



CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS

February 21, 2008

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, 2007. Beginning this year, our Statewide Single Audit of the Commonwealth of Kentucky report will be transmitted in two volumes in order to meet new reporting guidelines for financial statement findings established by the American Institute of Certified Public Accountants. 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 cursive script that reads "Crit Luallen".

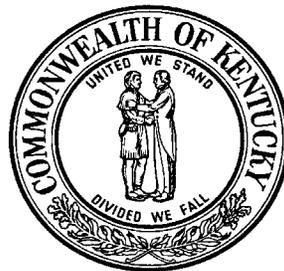
Crit Luallen
Auditor of Public Accounts



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

VOLUME I

**For the Year Ended
June 30, 2007**



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

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

The Statewide Single Audit of the Commonwealth of Kentucky
Volume I
For the Year Ended June 30, 2007

Background

The Single Audit Act of 1984, subsequent amendments, and corresponding regulations, requires an 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 *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). Beginning in FY 2007 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 Question 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;
- 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, 2007**

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 ending June 30, 2007, the total federal dollars expended by the Commonwealth of Kentucky was \$ 6,971,431,072. For fiscal year 2007, the total federal dollars expended as reported on the SEFA decreased in comparison with the total for June 30, 2006, but this difference is due to the exclusion of component units previously reported as noted below.

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 under 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. It should be noted that 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 federal expenditures.

CONTENTS

	Page
List of Abbreviations/Acronyms	1
Independent Auditor’s Report	7
Schedule of Expenditures of Federal Awards:	
U.S. Office of National Drug Control Policy	11
U.S. Department of Agriculture.....	11
U.S. Department of Commerce	12
U.S. Department of Defense	12
U.S. Department of Housing and Urban Development	12
U.S. Department of the Interior	12
U.S. Department of Justice	13
U.S. Department of Labor	14
U.S. Department of Transportation	15
U.S. Department of Treasury.....	16
U.S. Appalachian Regional Commission	16
U.S. Equal Employment Opportunity Commission	16
U.S. General Services Administration.....	17
U.S. National Aeronautics and Space Administration.....	17
U.S. National Foundation on the Arts and the Humanities	17
U.S. Department of Veterans Affairs	17
U.S. Environmental Protection Agency.....	17
U.S. Department of Energy	18
U.S. Department of Education.....	18
U.S. National Archives and Records Administration.....	20
U.S. Election Assistance Commission.....	20
U.S. Department of Health and Human Services	20
U.S. Corporation for National and Community Service.....	23
U.S. Social Security Administration.....	23
U.S. Department of Homeland Security	23
Other Federal Assistance	24
Notes To The Schedule Of Expenditures Of Federal Awards	25
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	39
Financial Statement Findings	
<i>Material Weaknesses Relating to Internal Controls</i>	
FINDING 07-KST-1: The Kentucky State Treasury Should Reconcile Commonwealth Bank Accounts With eMARS In A Timely Manner.....	45
FINDING 07-REV-2: The Department of Revenue Should Improve Procedures Over The Preparation Of The Closing Package To Ensure Financial Statement Data Is Free Of Material Misstatement.....	47

CONTENTS
(Continued)

Page

Financial Statement Findings (Continued)

