RFC forms. However, due to budgetary constraints, OET does not anticipate moving to this technology. Since the RFC forms are submitted and approved electronically through a simple process of typing an individual's name in the approver's field, there is not sufficient information maintained within the documentation to determine who provided an approval for a change. Furthermore, OET had not developed a listing of authorized Requesters/Owners who can request a change to the IT environment. These two features should be developed and used in conjunction to ensure only authorized requests are processed.

Further, changes to the KDE utilities are not consistently tracked through the OET change management process. Our review of five KDE utilities revealed there were 284 lines of code changed that affect processing within the source codes of two of these utility programs; however, these changes were not individually logged within the tracking spreadsheet. Therefore, we could not determine, based on the documentation provided, that approval was granted for each line changed within the code.

Also, testing of the Forward Schedule of Change (FSC) worksheet revealed four of the completed changes did not have actual start times and completion times properly documented. Finally, an examination of nine Request For Change (RFC) forms related to changes to the MUNIS system since our prior year review revealed one RFC form was not properly filled out to reflect the completion date. Another RFC form tested was not properly filled out to reflect personnel performing the testing, date of testing, and results of testing.

Failure to properly apply and monitor change control procedures increases the risk that incorrect or unauthorized changes could be made to critical applications and, potentially, be moved into the live production environment.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-28: The Kentucky Department Of Education's Office Of Education Technology Should Consistently Apply Program Modification Procedures (Continued)

Program modification control procedures should be consistently applied in order to ensure that only appropriately authorized changes to critical applications are made and implemented within the production environment. All program modifications are to be requested on a Request for Change form. They should 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. Changes to OET utilities should also be included in the change management process.

Recommendation

We recommend an expansion of the OET Change Management Policy and Procedure manual to identify specific individuals or groups responsible for performing changes, testing changes, authorizing promotion of changes, and moving changes into production. All change management controls should be consistently applied to critical system software and utility programs. This process should be attributed to changes for both the IT environment and the OET utilities.

All changes should be requested and approved using the RFC form. Individuals responsible for approving the RFC form either should be required to print, sign, and date the RFC form or provide email correspondence indicating approval which can be linked to the RFC form in order to validate approvals and avoid segregation of duties issues. Further, in the event a major change is made to utility codes, OET should perform a comparison of the old and new versions of the utility code to determine which lines specifically were changed. RFC forms as well as other supporting documentation should be maintained for audit purposes. Also, each time a change is made to the utility source code; it should be documented in the 'Revision' section of the coding.

Management's Response and Corrective Action Plan

KDE will review the KDE/KIDS Change Management documentation and add the following improvements:

- *Identify groups responsible for performing, testing, and approving changes for critical system software and utility programs.*
- *Identify major changes to utility code for critical systems in the Revision section of the code.*
- *Review and improve the monitoring and approval procedure for the Request for Change form and Forward Schedule of Changes documents.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-29: The Kentucky Department Of Education Should Ensure All Agency Machines Are Properly Configured To Include Only Necessary Services

As noted in the previous audit, our FY 2010 security vulnerability assessment on machines owned by the Kentucky Department of Education (KDE) revealed 56 of 70 scanned central level machines, or approximately 80.0 percent, could potentially be mis-configured. A mis-configured machine could waste resource, entice an attack using ports that are unnecessarily open, have default services running, or allow excessive hypertext transfer protocol (HTTP) methods. The ports open on each of these machines should be reviewed to ensure they have a specific business purpose and that the services are properly authorized. Nine of the machines contained open ports addressed with the agency during the previous audit. Of the 50 potentially mis-configured machines, four machines reported the potential use of a remote shell suite of programs.

For security purposes, detailed information that would identify the specific machines contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

System misconfigurations that allow unnecessary services can negate other security configurations established on the machine, increase potential security vulnerabilities, and provide enticements for intruders to enter the system. Specific to web servers, excessive HTTP methods provide additional avenues for system intrusion. The use of unsecured transmission programs also increases the risk of compromised data transmissions.

To assist in securing a network adequately, it is necessary to ensure all machines and web services are configured to only allow necessary services to operate. Only necessary business-related ports should be open. Default services should be disabled. Only the necessary HTTP methods (such as POST, HEAD, and GET) should be supported on agency web servers.

Recommendation

We recommend KDE take the necessary actions to ensure the noted services on each machine have a specific business purpose and are properly authorized. If the service is necessary, it should be reviewed to ensure it is properly authorized, licensed, and configured as well as adequately secured. Default services should be disabled or removed from all servers. Any unnecessary services should be disabled or the associated ports should be closed. HTTP methods not required for the operation and maintenance of a web server should be disabled. If the remote shell suite of programs is being utilized, it should be replaced by a more secured shell suite.

Management's Response and Corrective Action Plan

KDE will review all KDE managed servers noted and take action to address. We will remove unnecessary and default services where possible. Rtools are used on the UNIX environment supporting the MUNIS application. The UNIX hardware is dated and limits the ability to upgrade support tools. KDE is currently evaluating options to migrate the MUNIS application to another platform where Rtools would no longer be used. KDE will continue to revise the Security Best Practice documentation for districts and encourage them to resolve configuration and vulnerability problems identified in these or other scanning processes.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-30: The Kentucky Department Of Education's Office Of District Support Services Should Expand And Consistently Apply Its Logical Security Policies

As noted during the prior four audits, we determined through the review of the Kentucky Department of Education (KDE) controls the Office of District Support Services (ODSS) did not properly secure the critical financial data associated with the Support Education Excellence in Kentucky (SEEK) II program. This is the fifth consecutive year we have commented on similar weaknesses, although we did note some improvement since FY 2009. The logical security issues identified during our audit are presented below.

ODSS implemented the new SEEK II application on July 1, 2008. SEEK II allows for better control of user access through the assignment of individual user accounts and associated security roles. In addition, the SEEK II production and development servers were segregated with assigned server administrators having oversight responsibilities on each server. ODSS had also created a SEEK II User Manual, which documents vague logical security procedures surrounding SEEK II. Discussions with KDE staff revealed the manual has been finalized; however, the word 'DRAFT' is still noted on the front of the document. Also, the procedures still lack management and user responsibilities concerning Information Technology (IT) security surrounding the SEEK II program. Further, SEEK II password policies were not documented in the SEEK II User Manual to ensure user understanding and compliance.

Also, an ODSS Systems Access Request Form was developed on January 31, 2010 to assist in documenting user requests to ODSS-maintained systems, including SEEK II. However, no instructions were developed on how to complete the form or explanations of the levels of access available for the individual systems. Formal procedures were not developed related to the ODSS-maintained systems nor were application specific procedures incorporated into the SEEK II User Manual. A review of the SEEK II User Manual identified some information related to logical security; however, this information was scattered within the Manual and specific details related to user access levels available within the application were not discussed.

During FY 2010, we identified eleven new users with access to the SEEK II application. Seven of these users, or approximately 63.6 percent, had no documentation supporting their request for access. These requests were made verbally and were created prior to the implementation of the ODSS Systems Access Request Form.

We also identified one operating system group on the development server with an enticing name and unknown function. This group had Full Control rights on the development server. ODSS staff indicated the group was created by default at installation and was not actively used. During the prior year audit, this group was also noted on the production server, but was removed.

While auditing the logical security controls surrounding SEEK II, we discovered segregation of duties issues where two SEEK server administrators and a developer had excessive access to both production and development.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-30: The Kentucky Department Of Education's Office Of District Support Services Should Expand And Consistently Apply Its Logical Security Policies (Continued)

Without strong and formalized logical security controls, the opportunity increases for unauthorized modification of production files as well as the likelihood of errors or losses occurring from incorrect use of data and other resources. Without sufficiently strong password criteria and allowing excessive access rights to groups increases the risk of system exploration by unauthorized users.

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, and unnecessary accounts and groups should be removed. Unless a formal agency policy is in place that is more restrictive stating otherwise, agency passwords should conform to the Commonwealth Office of Technology (COT) standards as stipulated in the CIO-072 UserID/Password Policy. Of particular note, passwords should be a minimum of eight characters in length, should contain at least one special character, and should be changed at least every 31 days.

Recommendation

We recommend ODSS formalize the SEEK II User's Manual by removing the word 'DRAFT' on the front page. ODSS should incorporate a 'Revision History' section within the manual to capture future changes made. This history should show a brief description of what change was made, by whom, and when. ODSS should document the password policies for the SEEK II application and peripherals within the SEEK II User Manual. Specifically, password policies should be documented for the SEEK II application, the production database, the production web server, and the development server. The SEEK II User's Manual should also be expanded to include management and user responsibilities concerning IT security surrounding the SEEK II program.

We recommend ODSS develop general user request procedures requiring the use of the ODSS Systems Access Request Form. ODSS should expand the ODSS Systems Access Request form to include instructions on how to complete the form and explanations of the levels of access available for the individual ODSS-maintained systems.

Finally, the group on the development server identified with an enticing name should be disabled if there is no business purpose for its operation. If this is not feasible, ODSS should reduce the group's rights on the development server to Read Only.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-30: The Kentucky Department Of Education's Office Of District Support Services Should Expand And Consistently Apply Its Logical Security Policies (Continued)

Management's Response and Corrective Action Plan

Management has reviewed the recommendations and has identified the necessary correction plans for each identified issue. Here are the individual responses:

- *As indicated in the May 12th response, the word 'DRAFT' was an oversight when originally sent for review and was removed at that time.*
- *A revision history block was added to the manual as follows:*

<i>Date of Issue</i>	<i>Author(s)</i>	<i>Brief Description of Revision</i>
<i>8/16/2010</i>	<i>Tim Cooper</i>	<i>In response to Auditor comments added the following: additional security language, list of available roles, user request form step for new users, password requirements, and revision history block for the document.</i>

- *The following verbiage has been added to the manual to specifically document the password polices for the application, the databases and the servers. The password requirements for the application are as follows: minimum 5 characters in length, at least one numeric character, at least one upper-case character and does not expire. The same password requirements exist for the databases. The password requirements for the servers themselves follow AD requirements as defined by KDE OET, but a user of the SEEK II system does not need a login to either the servers or databases.*
- *The SEEK manual already indicated the basic user responsibilities concerning IT security and their individual responsibilities. For example the manual includes the following:*

Your password is confidential and should be known only by you. If someone else knows your password, they can make changes to very sensitive data and those changes, no matter how big or small will be attributed to you. Again, your password is confidential and should be known only by you.

Once each new user has been created and assigned rights, the system will handle the enforcement of user rights via the user ID used to log in to the system. For this reason, it is very important for SEEK users to never trade login IDs and/or passwords. It is also important that users refrain from leaving unattended, a workstation upon which they are logged in to the SEEK II system.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KDE-30: The Kentucky Department Of Education's Office Of District Support Services Should Expand And Consistently Apply Its Logical Security Policies (Continued)****Management's Response and Corrective Action Plan (Continued)**

To reinforce the responsibilities associated with utilizing the system, the following text was added to the manual to identify the user's security responsibilities that are applicable to the use of all KDE systems including SEEK II:

Users and management must understand that use of the system falls under KDE policies such as Acceptable Use Policy and Access Control Policy.

- *The ODSS Access Request form now has instructions for completing the form.*
- *The identified group on the development server that was thought to have an 'enticing name' has been removed.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-31: The Division Of Nutrition And Health Services Should Develop, Implement, And Consistently Apply A Formal Logical Security Policy

As noted during our previous audit, our FY 2010 audit of system controls determined the Kentucky Department of Education's (KDE) Division of Nutrition and Health Services (DNHS) had not developed or implemented formal logical security control policies and procedures concerning the Nutrition and Health Services Payment (NHSP) Application. Further, review of user accounts within the application revealed multiple accounts for active users and accounts associated with users no longer employed by DNHS.

In order to grant access to the NHSP Application, a completed Network/Server Access Request Form (COT-F-181) is sent to the Commonwealth Office of Technology (COT) requesting a user be established with access to the State's mainframe. Once mainframe access is granted by COT, security personnel at DNHS establish user access within the NHSP application. Currently, no formal procedure exists to regulate the request for user access, approval of the access requested, and the access level assigned to a user within the NHSP application, or removal of access when job duties change or an employee leaves DNHS. Discussions with DNHS staff revealed that the process of documenting system access processes was begun during FY 2010; however, a formal policy was not completed by the end of audit fieldwork.

Our review of the security table related to sponsorship access revealed the existence of six user Ids being explicitly associated with the previous Program Coordinator, who retired in July 2008. Additionally, four previous DNHS users continued to have access to the NHSP application during FY 2010. After identifying these 10 Ids, DNHS security staff deleted them from the system.