Significant Deficiencies Relating to Internal Controls

FINDING 07-CHFS-3: The Cabinet For Health And Family Services Should Strengthen The Security Of System Accounts	49
FINDING 07-CHFS-4: The Cabinet For Health and Family Services Should Ensure Adequate Security Is In Place Over Microsoft Outlook Public Folders	51
FINDING 07-CHFS-5: The Cabinet For Health And Family Services Should Review Supporting Documentation To Ensure Accuracy Of The Closing Package	54
FINDING 07-CHFS-6: The Cabinet For Health And Family Services Should Ensure Agency Policies Are Followed For Approval Of Leave And Overtime	55
FINDING 07-CHFS-7: The Cabinet For Health And Family Services Should Improve Its System For Tracking Payments Made On Contracts.....	57
FINDING 07-DMA-8: The Department Of Military Affairs Should Institute Controls To Prevent Material Errors To The Schedule Of Expenditures Of Federal Awards.....	59
FINDING 07-DWI-9: The Department For Workforce Investment Should Ensure Adequate Review Of The Closing Package	64
FINDING 07-EDU-10: The Kentucky Department Of Education Should Implement A Comprehensive Information Technology Policy And Ensure Adequate Oversight Authority Is Established	65
FINDING 07-EDU-11: The Kentucky Department Of Education’s Office Of District Support Services Should Update And Consistently Apply Its Change Management Process	68
FINDING 07-EDU-12: The Kentucky Department of Education’s Office Of Education Technology Should Formalize And Consistently Apply Logical Security Policies For The KETS Network And MUNIS	71
FINDING 07-EDU-13: The Kentucky Department Of Education’s Office Of District Support Services Should Formalize And Consistently Apply Its Logical Security Policies	75
FINDING 07-EDU-14: The Kentucky Department Of Education’s Office Of District Support Services Should Ensure Proper Segregation Of Duties	78
FINDING 07-EDU-15: The Kentucky Department Of Education Should Ensure That Security Information Leakage For Agency Computer Devices Is Minimized	80
FINDING 07-FAC-16: The Finance And Administration Cabinet Should Formalize And Consistently Apply Logical Security Procedures For ePayment Gateway	82
FINDING 07-FAC-17: The Finance And Administration Cabinet Should Ensure All Reporting From InfoAdvantage Is Accurate And Complete	84
FINDING 07-FAC-18: The Finance And Administration Cabinet Should Develop And Implement Formal Policy And Procedures To Govern The Security Of The eMARS Checkwriter Interface Process.....	88

CONTENTS
(Continued)

	Page
Financial Statement Findings (Continued)	
<i>Significant Deficiencies Relating to Internal Controls (Continued)</i>	
FINDING 07-FAC-19: The Finance And Administration Cabinet Should Strengthen, Formalize, And Consistently Apply Error Handling Procedures For Interface Files	90
FINDING 07-FAC-20: The Finance And Administration Cabinet Should Ensure eMARS Production Cycles Are Monitored And Logged, And That Sufficient Policies And Procedures Are Implemented To Govern eMARS Operations	93
FINDING 07-FAC-21: The Finance And Administration Cabinet Should Formalize Procedures Governing System Assurance Processing	96
FINDING 07-FAC-22: The Finance And Administration Cabinet Should Develop And Implement Formal Policy And Procedures To Govern The Security Of The eMARS Production Databases	100
FINDING 07-FAC-23: The Finance And Administration Cabinet’s Password Policy Should Be Consistently Applied To All eMARS Production Databases.....	103
FINDING 07-FAC-24: The Finance And Administration Cabinet Should Strengthen Input Validation Controls Over eMARS Machines	105
FINDING 07-FAC-25: The Finance And Administration Cabinet Should Improve Logical Security Over The UNIX Servers	106
FINDING 07-FAC-26: The Finance And Administration Cabinet Should Strengthen System Assurance Procedures Between Production And The Data Warehouse	111
FINDING 07-FAC-27: The Finance And Administration Cabinet Should Develop And Formalize Guidance Concerning Approval Rules Related To The eMARS Applications.....	113
FINDING 07-FAC-28: The Finance And Administration Cabinet Should Strengthen The Controls Over The Payee Vendor Field.....	115
FINDING 07-FAC-29: The Finance And Administration Cabinet Should Ensure eMARS Fixed Assets Are Converted Completely And Accurately.....	117
FINDING 07-FAC-30: The Finance And Administration Cabinet Should Develop And Implement A Policy Governing The Security Of Microsoft Outlook Public Folders	118
FINDING 07-FAC-31: The Finance And Administration Cabinet Should Monitor Contracts To Ensure Vendor Compliance With Terms Specified In The Contract	121
FINDING 07-FAC-32: The Finance And Administration Cabinet Should Ensure Contracts Are Not Improperly Extended Beyond The Renewal Periods Specified In The Original Contract.....	128
FINDING 07-FAC-33: The Finance And Administration Cabinet Should Improve Procedures Related To The Entity Removal Process Related To The CAFR Compilation	131

CONTENTS
(Continued)

	Page
Financial Statement Findings (Continued)	
<i>Significant Deficiencies Relating to Internal Controls (Continued)</i>	
FINDING 07-FAC-34: The Finance And Administration Cabinet Should Strengthen Policies And Procedures Related To Approvals and Tracking Of State-Owned Take Home Vehicles.....	133
FINDING 07-KOHS-35: The Kentucky Office Of Homeland Security Should Improve Controls Over The Preparation Of The Schedule Of Expenditures Of Federal Awards.....	136
FINDING 07-KST-36: The Kentucky State Treasury Should Segregate Duties Within The Cash Receipts Function And The Computer Application Access/Modification Processes	139
FINDING 07-KST-37: The Kentucky State Treasury And The Finance And Administration Cabinet Should Implement Internal Controls Over The Approval Process To Prevent Users From Bypassing Approvals On Transactions Within eMARS	142
FINDING 07-KST-38: The Kentucky State Treasury Should Improve Internal Controls Over The Processing Of NSF Documents	148
FINDING 07-OFM-39: The Office Of Financial Management Should Formalize And Consistently Apply The Program Modification Process	152
FINDING 07-OFM-40: The Office Of Financial Management Should Strengthen Logical Security Controls Over Investment Data And Resources	156
FINDING 07-OFM-41: The Office Of Financial Management Should Improve Segregation Of Duty Controls	159
FINDING 07-OFM-42: The Office Of Financial Management Should Ensure Contracts Are Recorded On The Appropriate eMARS Documents And All Payments Are Attributed To Those Documents.....	161
FINDING 07-REV-43: The Department Of Revenue Should Ensure Access To Production Libraries Is Limited	163
FINDING 07-REV-44: The Department of Revenue Should Ensure KY-OSCAR Access Forms Are Properly Completed	165
FINDING 07-REV-45: The Department of Revenue Should Work With COT To Strengthen Controls Governing Data Processing Of Taxpayer Accounts	167
FINDING 07-REV-46: The Department of Revenue Should Ensure All Agency Web Servers Have Updated Software And Security Patches Installed.....	169
FINDING 07-REV-47: The Department of Revenue Should Strengthen The Security Of System Accounts.....	171
FINDING 07-REV-48: The Department of Revenue Should Disable The Simple Network Management Protocol Service On All Machines	172
FINDING 07-REV-49: The Department of Revenue Should Comply With KRS 131.175 And End The Practice Of Waiving Interest Due	173

CONTENTS
(Continued)

	Page
Financial Statement Findings (Continued)	
<i>Significant Deficiencies Relating to Internal Controls (Continued)</i>	
FINDING 07-REV-50: The Department of Revenue And Office Of State Budget Director Should Ensure Tax Receipts Belonging To County Governments Are Properly Accounted For In The Fiduciary Fund At Year End	175
FINDING 07-REV-51: The Department of Revenue Should Exercise Care To Assure Returns And Other Significant Documents Are Neither Lost Nor Destroyed	178
FINDING 07-REV-52: The Department of Revenue Should Ensure Refunds And Distributions Are Properly Coded Within eMARS.....	181
FINDING 07-REV-53: The Department of Revenue Should Improve Security Arrangements During Processing And Ensure Existing Procedures Are Followed	183
FINDING 07-REV-54: The Department of Revenue Should Strengthen Its Cash Handling Procedures And Ensure Employees In All Divisions Comply	185
FINDING 07-TC-55: The Kentucky Transportation Cabinet Should Adhere To Established Procedures Governing System Access Request For The Transportation Information Payroll System.....	187
FINDING 07-TC-56: The Kentucky Transportation Cabinet Should Ensure Security Information Leakage For Agency Computer Devices Is Minimized	190
FINDING 07-TC-57: The Kentucky Transportation Cabinet Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose	193
FINDING 07-TC-58: The Kentucky Transportation Cabinet Should Ensure Management Is Aware Of Hiring Policies And Identify Penalties For Noncompliance.....	198
FINDING 07-TC-59: The Kentucky Transportation Cabinet Should Implement Formal Policies And Procedures Regarding Inventory Purchased With A Procurement Card.....	202
FINDING 07-TC-60: The Kentucky Transportation Cabinet Should Strengthen Inventory Controls To Ensure Proper Precautions Are Taken To Safeguard Assets.....	204
FINDING 07-TC-61: The Kentucky Transportation Cabinet Should Improve Procedures For Maintenance Materials	206
FINDING 07-TC-62: The Kentucky Transportation Cabinet Should Ensure Management Is Aware Of Equipment Purchase Procedures And Implement Procedures For Noncompliance	211
FINDING 07-TC-63: The Kentucky Transportation Cabinet Should Ensure Proper Approvals Are Constantly Applied	215
FINDING 07-TC-64: The Kentucky Transportation Cabinet Should Implement a Policy Or Written Procedures Regarding Capitalized Cost	217
FINDING 07-TC-65: The Kentucky Transportation Cabinet Should Ensure That Bridge Inspections Be Performed In A Timely Manner	219

CONTENTS
(Continued)