Testing of those accounts with transactional access within the NHSP application revealed 85 out of 1,405 unique users, or 6.0 percent, had one or more user Ids with specific access to the system, which were determined to be inappropriate. There were 121 unique user Ids associated with these 85 users. Issues noted with these accounts include:

- 19 user ids where a data entry error was made when establishing the user Id. These type errors were corrected by deleting the invalid user IDs from the system.
- 66 user Ids were no longer needed. These were due to a sponsor leaving the program. The associated user Id is deactivated (as opposed to being deleted) in the event that they return.
- 34 user Ids were identified as having more than one valid user Id, but there was no additional explanation provided to validate the necessity of multiple accounts.
- 2 user Ids are related to one user in order to complete testing associated with the system.

As previously noted, there were six user Ids associated with the previous Program Coordinator. These accounts continued to have level '7' access, or full access to sponsor claims. As recently as March 2010, all six user Ids associated with the previous Program Coordinator had access to sponsor data. Documentation was provided during the previous audit indicating the removal of these accounts was completed on November 5, 2009. However, review of the original security table for FY 2010 indicated that these user Ids either were not deleted or were subsequently reinstated. DNHS staff subsequently provided an updated Security table to document that the user Ids in question were deleted.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-31: The Division Of Nutrition And Health Services Should Develop, Implement, And Consistently Apply A Formal Logical Security Policy (Continued)

Furthermore, three DNHS staff members that have access to the NHSP application were not listed on the current NHS staff listing to show what security level was granted to them within the system.

Finally, review of the security table revealed one individual whose access level to the NHSP application was inappropriate based on current job duties. When brought to the attention of DNHS, this account was removed.

Failure to adequately document, implement, and communicate acceptable computer security policies and procedures could lead to a lack of understanding by management and users, thereby heightening the risk of noncompliance with security policies, failure to perform assigned security responsibilities, or inappropriate and inefficient use of system resources. This increases the likelihood of unauthorized or inaccurate data modification, destruction of assets, interruption of services, or inappropriate or illegal use of system resources.

Formal security policies set the tone of management commitment for strong system security and provide a security framework used to educate management and users of their responsibilities. Specific policies should be established related to system access controls to help ensure only authorized users are granted access to the application. These policies should include procedures for requesting new system access, changes to existing system access, and termination of system access. Management authorization of access requests should be documented. All supporting documentation should be maintained for management and audit review. Additionally, system users should be made aware of their responsibilities concerning data confidentiality, as well as appropriate and efficient usage of system resources. Consistent application of formalized security policy and procedures provides continuity for implementation and sets the tone of management concern for strong system controls.

Recommendation

We recommend DNHS develop and implement formal policies and procedures to administer the logical security over the NHSP application and ensure those procedures are consistently applied. Security access requests and applicable authorizations should be properly documented and maintained for all system users. DNHS should ensure all access requests contain adequate information necessary to grant approval to system resources and that appropriate approvals are applied. This policy should also address procedures to follow when employees are terminated or leave employment to ensure access is disabled appropriately and in a timely fashion. These policies and procedures, once developed, should be properly distributed and all system users made aware of their responsibilities concerning system access.

Further, we recommend DNHS perform a periodic review of all user accounts with access to the NHSP application to ensure users are current employees and associated access levels are appropriate based on job duties.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KDE-31: The Division Of Nutrition And Health Services Should Develop, Implement, And Consistently Apply A Formal Logical Security Policy (Continued)**

Management's Response and Corrective Action Plan

NHS concurs with these findings and will implement a more rigorous set of procedures to monitor and control system access. A new NHS assistant director will act as the security officer for NHS. All requests for access to the NHSP system will be routed through the assistant director, who will then review and approve access. Formal procedures regarding security policies will be developed and disseminated with NHS/COT personnel. The procedures will contain steps to ensure only valid users are given access, the appropriate security level will be assigned and steps will be formulated for monitoring. A separation checklist has been enacted that contains a section on terminating user accounts for departing staff. To verify system integrity, a periodic audit will be completed on user accounts. The list of active user accounts will be compared to all active sponsors and NHS staff to confirm the list of active user accounts is correct.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KDE-32: The Division Of Nutrition And Health Services Should Ensure Proper Segregation Of Duties**

As noted during our prior year audit, our FY 2010 audit of the Kentucky Department of Education's (KDE) Division of Nutrition and Health Services' (DNHS) Nutrition and Health Services Payment (NHSP) Application revealed DNHS did not employ proper segregation of duties between the system administration and processing functions.

Currently, it appears that security levels available within the application will not allow sufficient segregation of duties. DNHS made the necessary changes to staff roles and responsibilities to promote greater segregation of duties within the NHSP application. However, the Commonwealth Office of Technology (COT), which developed and currently maintains the application, has not made the necessary configuration changes to update the security levels in order to implement the newly designed roles.

Testing revealed there are differences between the available security access levels, the documented access rights for central level staff, and the actual rights provided to users. Specifically, two DNHS IT staff members, although identified for other access levels, were provided with full administrative control over the security as well as the ability to process data through the system. Also, two DNHS administrative staff members had access levels to the application which do not correlated to the documented levels to be provided to these users. Given the fact that the system does not retain historical data and no formal review process is in place, elevated or inappropriate levels of access could potentially allow controls to be circumvented.

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.

Employees that process payments should not be allowed to input or approve a claim on the system. Smaller organizations that cannot easily segregate duties should implement compensatory controls to supervise and monitor system activities to ensure erroneous claims are not processed.

Recommendation

We recommend DNHS continue to work with COT to ensure the newly developed security levels and associated roles promote adequate separation of duties within the NHSP application and are appropriately implemented within the current NHSP application. Once implemented, DNHS should perform a review of access rights granted to all central level staff to ensure access rights are appropriate and reasonable given their individual job functions. These new security levels and roles should also be taken into consideration when designing the security of the new NHSP application currently under development.

Further, we recommend DNHS develop a formal review process to ensure all claims submitted and approved within the current application are appropriate.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KDE-32: The Division Of Nutrition And Health Services Should Ensure Proper Segregation Of Duties (Continued)**

Management's Response and Corrective Action Plan

The security levels are in the development phase by COT. Rigorous testing will be performed by NHS in the test environment before these are released into production. NHS will reassign the appropriate security level to all staff members based on their current job duties. Security level assignment will be restricted to key management staff: NHS director, assistant director and the project manager. Security levels will be reviewed and potentially revised with the new system to meet the current security needs of NHS. This will be included within the RFP as a system requirement for the new system.

Regarding the quality control on claims payment, NHS will review this with COT to develop the best possible approach. Once a process has been developed a monthly review of claims will be conducted and documented to ensure the system is functioning properly.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-33: The Division Of Nutrition And Health Services Should Develop Formal System Documentation To Support Processing Performed By The Nutrition And Health Services Payment Application

As noted during our prior year audit, the Kentucky Department of Education's (KDE) Division of Nutrition and Health Services (DNHS) did not maintain current, basic documentation describing the processing performed by the Nutrition and Health Services Payment (NHSP) Application.

The NHSP application, which was developed by and is currently maintained by the Commonwealth Office of Technology (COT), went into production in 1982. Updates and expansions of services were made to the application over the last 28 years, most recently in February 2010. Discussion with COT personnel during the FY 2009 audit revealed no technical manuals existed documenting the design or functionality of the system. They did indicate a series of binders had been maintained containing notes documenting how to perform different tasks within the application; however, many of the notes were identified as being outdated or obsolete.

During FY 2010, DNHS staff produced a Nutrition and Health Services (NHS) Technology Manual. Although the manual was not dated with the most recent revision date, review of this manual determined the manual was several years out of date. Specifically,

- several key personnel referenced within the manual no longer work for DNHS;
- COT policies included in the manual are outdated; and,
- references are made to the Management Administrative Reporting System (MARS), the Commonwealth's statewide accounting system which was superseded in July 2006.

Further, during the planning phase of the FY 2010 audit, DNHS staff produced a copy of the CESN User Setup document, which provides a security administrator with the steps necessary to grant Customer Information Control System (CICS) access to a user. A review of additional documentation obtained during fieldwork related to the security levels available within the application do not consistently match the levels identified within this User Setup document.

We are aware DNHS had plans to hire a business analyst to formulate clear, comprehensive, and well-organized business rules of the existing system. This documentation will be used as part of the development process for a new NHSP application.

Lack of documentation increases the likelihood of erroneous or incomplete processing. It further increases the likelihood of unauthorized data modification, destruction of assets, and interruption of services.

Proper documentation should be maintained for each critical program in production in order to, at a minimum, identify the purpose of the programs, the origin of data, the specific calculations or other procedures performed, and the output of data or reports.

FINANCIAL STATEMENT FINDINGS*Significant Deficiencies Relating to Internal Controls and/or Noncompliances***FINDING 10-KDE-33: The Division Of Nutrition And Health Services Should Develop Formal System Documentation To Support Processing Performed By The Nutrition And Health Services Payment Application (Continued)**

Recommendation

We recommend DNHS work with COT to develop documentation that provides an understanding of critical programs or jobs currently running in production. All available guides or user documentation should be updated to reflect current policies or formally superseded with more up to date documentation. The documentation could include a network diagram; user and operational manuals; and flowcharts, diagrams, or descriptive narratives of functional areas. Information normally collected in design documents includes a technical description of the program, sources and location of files used by the program, and the processing steps for main functions. This documentation should be used during the planning of the new NHSP application for cross-walking procedures from the old to the new system.

Management's Response and Corrective Action Plan

NHS concurs with the findings regarding inadequate, incomplete and outdated documentation in regards to the current NHSP application. NHS documentation will be either developed or revised to reflect the current NHSP application status. COT will be enlisted to assist in this project. The new business analyst will assist in this effort to update the current system documentation. For the new system, procurement efforts are focused on a commercial off the shelf (COTS) application. As such, it is expected to be USDA compliant in all program areas with customization for Kentucky's own specific needs. The historical claims and application/agreement data is expected to be migrated over from the current system. Documenting the current system will assist us with developing the business requirements as well as with the migration effort.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KDE-34: The Division Of Nutrition And Health Services Should Enable System Auditing On Its Nutrition And Health Services Payment System

As noted during our prior year audit concerning application security over the Kentucky Department of Education's (KDE) Division of Nutrition and Health Services' (DNHS) Nutrition and Health Services Payment (NHSP) Application, our FY 2010 audit revealed historical transactions, including those related to security, are not logged or tracked within the system. The United States Department of Agriculture (USDA) Southeast Regional Office (SERO) of Food and Nutrition Service (FNS) had a finding related to this issue since FY 2007.

The NHSP application, which was developed and currently maintained by the Commonwealth Office of Technology (COT), retained the date of the last update to claims and approvals, as well as the user Id of the person that made the update. However, it did not identify what information was changed. Further, the system did not retain a historic version of transactions.

Additionally, users with an access level of '1' are given full control over claims, sponsor and organization screens, applications, agreements, approvals, system access, and bank balances within the application. Since the system did not maintain a history of changes to security levels, it was not possible for the system administrator or management to review changes to a user's security level within the system. DNHS had worked during FY 2010 to alter the staff's security roles and job tasks associated with each security level to improve segregation of duties; however, COT had not made the necessary system changes to accommodate these improvements.

DNHS did not believe it is feasible to enable security auditing on the current NHSP application since a new system is currently being developed.

Failure to adequately monitor security events and transaction logs could result in failure to identify suspicious activities that may be occurring on the system.

Without effective monitoring of event and security logs, the risk of inappropriate transactions being processed by the system increases. A logging and monitoring function within an application and consistent review of the results enables early detection of unusual or abnormal activities.

Recommendation

We recommend DNHS work in conjunction with COT to ensure the proposed security level changes within the NHSP application are incorporated to improve segregation of duties and, thereby, system security. DNHS should implement compensating controls to ensure only appropriate transactions are processed within the NHSP application. An appropriate level of management should perform regular reviews of the data maintained by the NHSP application. This review should be documented for audit purposes.

Further, we recommend DNHS ensure audit logging is a requirement for the new system. Once the new system is implemented, DNHS management should review the event and history logs on a regular basis. Identified security violations should be thoroughly documented to ensure they are resolved in a timely manner. This review should be documented for audit purposes.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KDE-34: The Division Of Nutrition And Health Services Should Enable System Auditing On Its Nutrition And Health Services Payment System (Continued)**

Management's Response and Corrective Action Plan

NHS is collaborating with COT to implement security levels that will ensure a greater segregation of job duties and allow for more defined control on system access. These new security levels have been assigned to COT and are in the development phase. NHS will request assistance from COT in developing mechanisms to review transactions for aberrant activity. Once this is implemented, a regular review will be initiated and the results documented.