	Page
Financial Statement Findings (Continued)	
<i>Significant Deficiencies Relating to Internal Controls (Continued)</i>	
FINDING 07-DOC-66: The Department Of Corrections Should Ensure All DOC Gateway Routers Managed By The Commonwealth Office Of Technology Are Properly Configured And Maintained	225
FINDING 07-DOC-67: The Department Of Corrections Should Ensure Anonymous FTP Access To Agency Machines Is Disabled.....	227
FINDING 07-DOC-68: The Department Of Corrections Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose	229
FINDING 07-DOC-69: The Department Of Corrections Should Develop And Implement A System Development Life Cycle Policy To Govern System Development, Testing, Modifications And Implementation.....	235
FINDING 07-DOC-70: The Department of Corrections Should Develop And Implement A Policy Governing The Security Of Microsoft Outlook Public Folders	239
FINDING 07-PERS-71: The Personnel Cabinet Should Strengthen The Security Of System Accounts	242
FINDING 07-PERS-72: The Personnel Cabinet Should Disable The Simple Network Management Protocol Service On All Machines	244
FINDING 07-PERS-73: The Personnel Cabinet Should Adhere To Established Procedures Governing System Access Requests For The Uniform Payroll And Personnel System.....	245
FINDING 07-PERS-74: The Personnel Cabinet Should Ensure That Formal Program Modification Control Procedures Are Consistently Followed To Properly Control Changes To The Uniform Personnel And Payroll System	247
FINDING 07-FAC-75: The Finance And Administration Cabinet Should Establish Controls Over Specific Purchase Order Documents To Ensure Contract Amounts Are Not Exceeded.....	250
Appendix.....	255

LIST OF ABBREVIATIONS/ACRONYMS

**COMMONWEALTH OF KENTUCKY
LIST OF ABBREVIATIONS/ACRONYMS
FOR THE YEAR ENDED JUNE 30, 2007**

AASHTO	American Association of State Highway and Transportation Officials
ABS	Accounting Based Spending
AFR	Annual Financial Reporting
AGR	Department of Agriculture
AIDS	Acquired Immunodeficiency Virus Syndrome
AMLR	Abandoned Mine Land Reclamation
AOC	Administrative Office of the Courts
APA	Auditor of Public Accounts
ATF	Bureau of Alcohol, Tobacco, Firearms and Explosives
BBALI	Balance Sheet Account
BMS	Bridge Management System
BOWD	Business Opportunity and Workforce Development
BSA	Balance Sheet Account
BZPP	Buffer Zone Protection Plan
CAB	Change Management Advisory
CAFR	Comprehensive Annual Financial Report
CAMRA	Complete Asset Management Reporting and Accounting
CAPSSSE	Community Assistance Program State Support Services Element
CARS	Compliance and Receivable System
CBALQ	Cash Balance
CDC	Centers of Disease Control
CDP	Custom Data Processing
CED	Cabinet for Economic Development
CFDA	Catalog of Federal Domestic Assistance
CFR	Code of Federal Regulations
CHFS	Cabinet for Health and Family Services
CICS	Customer Information Control System
CIM	Compaq Information Manager
CIO	Chief Information Officer
CMS	Centers for Medicare and Medicaid Services
CO	Controller's Office
COA	Chart of Accounts
Commonwealth	Commonwealth of Kentucky
COPS	Computer Oracle and Password System
CORR	Department of Corrections
COT	Commonwealth Office of Technology
CPA	Certified Public Accountant
CPU	Central Processing Unit
CR	Cash Receipt
CRC	Cyclical Redundancy Check
CRC	Customer Resource Center
CSD	Carbonated Soft Drink
CSO	Centralized Security Officer
CT	Contract

**COMMONWEALTH OF KENTUCKY
LIST OF ABBREVIATIONS/ACRONYMS
FOR THE YEAR ENDED JUNE 30, 2007
(Continued)**

CTS	Comprehensive Tax System
CW	Checkwriter
DBA	Database Administrator
DEM	Division of Employee Management
DCJT	Department of Criminal Justice Training
DISRQ	Disbursement Request Table
DLA	Department of Libraries and Archives
DMA	Department of Military Affairs
DMS	Department for Medicaid Services
DNS	Domain Name Server
DO	Delivery Order
DOC	Department of Corrections
DOC	Document
DOR	Department of Revenue
DOS	Denial of Service
DSU	Data Service Unit
DTOC	Document Control
DVOP	Disabled Veterans' Outreach Program
DW	Date Warehouse
DWI	Department for Workforce Investment
EDU	Department of Education
EFT	Electronic Funds Transfer
eMARS	enhanced Management Administrative Reporting System
EPA	Environmental Protection Agency
ePAY	ePayment Gateway
EPPC	Environmental and Public Protection Cabinet
EPSB	Education Professional Standards Board
ETV	Education and Training Vouchers
F&W	Department of Fish and Wildlife Resources
FAC	Finance and Administration Cabinet
FAP	Finance and Administration Policy
FFY	Federal Fiscal Year
FHWA	Federal Highway Administration
FIBALCQ	Fund Balance
FICA	Federal Insurance Contributions Act
Finance	Finance and Administration Cabinet
FMB	Financial Management Branch
FMNP	Farmers' Market Nutritional Program
FSC	Forward Schedule of Changes
FTP	File Transfer Protocol
FY	Fiscal Year
GAAP	Generally Accepted Accounting Principles
GASB	Governmental Accounting Standards Board

**COMMONWEALTH OF KENTUCKY
LIST OF ABBREVIATIONS/ACRONYMS
FOR THE YEAR ENDED JUNE 30, 2007
(Continued)**

GAX	General Accounting Expense/Expenditure
GAX2	General Accounting Revenue Refund
GAX3	General Accounting Balance Sheet Payable
GOLD	Governors Office for Local Development
GOPM	Governors Office for Policy & Management
HDR	Header
HIDTA	Highway Intensity Drug Trafficking Areas
HIPPA	Health Insurance Portability and Accountability Act
HIV	Human Immunodeficiency Virus
HRC	Kentucky Commission on Human Rights
HTML	Hyper Text Markup Language
HTTP	Hyper Text Transfer Protocol
IAS	Internal Audit and Security
ID	Identification
IN	Invoice
INTIDS	Interface Identification Setup
IP	Internet Protocol
IRS	Internal Revenue Service
IT	Information Technology
JCL	Job Control Language
JUST	Justice and Public Safety Cabinet
JUV	Department of Juvenile Justice
JVA	Advanced Journal Voucher
KAC	Kentucky Arts Council
KAR	Kentucky Administrative Regulations
KBE	State Board of Elections
KBIS	Kentucky Bridge Information System
KCHIP	Kentucky Children's Health Insurance Program
KD&A	Knowledge Development and Application
KDE	Kentucky Department of Education
KETS	Kentucky Education Technology System
KHC	Kentucky Heritage Council
KHEAA	Kentucky Higher Education Assistance Authority
KHS	Kentucky Historical Society
KIH	Kentucky Information Highway
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 Treasurer
KVE	Kentucky Vehicle Enforcement
KY-OSCAR	Kentucky's On-Line System for Collection of Accounts Receivables

**COMMONWEALTH OF KENTUCKY
LIST OF ABBREVIATIONS/ACRONYMS
FOR THE YEAR ENDED JUNE 30, 2007
(Continued)**

KYTC	Kentucky Transportation Cabinet
LAN	Local Area Network
LP	Limited Partnership
LRC	Legislative Research Commission
MA	Master Agreement
MARS	Management Administrative Reporting System
MD	Manual Disbursement
MIL	Military Affairs
MIXERS	Miscellaneous Taxes Registration System
MOA	Memorandum of Agreement
MRDB	Management Reporting Database
MUNIS	Municipal Users Network Information System
MVU	Motor Vehicle Usage
NA	Not Applicable
NBI	National Bridge Inventory
NBIS	National Bridge Inspection Standards
NCHIP	National Criminal History Improvement Program
NetBIOS	Network Basic Input Output System
NFS	Network File Sharing
NSF	Non-Sufficient Funds
O&M	Operations and Management
OAG	Office of Attorney General
ODSS	Office of District Support Services
OET	Office of Education Technology
OFM	Office of Financial Management
OHRM	Office of Human Resource Management
OIG	Office of Inspector General
OIT	Office of Information Technology
OMA	Office of Management and Administration
OMB	Office of Management and Budget
OMPS	Office of Materials and Procurement Services
OMS	Operations Management System
OPS	Office of Procurement Services
ORION	Offender Records Information Operations Network
OSBD	Office of State Budget Director
PARKS	Department of Parks
PATH	Projects for Assistance in Transition from Homelessness
PCR	Program Change Request
PDC	Primary Domain Controller
PDF	Portable Document Format
PDI	Pervasive Data Integrator
PDM	Pre-Disaster Mitigation
PE	Performance Evaluation