The future system will have role based security and is expected to have higher granularity in allowing access to the system than what is currently available. Event and history logs maintained by the system will allow NHS to closely monitor transactions. Periodic reviews will be undertaken for compliance with the security procedures.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KHP-35: The Kentucky Horse Park Should Enforce Controls Regarding Payroll Records And Segregate Duties For Payroll And Personnel Activities

The Kentucky Horse Park (KHP) employs full time and interim employees throughout the year. Approximately 200 employees worked at the KHP in FY 10. The employees complete a Time and Attendance (T&A) Report and the supervisor transfers the time from the T&A report onto a timesheet. The employee is required to sign the T&A report and the supervisor should sign both the T&A report and the timesheet; however, according to the Human Resource (HR) Manager, the time keeping is acceptable as long as one document is signed by the employee and supervisor. The HR Manager acts as the timekeeper and inputs the time into the state's payroll system, Unified Personnel and Payroll System (UPPS). UPPS generates a 1017 Report and the HR Manager compares the report to the timesheet and checks for errors.

During the FY 10 payroll audit, we requested 40 employees T&A Report and timesheets for various pay periods. Out of the 40 employees tested, we noted the following exceptions related to 11 employees:

- Ten instances in which the supervisor did not sign either the Time and Attendance (T&A) Report or the timesheet;
- One instance in which the employee did not sign either the T&A Report or the timesheet;
- One error in which the employee was not paid correctly according to the T&A Report, the timesheet, and the 1017 UPPS Report; and
- Forty instances in which the timekeeper did not sign the timesheets.

The internal controls over the payroll process were also reviewed. The prior year audit identified a significant deficiency in that the entire payroll process was completed by one person, the HR Manager. This deficiency continued to exist in FY 10. Specifically, the HR Manager is responsible for:

- Hiring new employees
- Sending employee information to the Personnel Cabinet
- Entering employee information in the UPPS
- Collecting timesheets from KHP employees
- Entering timesheet information in UPPS
- Reconciling timesheet information to the 1017 UPPS Report
- Receiving, sorting, and delivering payroll checks and check stubs to KHP employees
- Terminating employees
- Processing supplemental payrolls

This combination of these duties is incompatible, and, as a result, the errors identified above have gone undetected.

The KHP personnel are required to complete both a T&A report and timesheet. This is a duplication of effort since the supervisor re-enters the information on the T&A report (completed by employees) on timesheets (sent to KHP Personnel for entry into UPPS). Maintaining two separate timekeeping documents increases a risk of errors, especially if the personnel are not required to review and sign both documents.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KHP-35: The Kentucky Horse Park Should Enforce Controls Regarding Payroll Records And Segregate Duties For Payroll And Personnel Activities (Continued)

When an employee does not sign a T&A Report and/or timesheet they are not certifying that the reported time is accurate and complete. When the supervisor does not sign the T&A Report and/or timesheet they are not verifying that the time documented is accurate. If the regular timekeeper was absent and someone else entered time into UPPS, there is no way to determine who entered the time for each pay period without the timekeeper signing the timesheet.

As stated in the prior year, given the responsibilities of the HR Manager, the lack of segregated duties related to hiring, entering personnel information in UPPS, entering timesheet data in UPPS, reconciling timesheet data, processing supplemental payrolls, and receiving and distributing payroll checks increases the risk of intentional or unintentional errors. Under these circumstances, errors or fraud cannot be detected in the ordinary course of business. Subsequently, errors did occur in FY 10.

KHP did implement a few controls during FY 10, including assigning another individual to receive and deliver the payroll checks and check stubs to the KHP employees with management oversight for one pay period. Also, another employee did receive a UPPS report for a time period and validated the employees hired. No discrepancies were noted in either effort. Unfortunately, these efforts did not prevent the errors that did take place.

Proper internal controls dictate that one individual should not have authority to hire, enter the new employee information in UPPS, enter timesheet data, reconcile the same timesheet data, process supplemental payrolls, and receive and distribute checks.

Employing strong segregation of duty controls over payroll functions decreases the opportunity for unauthorized modification to transactions and files and decreases the likelihood of errors or losses occurring because of incorrect use of data.

Proper internal controls dictate the payroll records are accurate, properly authorized, and completed. Also, proper reconciliation of the time inputted into the UPPS system should be in place. This should be performed by a separate individual that inputs the employees time.

Recommendation

We recommend the KHP:

- Consider updating the payroll time and attendance procedures to reduce or eliminate the duplication of effort as a way to reduce potential errors caused by the re-entry of the same data.
- Develop and implement a consistent policy regarding who is to sign time and attendance forms, including timesheets. Extra signature lines should be removed from documents the employee/supervisor is not required to sign to avoid confusion and inconsistencies.
- Require the timekeeper initial or sign the timesheet form when time is entered into UPPS.
- Consider hiring additional personnel or reorganizing the job functions of existing employees to assist with the proper segregation of duties.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KHP-35: The Kentucky Horse Park Should Enforce Controls Regarding Payroll Records And Segregate Duties For Payroll And Personnel Activities (Continued)**

Management's Response and Corrective Action Plan

Auditor's recommendation: Consider updating the payroll time and attendance procedures to reduce or eliminate the duplication of effort as a way to reduce potential errors caused by the re-entry of the same data.

Management's response: The Time and Attendance (T&A) report is an essential managerial tool that records an employee's beginning and ending work day as well as records reasons an employee worked over or short their allotted time. There is not a place to record this information on the time sheet which is required to input data into the UPPS system. Although it might seem that there is a duplication of effort, the purpose of the two documents is different. An automated time keeping system would help eliminate potential errors that may occur when the summary data is taken from the T&A report and input into the time sheet. This purchase request has been discussed and may become part of a future budget. The new time system would have to be compatible with KHRIS.

Auditor's recommendation: Develop and implement a consistent policy regarding who is to sign time and attendance forms, including timesheets. Extra signature lines should be removed from documents the employee/supervisor is not required to sign to avoid confusion and inconsistencies.

Management's response: It is management's intent to implement a policy that requires the signature of the employee on the T&A report and supervisors are to sign both the T&A forms and timesheets.

Auditor's recommendation: Require the timekeeper initial or sign the timesheet form when time is entered into UPPS.

Management's response: It is management's intent to implement a policy that the person who enters the time will be required to initial as the timekeeper.

Auditor's recommendation: Consider hiring additional personnel or reorganizing the job functions of existing employees to assist with the proper segregation of duties.

Management's response: The KHP management has considered hiring an employee to help alleviate the substantial workload in both the personnel office and business office. At this time the budget is not available for this position. When possible, an interim employee will be instructed to provide assistance in the personnel office to help provide a segregation of duties as well as a check on proper procedure management. In addition, the business office will continue to test the controls in the personnel office. This, along with the regular assistance provided by the Executive Administrator, will improve the oversight within the personnel office.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KHP-36: The Kentucky Horse Park Should Ensure Invoices Are Paid Timely**

During testing of the Kentucky Horse Park's (KHP) FY 10 expenditure payment process, we requested a sample of 37 invoices to verify the propriety of the expenditures and accuracy of amounts posted to the eMARS accounting system. The results indicated 16 instances in which invoices were not paid in a timely manner. In addition, five test sample items related to object code E370, *Late Payment Interest-1099 Report*. Pursuant to Kentucky statutes, a 1% late fee may be applied when invoices are not paid by a state agency within thirty (30) working days. The 1% late fee was appropriately included in the total payment to the vendor for these five items. According to eMARS, the total paid in late fees during FY 10 was \$2,595.

Late payments have been a repeat issue with the Kentucky Horse Park since FY 07.

We noted several variables that possibly contributed to the late payment of invoices. The KHP business office personnel do not always receive invoices from the various departments within the park upon receipt, which impairs the timely payment of invoices.

Failure to make payments in a timely manner causes an unnecessary loss in KHP resources, primarily through the payment of late fees. This also could negatively impact the established vendor customer relationship, which in turn could affect future business transactions. Furthermore, the failure to input expenditures into the eMARS accounting system in a timely manner could result in inaccurate financial reporting of expenditures, particularly transactions at the end of the fiscal year.

Good internal controls necessitate that invoices are accounted for and paid timely to ensure accurate financial reporting. Failure to make timely payments constitutes a non compliance with KRS 45.453 which states, "All bills shall be paid within thirty (30) working days of receipt of goods and services or a vendor's invoice except when the purchasing agency has transmitted a rejection notice to the vendor."

Further, KRS 45.454 states that "An interest penalty of one percent (1%) of any amount approved and unpaid shall be added to the amount approved for each month or fraction thereof after the thirty (30) working days which followed receipt of the goods or services or vendor's invoice by a purchasing agency."

Recommendation

We recommend KHP develop and implement controls to ensure all invoices are paid timely as required by KRS 45.453. This includes working with all park departments to ensure all invoices are submitted to the business office as soon as possible.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KHP-36: The Kentucky Horse Park Should Ensure Invoices Are Paid Timely (Continued)**

Management's Response and Corrective Action Plan

The Kentucky Horse Park management agrees with the auditor's recommendation. One reason some invoices are not paid timely is that the volume of transactions are difficult on the Business Office staff to keep pace with. In addition, some invoices were not properly expedited by receiving staff which adds to the process time. Another reason why certain invoices were paid late is a continuing restricted cash flow situation that began in the last quarter of fiscal year 2008. Due to this, at fiscal year-end some invoices had to be held longer than appropriate. Together, these reasons have contributed to the late payment of a number of invoices. The Kentucky Horse Park understands the urgency of paying invoice in a timely manner and is constantly striving to improve this matter.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KSP-37: The Kentucky State Police Clothing Allowance Payments Should Be Reported As Taxable Fringe Benefits

The FY 2009 audit of the Kentucky State Police's payroll identified that Kentucky State Police provides a clothing allowance to eligible employees for non-uniformed assignments. Furthermore, the clothing allowances were not included on the employee's Federal Form W-2, Wage and Tax Statement.

Our FY 2010 follow-up of the clothing allowance finding, identified that Kentucky State Police did not implement procedures requiring employee clothing allowances be included as "Wages, Tips, Other Compensation" reported on Federal Form W-2, Wage and Tax Statement for taxable year 2010.

Failure to implement policies and procedures which incorporate tax legislation set forth in the Internal Revenue Code constitutes a noncompliance with Federal law.

The present practice of excluding the clothing allowance from the employees' taxable income is in error. Since the clothing allowance does not qualify as a deductible expense (e.g., uniforms), the payments should be treated as taxable fringe benefits and subject to income, social security, and Medicare taxes.

The Internal Revenue Code requires that all wages, tips, and/or compensation be reported on Federal Form W-2, including those benefits associated with clothing allowances. Good internal controls dictate that policies and procedures be implemented to ensure amounts are properly reported for income tax purposes.

Recommendation

As recommended in FY 09, policies and procedures should be implemented requiring employee clothing allowances be included as "Wages, Tips, Other Compensation" reported on Federal Form W-2, Wage and Tax Statement. As such, the allowances should be subject to federal income tax withholding and FICA withholding, as well as reported and remitted timely with the agency's regular payroll filings.

Management's Response and Corrective Action Plan

The Financial/Grants Management Branch of the Kentucky State Police in the past has processed the Clothing Allowance checks for the Department of State Police. Because their process is not W-2 reportable, the Clothing Allowance checks will now be processed through a dataset within the payroll system of the Human Resources Branch. We have discussed procedures with the Personnel Cabinet as to how we can process the Clothing Allowance and have it appear on the W-2.

During the 1st supplemental payroll of 2011 (January 1 - 15 supplemental), a spreadsheet will be generated by the Financial/Grants Management Branch of the Kentucky State Police including names, social security number, location and amount of money. The spreadsheet will be sent to the Human Resources Branch. The Personnel Cabinet will produce a dataset for the Clothing Allowance.

FINANCIAL STATEMENT FINDINGS*Significant Deficiencies Relating to Internal Controls and/or Noncompliances***FINDING 10-KSP-37: The Kentucky State Police Clothing Allowance Payments Should Be Reported As Taxable Fringe Benefits (Continued)**

Management's Response and Corrective Action Plan (Continued)

After the dataset is entered, there will be an audit conducted prior to payroll running. In addition, after supplemental payroll runs, the Human Resources Branch will conduct another audit to ensure that all individuals listed on the spreadsheet are paid the correct amounts.

At the conclusion of the audit, the Human Resources Branch will examine the efficiency of the process. If there are changes to be made, the changes will be set forth prior to the next Clothing Allowance cycle- July 1, 2011.