**COMMONWEALTH OF KENTUCKY
LIST OF ABBREVIATIONS/ACRONYMS
FOR THE YEAR ENDED JUNE 30, 2007
(Continued)**

PERS	Personnel Cabinet
PO	Purchase Order
PON	Proof Of Necessity
POP3	Post Office Protocol - Version 3
PPCMS	Probation and Parole Case Management System
PR	Purchase Request
PR	Payment Request
PRC	Commodity Based Purchase Request
PRCI	Commodity Based Internal Purchase Request
PRC2	Commodity Based Purchase Request ProCard
PUBAD	Department of Public Advocacy
QC/QA	Quality Control/Quality Assurance
R&D	Research and Development
REV	Department of Revenue
RFC	Request for Change
RFP	Request for Proposal
RPC	Unix Sun Remote Procedure Call
SA	System Assurance
SAM	Security Accounts Manager
SAS	Statewide Accounting Services
SDLC	System Development Life Cycle
SED	Serious Emotional Disturbances
SEEK	Support Education Excellence in Kentucky
SEFA	Schedule of Expenditures of Federal Awards
SFY	State Fiscal Year
SMTP	Simple Mail Transfer Protocol
SMS	Microsoft Systems Management Server
SNMP	Simple Network Management Protocol
SP	Standard Password
SQL	Standard Query Language
SSH	Secured Shell
SSN	Social Security Number
SSWAK	Statewide Single Audit of Kentucky
STOL	System Tolerance
SUID	Set User Identification
TC	Transportation Cabinet
TCP	Transmission Control Protocol
Telecom	Telecommunications Tax
TIPS	Transportation Information Payroll System
TP	Travel Payments
TPC	Technology Planning Council
TSCA	Toxic Substances Control Act
UGRI	Utility Gross Receipts License Tax

**COMMONWEALTH OF KENTUCKY
LIST OF ABBREVIATIONS/ACRONYMS
FOR THE YEAR ENDED JUNE 30, 2007
(Continued)**

UI	Unemployment Insurance
UID	User Identification
UNIX	Uniplexed Information and Computing System
UofL	University of Louisville
UPPS	Uniform Personnel and Payroll System
UPS	Unified Prosecutorial System
US	United States
USDA	United States Department Of Agriculture
VA	Department of Veterans' Affairs
VNC	Virtual Network Computing
WIA	Workforce Investment Act
XML	Extensive Mark-up Language



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, 2007, and have issued our report thereon dated December 18, 2007. 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, based on our audit and the reports of other auditors, 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 cursive script that reads "Crit Luallen".

Crit Luallen
Auditor of Public Accounts

December 18, 2007



SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS

COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. Office of National Drug Control Policy</u>					
Direct Program:					
07.NA(1)	HIDTA Program	KSP	\$ 786,420	\$	\$
07.NA(2)	Other Federal Assistance (Note 15)	KVE			
Total U.S. Office of National Drug Control Policy			\$ 786,420	\$	\$
<u>U.S. Department of Agriculture</u>					
Direct Programs:					
10.025	Plant and Animal Disease, Pest Control, and Animal Care (Note 10)	AGR	\$ 708,932	\$	\$
		F&W	68,702		
10.028	Wildlife Services (Note 10)	F&W	10,238		
10.069	Conservation Reserve Program	EPPC	5,318		
10.153	Market News	AGR	4,606		
10.156	Federal- State Marketing Improvement Program	AGR	58,782		
10.163	Market Protection and Promotion	AGR	84,383		
Food Stamp Cluster:					
10.551	Food Stamps (Note 2) (Note 14)	CHFS		671,445,934	
10.561	State Administrative Matching Grants for Food Stamp Program (Note 2)	CHFS	27,619,379		778,138
Child Nutrition Cluster:					
10.553	School Breakfast Program (Note 2)	EDU	46,305,690		46,232,284
		JUV	458,706		
10.555	National School Lunch Program (Note 2)	EDU	134,629,061		134,497,514
		JUV	794,592		
10.556	Special Milk Program for Children (Note 2)	EDU	79,590		79,590
10.559	Summer Food Service Program for Children (Note 2)	EDU	9,748,747		9,328,543
10.550	Food Donation (Note 14)	AGR		17,429,759	
10.557	Special Supplemental Nutrition Program for Women, Infants, and Children (Note 2)	CHFS	111,634,564		17,943,844
10.558	Child and Adult Care Food Program (Note 2)	EDU	28,306,984		27,610,964
10.560	State Administrative Expenses for Child Nutrition	EDU	2,173,823		7,720
		AGR	232,413		
10.565	Commodity Supplemental Food Program (Note 14) (Note 16)	AGR	844,812	2,563,211	
Emergency Food Assistance Cluster:					
10.568	Emergency Food Assistance Program (Administrative Costs)	AGR	810,243		
10.569	Emergency Food Assistance Program (Food Commodities) (Note 14)	AGR		3,046,192	
10.572	WIC Farmers' Market Nutrition Program (FMNP)	AGR	220,396		
10.574	Team Nutrition Grants	EDU	37,291		21,600
10.576	Senior Farmers Market Nutrition Program	AGR	335,906		
10.652	Forestry Research	EPPC	389,070		
10.664	Cooperative Forestry Assistance (Note 14)	EPPC	2,650,820	140,705	820,783
10.672	Rural Development, Forestry, and Communities	EPPC	48		
10.676	Forest Legacy Program	EPPC	2,187,533		
10.680	Forest Health Protection	EPPC	154,974		10,000
10.769	Rural Business Enterprise Grants	AGR	27,144		

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(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	EPPC	899,677		
		F&W	291,982		
10.912	Environmental Quality Incentives Program (Note 15)	EPPC			
10.913	Farm and Ranch Lands Protection Program (Note 15)	AGR			
10.914	Wildlife Habitat Incentive Program (Note 14)	F&W		17,499	
10.NA(1)	Rural Rehabilitation Student Loan Program (Note 3)	AGR	111,931		
Total U.S. Department of Agriculture			<u>\$ 371,886,337</u>	<u>\$ 694,643,300</u>	<u>\$ 237,330,980</u>
<u>U.S. Department of Commerce</u>					
Direct Programs:					
Public Works and Economic Development Cluster:					
11.307	Economic Adjustment Assistance	GOLD	\$ 186,875	\$	\$
11.469	Congressionally Identified Awards and Projects (Note 15)	PARKS DWI			
Total U.S. Department of Commerce			<u>\$ 186,875</u>	<u>\$</u>	<u>\$ 0</u>
<u>U.S. Department of Defense</u>					
Direct Programs:					
12.002	Procurement Technical Assistance For Business Firms	CED	\$ 141,861	\$	\$
12.113	State Memorandum of Agreement Program for the Reimbursement of Technical Services	EPPC	220,744		
12.400	Military Construction, National Guard	MIL	7,217,245		
12.401	National Guard Military Operations and Maintenance (O & M) Projects	MIL	13,617,713		
12.404	National Guard Civilian Youth Opportunities	MIL	1,862,145		
12.NA(1)	Chemical Demilitarization and Remediation Activity for Hazardous Waste Activities at Chemical Demilitarization Facilities	EPPC	228,067		14,451
12.NA(2)	Monitoring of Wildlife	F&W	219,663		
12.NA(3)	Teacher and Teacher's Aide Placement Assistance Program	EPSB	58,800		
Total U.S. Department of Defense			<u>\$ 23,566,238</u>	<u>\$</u>	<u>\$ 14,451</u>
<u>U.S. Department of Housing and Urban Development</u>					
Direct Programs:					
14.228	Community Development Block Grants/State's Program(Note 2) (Note 11)	GOLD	\$ 31,695,102	\$	\$ 31,231,978
14.401	Fair Housing Assistance Program-State and Local	HRC	78,307		
Total U.S. Department of Housing and Urban Development			<u>\$ 31,773,409</u>	<u>\$</u>	<u>\$ 31,231,978</u>
<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 14)	EPPC	\$ 12,226,011	\$ 33,589	\$ 50,960