The corrective action will be taken beginning January 1, 2011 and will be included as "Wages, Tips, Other Compensation" reported on Federal Form W-2, Wage and Tax Statement.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-38: The Kentucky State Treasury Should Strengthen System Security Settings And Values

As noted during the prior two audits, review of application security over the Kentucky State Treasury (Treasury) data processing system revealed Treasury did not establish sufficiently strong system values to properly secure the data processing system. Further, critical system values on the Treasury data processing system did not adhere to industry best practice recommendations. System values are flags that configure and control various aspects of the data processing system.

During fiscal year (FY) 2010, Treasury developed a System Value Change Requests policy; however, this policy is a very high level discussion of the request process. According to the System Value Change Requests policy, requests for system value changes should be submitted to the Division Director for justification, and the approved request should be submitted through email to the Information Technology (IT) Division Manager. Subsequent to review, IT staff perform changes and maintain the request email for documentation. Although a policy was developed, it did not include appropriate benchmark settings for system values as determined by Treasury, it omitted the retention location for request emails, and it did not reference the overarching Treasury program modifications policy.

Further, we reviewed industry best practice recommendations from the data processing system's vendor and another vendor partner for 42 system settings or values to ensure security was adequate to protect the system from known vulnerabilities. Of the 42 system values examined, we discovered 15 system values, or 35.7 percent, were more lax than the recommended industry best practices.

For security purposes, detailed information concerning the specific system values that contributed to these findings was intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

Failure to adequately document and communicate application-based security policies, including system settings or values, could lead to a lack of understanding by management and users. Without adequate security settings, the system may be subject to vulnerabilities that otherwise could have been prevented. By allowing excessive system value settings, Treasury exposes their processing system to a more heightened risk of unauthorized access and manipulation.

System settings and values are an integral part of the security environment within a system. It is important to note that the default values, which are set when the system is shipped and installed, do not represent industry best practices or the most secure values.

Recommendation

We recommend Treasury expand the System Values Change Requests policy to identify all security-related system settings deemed as being critical, a description of the function of the system setting, the suggested value established for the setting, and the justification for the selected value. Reputable resources should be used to ensure settings comply with industry best practices, and any required deviations should be explained and documented. In addition, the System Values Change Requests policy should be updated to stipulate the location where request emails will be retained and should reference the overarching Treasury program modifications policy for additional guidance on the process for requesting and completing changes.

FINANCIAL STATEMENT FINDINGS*Significant Deficiencies Relating to Internal Controls and/or Noncompliances***FINDING 10-KST-38: The Kentucky State Treasury Should Strengthen System Security Settings And Values (Continued)**

Recommendation (Continued)

Once the policy has been expanded, management should review the current settings on the data processing system to ensure compliance and make changes where necessary. The revised System Values Change Requests policy should be made available to staff that require this information to perform their job duties. Management should ensure strict adherence to the policy, and the policy should be updated as needed.

Management's Response and Corrective Action Plan

Treasury has addressed some of the system value recommendations, and has made the suggested changes to the Treasury systems. The others will be evaluated to determine the impact that the changes would have on system performance and production jobs. In addition, the Treasury will begin to keep a hard copy of all system change requests. A Data Processing Services Request Form will be developed for the office. This will allow the consolidation of all requests for changes, with complete documentation of the history of the change. The forms will be kept in a binder in the Data Processing Division.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-39: The Kentucky State Treasury Should Improve Segregation Of Duty Controls

As noted during the prior two audits, our fiscal year (FY) 2010 review of the Kentucky State Treasury (Treasury) system controls revealed Treasury did not employ sufficient segregation of duties between the system security administration, operation, programming, and librarian functions in relation to their data processing system. Our testing revealed all these functions had been granted to a single individual. This individual has unlimited access to every aspect of Treasury's data processing system including management of the use, configuration, functionality, and security of the system. Because of the lack of management oversight related to these functions, there are numerous security controls that could potentially be circumvented without detection.

Of major concern is the fact that this individual had unlimited access to the following production libraries through either a system profile or individual user profile:

- The vendor-supplied library housing all production and test libraries used to perform daily and monthly processing;
- The library housing 'new' objects used to pull enhanced Management Administrative and Reporting System (eMARS) data to assist with the monthly reconciliation; and,
- The library housing all source code objects used to process the reconciliation programs and generate the monthly reconciliation reports.

This individual had the ability to make any change deemed necessary, without management approval, to system values, user profiles, and critical objects and resource authorities. Along with vendor staff, this individual was granted the use of the vendor-supplied profiles to access the system.

During the course of fieldwork, it was noted this individual was functioning as the operator of the main monthly reconciliation program. In addition, this individual acted as the librarian for the library containing the reconciliation programs. Therefore, this individual was responsible for running the programs in production which generate the monthly reconciliation reports, but could also make changes to the programs producing the reconciliation reports. Further, this individual was responsible for monitoring a history log for suspicious activity on the data processing system, yet he had the ability to alter the data within this log.

Also, this individual, along with two computer operators, had read and write access to a directory on the processing system housing the Automated Clearing House (ACH) file provided by the Finance and Administration Cabinet (FAC), which contains several eMARS electronic fund documents. This file is generated from eMARS production tables, downloaded by the Treasury computer operators from a file transfer protocol (FTP) server and stored on the data processing system, and then submitted to the bank using software provided by the bank. The two computer operators are both responsible for the retrieval of the ACH file from FAC and submission of the file to the bank; the individual noted above with multiple incompatible duties serves as the backup for the computer operators. Although this is not considered direct access to eMARS production data, it still represents a segregation of duties issue since unauthorized changes could be made to this file prior to submission to the bank.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-39: The Kentucky State Treasury Should Improve Segregation Of Duty Controls (Continued)

It is possible that these segregations of duties issues have existed since the implementation of the data processing system, which dates back to FY 2000.

For security purposes, detailed information concerning the specific account profiles and libraries contributing to this finding are being intentionally omitted from this comment. However, these issues are thoroughly documented and will be sent hardcopy to the appropriate agency personnel.

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 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 librarian duties should implement compensatory controls to supervise programmer activities to ensure only properly tested and authorized programs are migrated into production.

Programmer duties should not include the migration of programs into production libraries or performing operator procedures such as executing production programs. Programmers should be restricted from the production environment and their activities should be conducted solely on “test” data. This control is designed to ensure an independent and objective testing environment without jeopardizing the integrity of production data.

The same individual should not retrieve the text file with eMARS funding data and also submit that same file to the bank, unless there are compensating controls in place to ensure no changes have been made to the data from the time it was received from FAC to the time it was submitted to the bank.

Recommendation

We recommend Treasury review the current job duties of the individual performing the security administrator, programmer, librarian, and operator function within the data processing system, and determine how these job functions can be redistributed among staff to ensure a proper segregation of duties. Specifically, Treasury should ensure:

- Someone other than the system administrator, who has unlimited access to the system, be the primary programmer who creates changes within the production programs.
- Someone other than the system administrator or the accounting staff be the operator that processes the reconciliation programs.
- Someone other than the programmer or operator be required to move changes into the production environment as the librarian.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-39: The Kentucky State Treasury Should Improve Segregation Of Duty Controls (Continued)

Recommendation (Continued)

In addition, Treasury should ensure the individual performing the programming function is restricted to a "Read Only" level of access within the production environment (including libraries, files, programs, etc.). Treasury should closely monitor the use of the vendor-supplied profiles for accessing the system. The individual responsible for monitoring the history log of suspicious activity should have "Read Only" access to that file.

Further, we recommend one computer operator be primarily responsible for the retrieval of the ACH file from FAC and the other be primarily responsible for the submission of the ACH file to the bank. In addition, we recommend the operator sending the file to the bank review it against the original file downloaded from FAC to identify any changes prior to submission. A log with the date, time, and name of the reviewer should be maintained to document this review. In the event one of the computer operators cannot fulfill his duties, a backup should be appointed to perform his part of the above process.

Management's Response and Corrective Action Plan

In a perfect world, and particularly in a much larger computer operation, the type of segregation of duties envisioned by the Auditor would be both useful and desirable. We certainly cannot disagree with their point of view from a theoretical standpoint. However, the reality is that the Treasury Data Processing Division is a very small operation, with only 5 total members. There is only one data processing system expert. By default, that person must perform the duties of system security administrator, programmer, librarian, operator, and every other function associated with the data processing system. He is the only one with the knowledge to write, test, and put into operation any new programs. There is no one else with whom he can share those duties. The Treasury Department has requested funding in the last two budget cycles to add an additional programmer, citing the Auditor's concern as justification. It is estimated that an additional programmer to allow this segregation would cost \$85,000 - \$90,000 per year. That funding has been denied. Until there are funds to have the necessary staff to do so, the type of segregation of duties called for by the Auditor cannot happen.

Similarly, it is not possible to segregate duties between the two computer operators. There are only two people. If one is absent, the other must perform all of the duties. These daily responsibilities include drawing down payment data from eMARS, printing all checks, and transmitting ACH files to the depository bank. The process for sending the ACH files to the bank is simply a conduit for that file. The operators do not have the knowledge of the file layout or ACH file requirements to make any changes in the file content. To segregate the duties as desired by the Auditor would require an additional operator, at an approximate cost of \$65,000 per year.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KST-39: The Kentucky State Treasury Should Improve Segregation Of Duty Controls (Continued)**

Management's Response and Corrective Action Plan (Continued)

The type of segregation of duties envisioned in this comment is not feasible at the present time, and will not be in the foreseeable future. The additional personnel cost to the Treasury of \$150,000 - \$155,000 that would be required to make this level of segregation possible is not available.

Auditor's Reply

We acknowledge the efforts Treasury made to add an additional staff member to properly segregate job duties on the data processing system, yet we will continue to make this recommendation to ensure, when funding is available, a proper segregation of duties is achieved through additional personnel.

With regard to the ACH retrieval and submission process, the opportunity remains for the computer operators to alter the file prior to submission to the bank. The issue is not that they necessarily have the expertise to do so; however, it is that the opportunity is present. Further, we recommend a backup be formally appointed in the event that a computer operator is absent.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-40: The Kentucky State Treasury Should Strengthen Logical Security Controls To Ensure Only Authorized Users Can Access The Data Processing System

As noted during the prior two audits, during our fiscal year (FY) 2010 audit of the application security of the Kentucky State Treasury (Treasury) data processing system, we determined Treasury did not implement adequate logical security controls governing user access to the data processing system. During our review, 72 user profiles were shown as having access to the data processing system. Based on a review of the profile naming conventions, there appear to be three types of profiles - individual user, vendor-supplied, and group.

Fifty-one profiles with access to the data processing system were vendor-supplied. Forty-four of these profiles did not require a password in order to access the data processing system. The remaining seven profiles required a password to access the system; however, two of the profiles, or approximately 28.6 percent, were enabled and had not changed their password since 1988. Additionally, one profile complied with the password age requirement; however, it was noted the profile functioned as a group account. The group account was shared by two system operators. Treasury established an individual profile for one of the two operators; however, the user still accessed the group profile. An individual profile was not created for the remaining operator.

Detailed profile setting documentation was obtained for one of the individual user profiles and one of the vendor-supplied profiles to determine if adequate security settings were established for the profile. All settings appeared appropriate, with the exception of one. The 'Limit Device Sessions' setting on each profile was set according to the system value setting, which allowed users to have more than one active device session at a time.

Treasury has implemented the Information Technology (IT) Security Access Request Policy governing access requests to the data processing system. According to the policy, requests are to be discussed with the Division Director and, when determined appropriate, submitted to the Information Technology Division Manager through email. The policy does not include the requirement to maintain supporting email documentation, the location where the emails are to be stored, specific information that should be included in the request email, guidelines for determining appropriate access for users, or approval and completion notifications. An examination of profiles within the system identified three user profiles that were granted access to the data processing system during FY 2010. Testing revealed an email request was not on file for one of the three, or approximately 33.3 percent, new user profiles. This user profile was created for testing of individual profiles for operators recommended in the prior year audit. Although reasonable, the creation of this profile did not follow the new IT Security Access Request Policy in place.

During testing related to the security surrounding critical utilities and commands, we found out of a sample of five key commands, a vendor-supplied group account had access to one of the five key commands sampled, or 20 percent. In addition, the public user authority was granted excessive access to one of these resources, or 20 percent. While the public user authority is not an individual, vendor-supplied, or group account, when active it does allow anyone with access to the data processing system the ability to access an object. In follow-up performed regarding three commands reported during the prior year to which the public user authority was granted excess access, we noted this access was still granted access to two commands, or approximately 66.7 percent.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KST-40: The Kentucky State Treasury Should Strengthen Logical Security Controls To Ensure Only Authorized Users Can Access The Data Processing System (Continued)**

Testing related to the security surrounding critical files and programs revealed the public user authority was granted access to the reconciliation program and resulting report file. The employee responsible for generating the reconciliation reports did not have direct access to the reconciliation report file; however, the public user authority granted access to read the file. Although her job duties necessitated this access, all users of the data processing system would also have these rights as they were granted through the public user authority and not through the individual user profile. In addition, the vendor-supplied group account had access to the reconciliation report file.

The public user authority also had elevated access to the directory on the processing system housing the Automated Clearing House (ACH) file. The ACH file contains electronic payment information that is to be submitted to the bank. This elevated access would grant all users the ability to make changes to the directory and underlying ACH files prior to their submission to the bank.

Finally, testing of the audit history log file permissions determined the vendor-supplied group account was provided access.

For security purposes, detailed information concerning the specific profiles that contributed to these findings was intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

Incomplete logical security procedures increase the risk that users are provided inappropriate or unauthorized access to the system. Allowing users the ability to access information without proper authorization may subject the processing of data to errors and/or omissions and may compromise the integrity of data processed through the system. Granting access to the public user authority could provide users the ability to access resources beyond the scope of their required job duties. The use of group profiles increases the risk that account passwords could be compromised and limits the ability to maintain an accurate audit trail. Permitting concurrent device sessions increases the risk that an account could be exploited through another machine. The existence of unused accounts also increases the risk of unauthorized use.

Management should ensure that the agency's logical security procedures are sufficiently thorough to reflect the entire logical security process. The user profile is one of the most powerful and versatile objects on the system. It contains things such as the user's password, special authorities and what menu the user sees after signing on. The user profile defines what a person can and cannot do on the system. Adequate security should be applied to user profiles to limit unauthorized access to the data processing system. Management should review all access requests to the network and data processing system and approve the requests only where appropriate based on job duties. Unnecessary accounts should be disabled, as well as concurrent device sessions. Security surrounding system objects and commands should be controlled at the individual profile level and the public user authority should be removed or set to EXCLUDE. Group profiles should be avoided in favor of individual user profiles.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KST-40: The Kentucky State Treasury Should Strengthen Logical Security Controls To Ensure Only Authorized Users Can Access The Data Processing System (Continued)**

Recommendation

We recommend Treasury strengthen its IT Security Access Request Policy related to data processing system access. Specifically, the policy should be expanded to include:

- A requirement to maintain all supporting documentation regarding additions, changes, or deletions to access, as well as the location of retained files;
- A listing of required information to be included in a request email, (at a minimum, this should include the user name, date access should become effective, reason requested, type of access/change requested, and a statement of division director approval);
- Guidelines for determining appropriate access for users based on necessary job functions;
- A requirement for an approval or denial email from the IT Division Manager to the requesting division director, as well as retention of this email in the designated repository; and,
- A requirement for a completion email from the IT Division Manager to the requesting division director indicating the requested action has been taken. This email should be retained in the designated repository.

All new user profiles developed and provided access to the data processing system should have a formal email request on file showing justification for the access granted and authorization from management. We recommend Treasury perform a periodic review of all user and vendor-supplied user profiles to ensure access is appropriate. All unnecessary accounts should be disabled. All vendor-supplied user profiles should be required to provide a password to access system resources and should be forced to comply with the password age requirement. The number of concurrent device sessions should be set to one in accordance with industry best practices. In addition, the vendor-supplied group profile should be disabled, and an individual user profile should be created for each computer operator. Treasury should either remove the public user authority from all command, utility, file, and program resources or change its Object Authority to *EXCLUDE, which would restrict access to the object to only the owner, security officer, and users with specific authority. If individuals who previously used the public user authority to gain access to libraries or object and still require this access, their individual profiles should be granted access to only those resources required for the completion of their job duties.

Additional recommendations regarding segregation of duties were also addressed in comment 10-KST-39.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KST-40: The Kentucky State Treasury Should Strengthen Logical Security Controls To Ensure Only Authorized Users Can Access The Data Processing System (Continued)**

Management's Response and Corrective Action Plan

The Treasury Department will develop a Data Processing Services Request Form to document all change requests. This form will be stored in hard copy in a binder, ready for easy review by the Auditor. The form will show the history of the request, with approvals or denials, testing and implementation dates, and similar information.

Most of the user profiles have been evaluated for need, and the ones not needed have been disabled or removed. This includes vendor profiles. The vendor profiles that we do not use have been disabled. The remaining vendor profiles are needed to run system processes. Those that do not require passwords are disabled. Some vendor profiles are sent without passwords.

We are in the process of going through the system to eliminate the public authority. It is a very time consuming task.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-41: The Kentucky State Treasury Should Ensure Critical Libraries Are Adequately Secured To Protect System Resources

As noted during the prior two audits, during our FY 2010 audit concerning application-level security over the Kentucky State Treasury (Treasury) data processing system, we determined that Treasury did not have adequate procedures in place governing the security over critical libraries housed on the data processing system. Our examination of the directory for the main system library supplied by the vendor revealed there were 138 libraries maintained on the data processing system. Of these libraries, 135 had a library type of 'production' and the other three had a library type of 'test.' However, testing revealed the library type attribute was not consistently used to accurately label production and test libraries. Specifically, 93 of the 138 libraries, or approximately 67.4 percent, did not have a description. Of the remaining 45 libraries, 2 had library type attributes indicating they were used in production; however, the descriptions indicated they may not be used in production. Specifically, one description contained the word 'test,' and the other indicated an older date. Therefore, it was not possible to conclusively separate those libraries used in production from those used for test purposes, which limited the ability to ensure the libraries were properly segregated and restricted based on function.

In addition to the vendor supplied system library, we identified three additional critical libraries. These libraries contained critical objects, such as bank master files and individual bank files that provide bank activity, bank reconciliation programs, check information, check writer programs, payroll files, bank deposit files, and program development files. Review of these libraries revealed the Treasury employee responsible for multiple duties related to the data processing system, including programming, librarian, operator, and administration functions had elevated access rights through both personal and assigned system accounts.

For security purposes, detailed information concerning the specific account profiles and libraries that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

Without an adequate object authority scheme, unauthorized excessive access could be granted to production libraries as well as critical objects and data. Granting a user unlimited concurrent access to critical production, test, and development libraries increases the risk of unauthorized or inaccurate changes being implemented and executed in production.

System resources should be specifically identifiable as to whether they are part of the production, development, or test environment. Further, access to production, development, and test libraries should be restricted to only those individuals requiring access based on their job duties in order to protect critical resources on the data processing system. Default security settings should be altered as needed to properly restrict user access to confidential or otherwise critical programs and data. Programmers and program operators should not have direct access to make changes to critical production libraries.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KST-41: The Kentucky State Treasury Should Ensure Critical Libraries Are Adequately Secured To Protect System Resources (Continued)**

Recommendation

We recommend Treasury review all users with access to the critical production, development, and test libraries to ensure the access is required and properly segregated. We also recommended Treasury review all libraries and ensure the library type field appropriately reflects the function of those objects held within the library.

A separate comment, 10-KST-39, has been issued related to the segregation of duties issue.

Management's Response and Corrective Action Plan

The Treasury Department has addressed many of these concerns. All libraries are now designated as "production", and descriptions have been added. Relative to the vendor libraries, if a description was not given when the library was installed, none will be given. That would fall to the vendor.

The Treasury Department has addressed the issue of segregation of duties in 10-KST-39. The Data Processing Supervisor must have access to all levels of security. He is the only data processing system expert in the office. The very nature of his position requires this access. Until such time as the Treasury Department's budget provides funding for an additional programmer, this situation will not change.

Auditor's Reply

As noted in 10-KST-39, we acknowledge the efforts Treasury made to add an additional staff member to properly segregate job duties on the data processing system, yet we will continue to make this recommendation to ensure that, when funding is available, a proper segregation of duties is achieved through additional personnel.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-42: The Kentucky State Treasury Should Update Formal System Documentation To Reflect Processing Performed

As noted during the prior two audits, our fiscal year (FY) 2010 audit of the Kentucky State Treasury (Treasury) system controls related to their main data processing system revealed Treasury did not maintain clear and accurate descriptions of critical system programs and associated files utilized in the bank reconciliation process. Based on testing and discussions held with agency personnel, it appears this lack of documentation has existed since the implementation of the data processing system in 2000.

The Treasury Bank Reconciliation Manual provides a high-level general overview of the reconciliation process, the reconciliation data extract process, each of the critical programs that are run to generate the monthly reconciliation reports, and timing difference and analysis reports. Treasury has also implemented an Operators Guide for performing critical tasks on the data processing system.

During the examination of the contents of three critical computer libraries used by Treasury, it was determined that documentation was insufficient to allow a user to determine if the individual objects (files, programs, etc.) maintained within the libraries were used in production. The following specific issues were identified during testing:

- Of the 257 objects residing within the library housing the 'new' check processing/accounting objects, 186 objects, or approximately 72.4 percent, did not have a description. Of the remaining 71 objects containing descriptions, 5 objects, or approximately 1.9 percent, contained the word 'test' within the description, indicating the object may not be used in production.
- Of the 2,002 objects residing within Treasury's main production library used to run the reconciliation programs, 1,280 objects, or approximately 63.9 percent, did not have a description. Of the remaining 722 objects containing descriptions, 98 objects, or approximately 4.9 percent, did not appear to be run in production based on the description. Words found within the descriptions included 'onetime,' 'under development,' 'Y2K,' 'test,' 'MARS,' 'temporary,' 'temp,' and 'special run.' Additionally, 41 objects, or approximately 2.0 percent, had descriptions only reflecting the name of the object.
- Of the 14 objects residing within the library used by the Treasury employee responsible for making program changes, 12 objects, or approximately 85.7 percent, did not have a description.

During the FY 2008 audit, Treasury indicated the intention to re-name the library objects to provide a better understanding of the individual program functionality. However, this project has not yet been started and is not anticipated to occur until the reconciliation process is current.

For security purposes, detailed information concerning the specific objects that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-42: The Kentucky State Treasury Should Update Formal System Documentation To Reflect Processing Performed (Continued)

Lack of documentation increases the likelihood of erroneous or incomplete processing. This increases the likelihood of unauthorized data modification, destruction of assets, and interruption of services. Failure to appropriately update system documentation increases the risk that users will be unaware of changes that could potentially alter their business processes. The inability to determine the function of library objects could lead to agency staff being unable to differentiate between production, development, and test objects.

Proper descriptive documentation should be maintained for each critical library object in order to, at a minimum, identify the purpose of the objects, the origin of data, the specific calculations or other procedures performed, and the output of data or reports. Object descriptions should provide a clear distinction between active production and test objects.

Recommendation

We recommend Treasury thoroughly review the objects within each library and ensure all objects are needed. All unnecessary objects should be removed. If any objects are housed in an incorrect library, such as testing objects in a production library, the objects should be moved to the appropriate library. For all necessary objects, adequate descriptions should be provided identifying the intended function of each object. This information is critical given the complexity of the programs currently used by Treasury to perform monthly processing.

We further recommend Treasury follow through with the renaming of library objects to better reflect their functionality.

Management's Response and Corrective Action Plan

The Auditor's recommendation represents a monumental task which cannot be accomplished with present personnel and resources. To accomplish this in a timely manner would require an additional programmer devoted solely to this task until completed. The cost of an additional programmer, including all benefits, would be approximately \$85,000 per year.

There are currently over 35,000 objects on the Treasury system. Since the Auditor's comments last year, the Treasury Department has been in the process of removing unneeded objects. It is an extremely slow process, however. With so many objects on the system, it takes time to research and verify the object's use. This will be an on-going process which will span many years' audit periods. As the Auditor has indicated, some of these programs were developed before 2000. Some are actually much older than that, and represent the work of many different programmers and data processing managers. To go back and analyze decades of work done by numerous people is daunting. It takes time to evaluate the impact to the functions of the system and applications. If the name on an object is changed, that name must be changed in every single program that utilizes that object.

FINANCIAL STATEMENT FINDINGS*Significant Deficiencies Relating to Internal Controls and/or Noncompliances***FINDING 10-KST-42: The Kentucky State Treasury Should Update Formal System Documentation To Reflect Processing Performed (Continued)**

Management's Response and Corrective Action Plan (Continued)

With the ongoing Treasury reconciliation project, the new payroll and personnel system (KHRIS) which will go live in March, the new Revenue Department collection system, and other immediate projects demanding programming time, it will not be possible to give this priority treatment.

Auditor's Reply

We acknowledge the intentions of Treasury to perform a review of all database objects for necessity. We also understand the demands of daily operations, as well as the new initiatives scheduled for implementation in the near future. However, due to the potential risk to processing, we will continue to recommend that unneeded objects on the data processing system be eliminated as time is available for this task.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-43: The Kentucky State Treasury Should Develop And Implement An Application Security Policy Related To The Data Processing System

As noted during our two prior year audits, our FY 2010 audit of application-level security over the Kentucky State Treasury (Treasury) data processing system revealed Treasury did not have formal security control policies or procedures in place concerning critical functionality on the data processing system. Of greatest concern is the lack of management-defined security controls related to critical utilities, commands, libraries, and objects such as programs and files residing on the data processing system.

Treasury has created an Information Technology (IT) Security Access Request Policy; however, this policy only discusses the process to request access to the network and data processing system. It does not discuss any security controls specific to the critical aspects of the data processing system.

Failure to adequately document, implement, and communicate acceptable application security policies and procedures could lead to a lack of understanding by management and users. This lack of understanding could potentially result in a failure to comply with security policies, failure to perform assigned security responsibilities, or inappropriate and inefficient use of system functionality or resources. Additionally, it increases the likelihood of unauthorized or inaccurate data modification, destruction of assets, interruption of services, or inappropriate or illegal use of system resources.

Formal policies should be established specifically addressing security controls over critical utilities, commands, libraries, and objects to help ensure only authorized access is granted to these resources and appropriate actions can be taken against Treasury's data processing system. Consistent application of formal security policies and procedures provides continuity for implementation and sets the tone of management concern for strong system controls.

Recommendation

We recommend Treasury develop formal policies and procedures to administer the security of their data processing system. The system security policy should include:

- functional and technical requirements;
- management's objectives and expectations for information security in clear, unambiguous terms, along with the implications of noncompliance;
- key risks and mechanisms for dealing with those risks;
- roles and responsibilities of management and users;
- a process for regular monitoring and feedback to ensure the policies are enacted and enforced;
- flow charts of the system and interfaces;
- procedures for performing major functions;
- sample reports, screens, and forms;
- recovery procedures;
- physical security procedures;

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-43: The Kentucky State Treasury Should Develop And Implement An Application Security Policy Related To The Data Processing System (Continued)

Recommendation (Continued)

- virus prevention and protection procedures;
- end user accountability and acceptable use;
- policy for enabling auditing and frequency of review; and,
- listing of critical libraries, commands, utilities, and objects and authority that should be established over them.

These policies and procedures, once developed, should be properly distributed and all necessary system users made aware of their responsibilities. Further, management should ensure the consistent application of these procedures.

Management's Response and Corrective Action Plan

While Treasury does not dismiss the importance of the security of the network or applications, the suggestions would seem to be somewhat excessive for an agency this size. It is important not to lose sight of the fact that the entire Treasury Data Processing Division consists of five people: a data processing system manager/programmer; 2 operators who run the check print program, an agency network administrator, and a data coordinator. The entire office staff is approximately 30 people. The elements recommended to be included in the system security policy, though certainly desirable, may be difficult to put together quickly with current staff levels and workloads. Many of the major recommendations are already in place, however. We have procedures for major functions (i.e. Operator's Manual), recovery procedures included in the Business Recovery Plan, and physical security procedures. A virus prevention and protection package is already in place and is updated regularly per COT recommendations. COT Alerts are disseminated throughout the office each time one is issued. End user accountability standards and acceptable policies are in place and are distributed to all employees upon employment.

The Treasury Department will continue to upgrade and enhance its formal security policy and procedure elements as conditions and time allow. It will be an on-going process, with the end goal of having a completely documented and accountable system.

Auditor's Reply

Our recommendation addresses the need for a comprehensive security policy to include key security elements. We acknowledge that Treasury does have certain procedures currently in place; however, procedures have not been created for the critical elements of the data processing system, including utilities, commands, libraries, and objects. Since the data processing system is an integral component of Treasury operations, it is necessary that adequate policies and procedures be developed. We also recognize that the creation of policies will not occur immediately and will, therefore, continue to recommend policy development until a comprehensive policy governing the data processing system is complete.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-44: The Kentucky State Treasury Should Enable System Auditing On Its Data Processing System

As noted within our prior two audits, during our FY 2010 audit concerning application security over the Kentucky State Treasury (Treasury) data processing system, we determined that, according to the system value settings at the time of our review, security auditing of the system was not being performed.

Although these system settings did not require security auditing to be performed, a history log is produced by the system. This log contains past system operator messages, device status, job status changes, and program temporary fix activities that are stored as system messages. While the information reported on this log appears to be useful, we were not able to confirm that Treasury is actively monitoring this log sufficiently to ensure security of the system. The program administrator stated that he performs a review of the history log three to four times a year in order to identify suspicious activity. However, no documentation is maintained to support these reviews nor is anyone outside of the program administrator performing this review.

As was noted in the previous year, it appears that the system audit feature was not made operational since the implementation of the data processing system, which dates as far back as year 2000.

Failure to adequately monitor security events and logs could result in failure to identify suspicious activities that may be occurring on the system.

With effective monitoring of event and security logs, a decreased risk of fraud exists due to unauthorized access and system changes. A logging and monitoring function enables the early detection of unusual or abnormal activities that may need to be addressed.

Recommendation

We recommend Treasury enable security auditing for critical objects on the data processing system and ensure management reviews the event and history logs on a regular basis. The reviews of event and history logs should be documented and retained for audit purposes.

Management's Response and Corrective Action Plan

Treasury will evaluate the audit log process to determine the best option, and will request additional funds in the budget for an outside service to perform audit log reviews. The Commonwealth Office of Technology does not have any professionals for the Treasury data processing system. This will be a new budget item for the Treasury to fund this regular review.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-KST-45: The Kentucky State Treasury Should Expand And Strengthen Formal Program Change Control Procedures

As noted during the prior two audits, our FY 2010 audit of system controls revealed weaknesses with regard to the program change control procedures of the Kentucky State Treasury (Treasury). In response to the prior year recommendations, Treasury developed and implemented a formal Programming Requests Policy governing controls for program development and modifications of critical data processing systems. However, the policy did not adequately address all phases of the program change control process.

The Programming Requests Policy dictates that all programming requests for new development or modification to existing systems are to be discussed with the appropriate Division Director. Once there is justification for the change request, the Division Director makes a formal request by email to the Information Technology (IT) Division Manager. The requests are then reviewed for feasibility by the IT Division Manager and either approved, returned for more information, or rejected with explanation. Although not specified in the policy, the IT Division Manager stores all requests in a Microsoft Outlook folder.

The Programming Requests Policy is stated at a very high level and does not contain specific requirements related to the following areas:

- Supporting content of the initial request email;
- Testing of program changes prior to submitting to production;
- Approval to move to production;
- Final acceptance notification;
- Retention of all documentation supporting change, including request emails, testing documentation, and approval documentation; and,
- For new program development, the creation and retention of program specifications and other related technical documentation.

Further, testing of supporting documentation for two secondary program changes made since the prior year review revealed adequate documentation was not on file for the implementation of these changes. Both changes had an email on file requesting the change, but no emails were maintained to show approval of the change, approval to move the change from testing to production, and final approval of the change. Further, there was no documentation on file showing the changes were tested prior to being moved to production.

Also, the operating system running the main reconciliation program was updated since the prior year review. However, no documentation was on file to substantiate who made the update, when the update was made, or who approved the update to be installed.

Without specific and detailed program change control procedures, management increases the risk of developing and implementing ineffective or inaccurate systems and the risk of unauthorized changes being placed into the production environment that have an adverse affect on system processing results.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KST-45: The Kentucky State Treasury Should Expand And Strengthen Formal Program Change Control Procedures (Continued)**

Policies and procedures ensure that an organization's program change control methodology applies to the development of new systems and programs, major changes to existing systems and programs, and user participation. Program change control procedures require adequate program specifications be provided to a programmer prior to program development to mitigate processing errors and the need for numerous program modifications. Sufficient procedures dictate that complete and accurate system documentation be developed and maintained for all critical systems, as this information is vital to ensuring longevity of the system. Program change control procedures must be consistently applied and include adequate procedures to segregate the live production environment from development and testing environments. They should also be distributed to all key personnel to ensure consistent implementation of new systems.

Recommendation

We recommend Treasury expand their current Programming Requests Policy to ensure all steps of a complete program change control process are adequately defined. With regards to the formal request by email, the policy should state the requirements of the emails. The initial request emails should include (at a minimum) the following:

- a necessity for the change;
- programmatic specifications related to the proposed change;
- the affected system(s); and,
- the program and/or report the change will affect.

We also recommend the following expansion of the procedures in order to strengthen the Programming Requests Policy:

- add requirement to retain all documentation supporting the change, including request emails, testing documentation, and approval documentation within the specific retention location;
- add requirement to test program changes prior to submitting to production;
- add requirement for approving changes to be implemented in production;
- add requirement for a final acceptance notification from requestor accepting changes after moved to production; and,
- add requirement for new program development related to the main accounting/reconciliation system to create and retain detailed program specifications and technical documentation.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-KST-45: The Kentucky State Treasury Should Expand And Strengthen Formal Program Change Control Procedures (Continued)**

Recommendation (Continued)

Once these changes have been made to the Programming Requests Policy, Treasury should provide this information to all appropriate staff and ensure strict adherence to the policy going forward.

Further, documentation should be maintained regarding any updates or fixes concerning system maintenance and changes. This documentation should include who made the update, when the update occurred and who approved the update.

Management's Response And Corrective Action Plan

The Treasury Department will design and implement a "Data Processing Services Request Form" for use within the office. This will be an on-line Word document that will establish justification for any data processing change request. The document will also provide a history of that request. It will be printed and kept in hard copy in a binder in our Data Processing Division, ready for inspection by the Auditor. On this form the Data Processing Staff will be able to document all approvals, testing and implementation. It should provide a concise but thorough record of the change. This will primarily be used for internal requests.

In actuality, most of the Treasury Department's change requests come from other agencies. These requests are usually made verbally and by email. When made verbally, they are followed by a written request, usually by email. The email chain is kept as documentation for that request. We would envision that these, too, could be printed, coupled with a "Data Processing Services Request Form" completed by our staff, and retained in the binder for future review by the Auditor.

We will also maintain documentation regarding any updates or fixes concerning system maintenance and changes. This documentation will include who made the update, when the update occurred and who approved the update.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-PARKS-46: The Department Of Parks Should Ensure That Vendors Are Paid Timely In Compliance With Statute

During the FY 2010 audit of the Department of Parks (Parks), the auditor discovered 10 instances in which invoices were not paid within 30 working days as required by statute. One of these instances involved a payment exceeding 60 working days from the date of the invoice.

Agencies are responsible for a 1% penalty on each payment not made within 30 working days. Failure to pay vendors in a timely manner also erodes relationships with those vendors who may decide to stop doing business with Parks. Thus, failure to pay invoices on time costs the agency money, can affect the running of the state parks, and can negatively impact the services provided to guests.

KRS 45.453 states, "All bills shall be paid within thirty (30) working days of receipt of goods and services or a vendor's invoice except when the purchasing agency has transmitted a rejection notice to the vendor."

In addition, the purchasing agency is responsible for a 1% penalty when payment is not made within 30 working days.

Recommendation

While there were a significant number of late invoices noted during testing, there was a significant decrease in the number of late payments noted during the previous year's audit.

We continue to recommend that payments be made in a timely manner. Controls should be developed and implemented to ensure payments are made in a reasonable time frame in compliance with legal statutes. The agency should review the statutes and policy noted above to ensure full compliance. The agency should take steps to ensure that the people involved in processing and approving payments read and understand the relevant laws and policies.

Management's Response and Corrective Action Plan

The Department of Parks is in agreement with the findings and has addressed the issue with the parks involved directly. We will continue to monitor timeframe of payments made and address those falling outside the guidelines. In most instances, with the specific documents listed, it is difficult to tell if the invoice was truly paid late or if the items in question arrived after the date of the invoice thus delaying the payment. With the recent addition of new staff, we are in the process of realigning job duties and responsibilities. This realignment includes specific staff being assigned to specific parks for auditing of all payment documents.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-PARKS-47: The Department Of Parks Should Ensure That Timesheets And Leave Forms Are Completed And Approved To Support Payroll Expenditures

During testing of payroll expenditures for the FY 2010, the auditor noted the following exceptions:

- Five timecards or timesheets that were not signed by either the employee, their supervisor or both.
- Four timecards with changes made to the electronically stamped time that was not initialed.
- Five timecards were not mathematically accurate or not totaled on the card. In two of these instances overtime or compensatory time earned does not agree to the approved overtime form.
- Five instances where there was no documented approval of overtime worked or leave time taken for the time period.
- Four instances where approved overtime or leave time forms did not agree to the timecard.

Expenditures including payroll should be supported by documentation that agrees to the amount paid for that expenditure. Due to the errors and omission described above these payroll expenditures were not adequately substantiated by the documentation including timesheets, properly approved leave requests, and overtime forms.

Good internal control over payroll dictates that payroll charges should be supported by adequate documentation including signed timesheets or timecards, leave and overtime forms that detail and substantiate hours and times worked by each employee.

Recommendation

We recommend Parks review established standards for recordkeeping including requirements for the use of leave and overtime approvals and ensure that procedures are uniform across all Parks facilities. In addition, Parks should consider establishing a periodic review of payroll at each park that includes agreeing timecards and other supporting documents to ensure that they support payroll and are completed per the established guidelines.

Management's Response and Corrective Action Plan

The Human Resources Director and a Human Resources Specialist have reviewed the exceptions and agree with the findings. We are in the process of contacting each park manager that had exceptions. The Human Resources Director will be reviewing the errors and have the park manager and payroll officer make corrections as required. The parks with exceptions were Barren River SRP, Dale Hollow SRP, EP Tom Sawyer SP, Cumberland Falls SRP, and Parks - Cafeteria.

Department of Parks currently has a park policy that requires employees and supervisors to sign all timecards as well as initial any times written in or any changes made to the time card. Park Policy also requires employees to utilize the leave slip for all leave time and compensatory time earned and used.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-PARKS-47: The Department Of Parks Should Ensure That Timesheets And Leave Forms Are Completed And Approved To Support Payroll Expenditures (Continued)**

Management's Response and Corrective Action Plan (Continued)

On December 15, 2010 the Human Resources Director sent a memo, via email, to all park managers, business managers, and payroll officers reiterating established standards for recordkeeping including requirements for the use of leave and overtime approvals and ensure that procedures are uniform across all Parks facilities. The Human Resources Director reiterated Park Policy 01-01, instructing managers/payroll officers to review with supervisors and employees the payroll policies as well as the types of errors that were found to ensure that all employees are fully aware of the payroll policies and to ensure that payroll officers are reviewing employee payroll more carefully. The Human Resources Director believes that our payroll officers and managers have a good understanding of the payroll process. However they do need to review the payroll more closely and catch these type errors.

In a memo to park managers and payroll officers the Human Resources Director did inform them that all employees are required to use the leave/compensatory earned slip to record all hours worked on holidays. Even though the holiday may be the employee's scheduled work day, the hours should be coded as compensatory time earned on the slip. The Human Resources Director did discover that our parks were not consistent with this process.

The Human Resources Director also discussed the exceptions with our internal auditor. She will be scheduling an internal payroll audit in a few months as a follow up. This review will agreeing timecards and other supporting documents to ensure that they support payroll and are completed per the established guidelines.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-PC-48: The Personnel Cabinet Should Ensure Sufficient Authentication Is Required To Access Potentially Sensitive Information

As noted during the prior year audit, while performing the FY 2010 audit of the Personnel Cabinet, we discovered instances where no authentication was required to allow an outside user to gain access either to information about the machine or to the service running on a designated port. We determined 4 out of the 16 machines scanned, or 25 percent of the population, were running the File Transfer Protocol (FTP) service allowing unauthorized access through the anonymous default accounts on the machines. One of these machines was commented on during the prior year audit.

For security purposes, detailed information that would identify the specific machines contributing to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

If a machine properly configured to allow only authorized users access to the service, the risk of intentional or unintentional modifications to system data and resources is increased.

Services running on agency machines should be properly configured and default accounts should be disabled to ensure unauthorized access is prohibited.

Recommendation

We recommend the Personnel Cabinet review the services noted within this comment to ensure that they are properly configured to ensure only authorized users gain access. If a service is determined not to have a specific business purpose, it should be disabled. For those services that do have a business purpose, authentication features should be reviewed to ensure that they are configured to restrict access to only users who have a need for the service.

Management's Response and Corrective Action Plan

The Personnel Cabinet Network Support Branch staff has reviewed the machines identified from the previous scan. The indicated VoIP device is maintained by an outside vendor; to our knowledge this service is properly authorized, configured, and up-to-date. Further, this proprietary device has no domain rights to the Personnel Cabinet network. The indicated printers will be moved to a private IP address upon implementation of the Deferred Compensation Authority's new third-party administrator. Thank you for your continued efforts in scanning mission critical systems to secure the information resources of the Commonwealth.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-PC-49: The Personnel Cabinet Should Strengthen Logical Security Procedures Over The Uniform Personnel And Payroll System**

As noted within our previous audit, during the FY 2010 audit of the logical security controls over the Personnel Cabinet's Uniform Personnel and Payroll System (UPPS), we noted that while a formal policy was developed for establishing access to the UPPS, it was not consistently adhered to for granting user access to the application.

In order to request access to UPPS, an electronic copy of the Customer Information Control System (CICS) Access Request form must be completed by the security officer of the applicable agency. On this form, the user's supervisor or manager must indicate what type of access should be granted to each of the applications that make up the UPPS. The form is then forwarded to Personnel Cabinet security staff where verification of approval by the appropriate supervisor/management is performed prior to establishing requested access. To ensure compliance with this process, we examined the CICS Access Request forms for 15 users that had been granted access to UPPS during FY 2010. Our testing revealed insufficient documentation was maintained to support the access granted to four users, or 26.7 percent.

In addition, we identified two users that had more than one user Id with access to the UPPS. Subsequent to bringing this situation to management's attention during our field work, the Personnel Cabinet removed the unnecessary access associated with these users. Also, we identified eleven accounts that appeared to be used by more than one individual, none of which had supporting documentation available to support this access. Additionally, four apparent group accounts were found to be active, only one for which the Personnel Cabinet could identify the underlying users.

We are aware informal procedures were implemented by Personnel Cabinet security staff in August 2009 to attempt to mitigate issues identified during the prior year audit. Also, the formal security policies were under review by management during audit field work. However, they were not completed during FY 2010.

Failure to consistently apply logical security controls could lead to a lack of understanding by management and users that could result in a failure to comply with security policies, failure to perform assigned security responsibilities, or inappropriate and inefficient use of system resources. This situation increases the risk of unauthorized data modification, destruction of assets, interruption of services, and inappropriate or illegal use of system resources.

The foundation of logical security is access control, which refers to how system access is determined and granted to users. Formal policies provide a security framework to educate management and users of their security responsibilities. These controls must be comprehensive in nature and consistently applied to ensure the security of agency resources and data. Consistent application of formal security policies and procedures provides continuity for implementation and sets the tone of management concern for strong system controls.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-PC-49: The Personnel Cabinet Should Strengthen Logical Security Procedures Over The Uniform Personnel And Payroll System (Continued)**

Recommendation

We recommend the Personnel Cabinet ensure all procedures related to the establishment of access for the UPPS system and associated datasets, are consistently and completely performed. The Personnel Cabinet should ensure the CICS Request Form is completed properly and authorization is obtained prior to granting access to the application. Any group accounts in use should be disabled and individual accounts for related users should be established with similar rights. The Personnel Cabinet should also review all accounts and ensure users only have one active account on file. Unnecessary accounts should be removed. All documentation should be maintained for audit purposes.

Management's Response and Corrective Action Plan

The Personnel Cabinet (Personnel) agrees with this finding and continues to strengthen security measures with improved policies and procedures related to system security. Effective July 2010, Personnel revised and updated procedures for providing access to mission critical systems. These policies and procedures will be followed to ensure authorization is granted appropriately for all users. Personnel security is currently reviewing the four user group accounts and detail of multiple userids to determine the status of these accounts.

The security staff will work with all necessary parties to ensure correct access and/or reassignment from group accounts. All related parties will be kept informed and involved as we resolve these issues. Further, Personnel security will utilize the PERPOPA2 report to produce a list of all users by agency. This report will be used to locate multiple users assigned to one account and correct these account assignments.

The updated policy and procedures require agency designated security contacts (DSC) to analyze this system report on a monthly basis and correct inconsistencies and discrepancies in user access. Documentation related to user access is now being stored using the Front Range "helpdesk" application. Use of this application provides electronic storage of security request documentation. Thank you for your continued assistance in protecting the information resources of the Commonwealth.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-REV-50: The Department Of Revenue Should Strengthen Logical Security Controls Over The On-Line System For The Collection Of Accounts Receivable

As noted during the previous three audits, our FY 2010 audit of the Department of Revenue (DOR) logical security controls revealed that the Systems Administration Branch within the Division of Collections did not consistently follow the existing procedures for granting access to Kentucky's On-Line System for the Collection of Accounts Receivable (KY OSCAR).

According to Finance and Administration Cabinet (FAC) standard procedure 6.5.2, the DOR requires supervisors or managers to complete the Authorization to Access Department of Revenue Confidential Computer Information and the KY OSCAR User ID Request forms to request system access. Both forms are then submitted to the DOR Security Office. The DOR Security Office reviews the Authorization to Access Department of Revenue Confidential Computer Information form to ensure it is approved and properly indicates access to KY OSCAR and ensures the user has also submitted a KY OSCAR User ID Request form. The DOR Security Office then grants access to the KY OSCAR group and initials both forms. Once completed by the DOR Security Office, the Authorization to Access Department of Revenue Confidential Computer Information form is filed for audit purposes, and the KY OSCAR User ID Request form is forwarded to the Systems Administration Branch within the Division of Collections for processing. The Systems Administration Branch next establishes the KY OSCAR User ID, and they sign and retain the KY OSCAR User ID Request form.

Review of the Authorization to Access Department of Revenue Confidential Computer Information and KY OSCAR User ID Request forms specific to a sample of 20 KY OSCAR new users revealed DOR did not adhere to the established procedures as follows:

- Three Authorization to Access Department of Revenue Confidential Computer Information forms, or 15 percent of the tested user population, were not on file.
- Two KY OSCAR User Id Request Forms, or 10 percent of the tested user population, did not specify a user capability level.
- One KY OSCAR User Id Request Form, or 5 percent of the tested user population, lacked supervisor approval.

Allowing users the ability to access information without proper authorization may subject the processing of data to errors, omissions, or unauthorized transactions and may compromise the integrity of data processed through the KY OSCAR.

The foundation of logical security is access control, which refers to control of how the system is being accessed and by whom. Guidelines provide a framework to educate users of their security responsibilities. The Authorization to Access Department of Revenue Confidential Computer Information and KY OSCAR User Id Request forms should be completed and authorized for each new user in order to substantiate access to KY OSCAR.

FINANCIAL STATEMENT FINDINGS*Significant Deficiencies Relating to Internal Controls and/or Noncompliances***FINDING 10-REV-50: The Department Of Revenue Should Strengthen Logical Security Controls Over The On-Line System For The Collection Of Accounts Receivable (Continued)**

Recommendation

We recommend the DOR consistently adhere to the established procedures for requesting and granting access to KY OSCAR. Specifically, the DOR should ensure all forms are completed and properly authorized and the Security Office and Systems Administration Branch signs off on the applicable forms identifying approval for processing the access request.

Management's Response and Corrective Action Plan

DOR will continue to ensure consistent adherence to established procedures for requesting and granting access to KY OSCAR. In addition, the DOR Security Office will continue to work with the Division of Collections, Systems Administration Branch to ensure that all KY OSCAR forms are properly authorized.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-TC-51: The Transportation Cabinet Should Ensure Inventory Values Entered By Personnel Are Reasonable**

During the FY 2010 audit of inventory, an OMS (Operations Management System) operator entered the linear feet of backer rod instead of the number of 200 foot sections (or rolls) received. The operator was charging out the linear foot for each project. An adjustment to the closing package in the amount of \$318,798 was required as a result of the error.

In the preliminary planning of the inventory audit, the auditor requested a report of inventory for each area (Materials, Traffic, and Equipment). After receiving the report, the Office of Internal Audit informed the auditor a data entry error occurred. For signs, personnel had entered a unit cost of \$209,171 for each sign when the actual unit cost was about \$8. This overstated the inventory in District 2 by approximately \$11,713,130 prior to the end of the fiscal year.

The cause of both issues noted above is data entry error, one error related to quantity and the other cost. The backer rod data entry resulted in the year-end inventory showing a quantity of 8900 instead of 44.5. The cost was \$36 per roll so the inventory on hand at year end was actually \$1,602 instead of \$320,400, a decrease of \$318,798.

If the Office of Audits had not noticed the \$11,713,130 error, a material misstatement of traffic inventories could have occurred in the financial statements. Good internal controls should ensure the quantity and cost of materials entered is reasonable.

Recommendation

We recommend KYTC:

- Establish maximum values in OMS.
- Consider reviewing inventory amounts at various times throughout the year to determine if the amount of each item appears reasonable.

Management's Response and Corrective Action Plan

OMS was recently updated to include maximum and minimum unit costs for all materials. Routine spot inspections for all material unit costs will be conducted until we are comfortable that this has resolved the issue.

District 2 Response on the Backer Rod inventory

We will set maximum allowable amounts in OMS in order to control this type of error in the future and management will review inventory periodically to determine if the amount indicated is within reason.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-TC-52: The Transportation Cabinet Should Implement Procedures To Ensure Compliance With Kentucky Laws For Transferring Property

The Auditor of Public Accounts (APA) received concerns indicating that unauthorized right of way transfers may have occurred between the Kentucky Transportation Cabinet (KYTC) and a coal company in eastern Kentucky. Four filed Quitclaim deeds were reviewed to determine whether the right of way conveyances were performed in accordance with state statutes. The detail of these records, in which KYTC is the grantor in two of the conveyances and the grantee in the other two, are listed below:

- Deed 1 (recorded June 29, 2007): The grantor (KYTC) conveyed to the grantee all of the grantor's interest in a parcel of land in Perry County, with certain agreements. These agreements included the grantee's agreement to convey a section of property to KYTC to be used as a temporary roadway during construction of a new section of road, as well as the conveyance to KYTC the surface rights for right of way associated with the newly constructed section of highway once it is complete.
- Deed 2 (recorded June 29, 2007): Per the agreement in Deed 1, the grantor conveyed to the grantee (KYTC) the surface rights of certain property noted in Deed 1 that is to be used for a temporary roadway during construction of a new section of highway. The deed contained an agreement that KYTC would convey this parcel back to the grantor upon the completion of the construction of the new section of highway.
- Deed 3 (recorded December 8, 2008): Per the agreement in Deed 1, the grantor conveyed to the grantee (KYTC) surface rights to right of way associated with the newly constructed section of highway.
- Deed 4 (recorded December 8, 2008): Per the agreement in Deed 2, the grantor (KYTC) conveyed to the grantee its interest in the parcel of land transferred to it in Deed 2 and used for a temporary road.

Upon review of these deeds, it appears the only person authorizing these conveyances on behalf of KYTC and the Commonwealth of Kentucky was the KYTC district Right of Way Supervisor. The conveyance of property from another party in this manner is inconsistent with KYTC's written policies and procedures on the acquisition of right of way. KYTC does not have the authority to dispose of property or transfer property, and therefore the conveyance of property to another party in this manner is not compliant with KRS 45A.045, which requires all instruments required by law to convey property be executed and signed by the secretary of the Finance and Administration Cabinet (FAC) and approved by the Governor.

It appears internal controls within the agency were circumvented in order to complete these property conveyances. When district personnel implement procedures outside the agency's standard processes, then central office personnel do not have the appropriate knowledge of the activity to provide proper monitoring and oversight, and to assess whether procedures are being performed in accordance with state and federal requirements.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-TC-52: The Transportation Cabinet Should Implement Procedures To Ensure Compliance With Kentucky Laws For Transferring Property (Continued)**

The APA recognizes it is difficult to implement sufficient procedures to prevent the circumvention of controls by an employee or employee(s), however, appropriate disciplinary actions taken against employees involved in such actions should be clearly communicated. The effect of unauthorized property conveyances could expose KYTC and the Commonwealth to significant loss of assets. In this situation, the conveyances of property from the Commonwealth to the grantee may be considered void due to the KYTC employee not having appropriate authority to convey property to other parties.

KRS 45A.045 (4) states, "...All instruments required by law to be recorded which convey any interest in any real property so disposed of shall be executed and signed by the secretary of the Finance and Administration Cabinet and approved by the Governor. Unless the secretary of the Finance and Administration Cabinet deems it in the best interest of the state to proceed otherwise, all interests in real property shall be sold either by invitation of sealed bids or by public auction. The selling price of any interest in real property shall not be less than the appraised value thereof as determined by the cabinet, or the Transportation Cabinet for the requirements of that cabinet."

Recommendation

We recommend:

- KYTC should work with FAC legal counsel to determine what, if any, remedies are appropriate to rectify the unauthorized property conveyances. The opinion of the FAC legal counsel should be documented in writing and maintained by KYTC.
- KYTC should consider the circumstances that created or permitted the circumvention of controls, and determine the additional procedures that can be put in place to further protect assets from such risk.

Management's Response and Corrective Action Plan

We agree with your recommendations. We will work with FAC General Counsel on an appropriate resolution to rectify the unauthorized property conveyances. We will obtain an FAC legal counsel opinion in writing and maintain that on file at KYTC.

We have documented policies and procedures in the Right of Way Manual (ROW 1502 and 1503) regarding property transfer and have had those for many years. The Secretary of State Highway Engineer will send a reminder to all Chief District Engineers, Right of Way Supervisors and other appropriate personnel and require a signed acknowledgement form from all pertinent personnel. We will do this within the next 2 months.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls and/or Noncompliances

FINDING 10-TC-53: The Transportation Cabinet In Coordination With The Commonwealth Office Of Technology Should Strengthen The Security Of System Accounts

While performing the FY 2010 security vulnerability assessments for Kentucky Transportation Cabinet (KYTC) machines, which are partially managed by the Commonwealth Office of Technology (COT), we identified various system user accounts with password ages that exceeded the established password policy or that had never been used.

We obtained NetBIOS account information from two Domain Controllers (DC). To determine if user accounts on these machines were in compliance with established KYTC policies, the auditor used the criterion that account passwords with ages over 31 days were non-compliant, which is the established agency policy. On both the Primary Domain Controller (PDC) and Backup Domain Controller (BDC), there were 196 accounts out of a total of 867, or approximately 22.6 percent, that met this criterion. In relation to the PDC, 21 of these accounts appear to have never been used. There were 85 accounts on the BDC that appeared to have never been used. These accounts had password ages between 33 and 2520 days.

For security purposes, detailed information concerning the specific machines or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues were thoroughly documented and communicated to the appropriate agency personnel.

Lax enforcement of the agency's established password policy or the existence of unused accounts increases the likelihood that accounts could be compromised, as well as the underlying data accessible by those accounts.

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. Established password policies should be consistently applied and enforced.

Recommendation

We recommend KYTC work with COT to review all user accounts on the identified machines to ensure compliance with the established security and password policies. These accounts should be evaluated to determine if they are still valid accounts and are required for a business related purpose. If they are needed, then they should be forced to comply with agency password policies. Otherwise, the accounts should be disabled or deleted depending on the necessity of reinstatement of the account.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls and/or Noncompliances*****FINDING 10-TC-53: The Transportation Cabinet In Coordination With The Commonwealth Office Of Technology Should Strengthen The Security Of System Accounts (Continued)**

Management's Response and Corrective Action Plan

KYTC Response: KYTC ISO contacted KYTC Drivers License Agency Contact requesting review and validation of the user accounts reported. KYTC IT Request Log # 201002016 has been created for tracking purposes. KYTC will work to validate and take action on inactive/stale accounts.

COT Response: COT assumed the management of accounts in the domain in question in September of 2006. The detail findings from the auditors have been provided to the Commonwealth Service Desk for review. Some of these accounts may have been in existence prior to COT taking ownership of the account management responsibilities for this domain. The Commonwealth Service Desk is aware of the enterprise policy and accounts should not be created with password expiration exceeding 31 days without the appropriate approvals. All actions taken on accounts in this domain are taken at the specific request of KYTC. KYTC should work with COT to remediate the issues identified by the auditors in the detail findings.

COT currently employs a process to review stale accounts located in the enterprise Active Directory Forest. The domain in question resides outside of the enterprise Active Directory Forest and therefore is not included in this process. KYTC is currently working with COT to make considerable changes to this domain but these efforts are in the early planning phase and no completion date has been defined at this time. These changes may allow the ability to include all or some of these accounts in the COT review processes in the future. All actions taken on accounts in this domain are taken at the specific request of KYTC. KYTC should work with COT to address the potentially stale accounts identified by the auditors in the detail findings.

THIS PAGE LEFT BLANK INTENTIONALLY

APPENDIX

**COMMONWEALTH OF KENTUCKY
APPENDIX
FOR THE YEAR ENDED JUNE 30, 2010**

This report is available on our website, www.auditor.ky.gov in PDF format. For other requests, please contact Gregory Giesler, APA's Open Records Administrator, at (502) 564-5841 or gregory.giesler@auditor.ky.gov. If copies of the CAFR for FY 10 are required, please contact Jonathan Miller, Finance and Administration Cabinet Secretary, at (502) 564-4240 or jonathan.miller@ky.gov.

The list includes agencies receiving financial statement audits by Certified Public Accounting firms (CPA) used for preparing the Commonwealth's CAFR. CPA reports are available upon request to the respective agency.

Bluegrass State Skills Corporation
Capital Plaza Tower
500 Mero Street
Frankfort, Kentucky 40601

Turnpike Authority of Kentucky
Room 78, Capitol Annex Building
Frankfort, Kentucky 40601

Kentucky Transportation Cabinet
Kentucky Transportation Cabinet Worker's Compensation
200 Mero Street
Frankfort, Kentucky 40622

Kentucky Center for the Arts
5 Riverfront Plaza
Louisville, Kentucky 40202-2989

Kentucky Economic Development Finance Authority
Capital Plaza Tower
500 Mero Street
Frankfort, Kentucky 40601

Kentucky Housing Corporation
1231 Louisville Road
Frankfort, Kentucky 40601

Kentucky Retirement Systems
Perimeter Park West
1260 Louisville Road
Frankfort, Kentucky 40601

Kentucky Teachers' Retirement System
479 Versailles Road
Frankfort, Kentucky 40601

**COMMONWEALTH OF KENTUCKY
APPENDIX
FOR THE YEAR ENDED JUNE 30, 2010
(Continued)**

University of Louisville
2301 South 3rd Street
108 Grawemeyer Hall
Louisville, Kentucky 40292

Western Kentucky University
Vice President for Finance and Administration
1 Big Red Way
Bowling Green, Kentucky 42101-3576

Murray State University
322 Sparks Hall
Murray, Kentucky 42071

Kentucky State University
Office of Administrative Affairs
400 East Main Street
Frankfort, Kentucky 40601

Kentucky Lottery Corporation
1011 West Main Street
Louisville, Kentucky 40202-2623

Kentucky State Fair Board
Kentucky Fair and Exposition Center
P.O. Box 37130
Louisville, Kentucky 40233-7130

Kentucky Educational Television Authority
600 Cooper Drive
Lexington, Kentucky 40502

Kentucky Higher Education Assistance Authority
1050 U.S. 127 South, Suite 102
Frankfort, Kentucky 40601

Kentucky Higher Education Student Loan Corporation
Financial Services Department
10180 Linn Station Road, Suite C200
Louisville, KY 40223

Kentucky Infrastructure Authority
1024 Capital Center Dr., Suite 340
Frankfort, Kentucky 40601

**COMMONWEALTH OF KENTUCKY
APPENDIX
FOR THE YEAR ENDED JUNE 30, 2010
(Continued)**

Kentucky Local Correctional Facilities Construction Authority
Suite 261 Capitol Annex
Frankfort, Kentucky 40601

Kentucky Judicial Form Retirement System
P.O. Box 791
Frankfort, Kentucky 40602

University of Kentucky
301 Peterson Service Building
Lexington, Kentucky 40506-0005

Eastern Kentucky University
Vice President for Business Affairs
521 Lancaster Avenue
Richmond, Kentucky 40475-3101

Morehead State University
Office of Accounting and Budgetary Control
207 Howell-McDowell Administration Building
Morehead, Kentucky 40351-1689

Northern Kentucky University
Office of Business Affairs
Lucas Administration Center
726 Nunn Drive
Highland Heights, Kentucky 41099-8101

Kentucky Community and Technical College System
300 North Main Street
Versailles, KY 40383

Kentucky Council on Postsecondary Education
1024 Capital Center Drive, Suite 320
Frankfort, Kentucky 40601

Office of the Petroleum Storage Tank
Environmental Assurance Fund
81 C. Michael Davenport Boulevard
Frankfort, KY 40601

Kentucky Public Employees' Deferred Compensation Authority
101 Sea Hero Road, Suite 110
Frankfort, KY 40601-5404

**COMMONWEALTH OF KENTUCKY
APPENDIX
FOR THE YEAR ENDED JUNE 30, 2010
(Continued)**

Workers' Compensation Program
State Office Building, 3rd Floor
501 High Street
Frankfort, KY 40601

Kentucky Department of Labor - Special Fund
1047 US Highway 127 S, Suite 4
Frankfort, KY 40601

Kentucky Horse Park Foundation
4089 Iron Works Parkway
Lexington, Kentucky 40511