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. Department of the Interior (Continued)</u>					
Direct Programs (Continued):					
15.252	Abandoned Mine Land Reclamation (AMLR) Program	EPPC	15,123,352		3,662,704
Fish and Wildlife Cluster:					
15.605	Sport Fish Restoration (Note 10)	F&W	3,696,227		
15.611	Wildlife Restoration (Note 12)	F&W	4,183,135		
15.614	Coastal Wetlands Planning, Protection and Restoration Act	F&W	42,672		
15.615	Cooperative Endangered Species Conservation Fund (Note 10)	F&W	151,935		
		EPPC	83,067		6,000
15.616	Clean Vessel Act	F&W	62,377		
15.622	Sportfishing and Boating Safety Act	F&W	385,297		
15.623	North American Wetlands Conservation Fund (Note 15)	EPPC			
15.632	Conservation Grants Private Stewardship for Imperiled Species	F&W	21,668		
		EPPC	7,001		
15.633	Landowner Incentive	F&W	323,876		
		EPPC	159,850		
15.634	State Wildlife Grants (Note 10)	F&W	403,143		
15.808	U.S. Geological Survey-Research and Data Collection (Note 15)	COT			
15.904	Historic Preservation Fund Grants-In-Aid	KHC	749,636		102,679
15.916	Outdoor Recreation-Acquisition, Development and Planning (Note 8) (Note 15)	GOLD PARKS	1,117,376		1,117,375
Total U.S. Department of the Interior			<u>\$ 38,736,623</u>	<u>\$ 33,589</u>	<u>\$ 4,939,718</u>
<u>U.S. Department of Justice</u>					
Direct Programs:					
16.003	Law Enforcement Assistance-Narcotics and Dangerous Drugs Technical Laboratory Publications (Note 15)	COT	\$	\$	\$
16.203	Comprehensive Approaches to Sex Offender Management Discretionary Grant (Note 15)	CORR JUST	1,606		
16.523	Juvenile Accountability Incentive Block Grants (Note 15)	JUV UPS AOC PUBAD	1,044,592 33,333 9,019		51,129
16.540	Juvenile Justice and Delinquency Prevention-Allocation to States	JUV	668,428		534,414
16.541	Part E-Developing, Testing and Demonstrating Promising New Programs	AOC	2,000		
16.543	Missing Children's Assistance	KSP	232,448		
16.548	Title V-Delinquency Prevention Program	JUV	4,120		3,291
16.549	Part E-State Challenge Activities	JUV	5,133		5,133
16.550	State Justice Statistics Program for Statistical Analysis Centers	JUST	13,319		13,319
16.554	National Criminal History Improvement Program (NCHIP) (Note 15)	JUST KOHS			
16.560	National Institute of Justice Research, Evaluation, and Development Project Grants	KSP JUST	624,486 10,934		
16.575	Crime Victim Assistance	JUST UPS	5,211,882 280,334		5,058,511
16.576	Crime Victim Compensation	EPPC	1,272,111		
16.579	Edward Byrne Memorial Formula Grant Program (Note 15)	JUST KSP CORR AOC	705,868 405,967 325,855 2,601		564,314

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. Department of Justice (Continued)</u>					
Direct Programs (Continued):					
16.579	Edward Byrne Memorial Formula Grant Program (Note 15)	JUV PUBAD			
16.580	Edward Byrne Memorial State and Local Law Enforcement Assistance Discretionary Grants Program (Note 15)	AOC	1,350,497		
		JUST KSP PUBAD	200,000 199,717		
16.585	Drug Court Discretionary Grant Program (Note 10)	AOC	529,297		
16.586	Violent Offender Incarceration and Truth in Sentencing Incentive Grants (Note 15)	CORR JUV			379,856
		JUST	4,658		
16.588	Violence Against Women Formula Grants	JUST	1,855,471		1,653,939
		UPS CHFS OAG	185,072 73,779 69,965		
16.589	Rural Domestic Violence and Child Victimization Enforcement Grant Program	JUST	121,581		121,581
16.592	Local Law Enforcement Block Grants Program (Note 15)	KSP JUST	3,007		
		KVE			
16.593	Residential Substance Abuse Treatment for State Prisoners (Note 15)	CORR JUST	237,020		
16.606	State Criminal Alien Assistance Program (Note 15)	CORR			
16.607	Bulletproof Vest Partnership Program (Note 15)	CORR JUST	9,619		
		UPS			
16.609	Community Prosecution and Project Safe Neighborhoods (Note 15)	COT			
16.610	Regional Information Sharing Systems (Note 15)	AOC	38,592		
16.710	Public Safety Partnership and Community Policing Grants (Note 15)	KSP OAG	25,845		
		KSP	377,249		
16.727	Enforcing Underage Drinking Laws Program	TC			
16.728	Drug Prevention Program (Note 15)	CORR	368,672		
16.735	Protecting Inmates and Safeguarding Communities Discretionary Grant Program				
16.738	Edward Byrne Memorial Justice Assistance Grant Program	JUST	2,284,554		2,113,717
		KSP AOC UPS KVE	624,260 148,141 29,981 3,133		
16.NA(1)	Drug Enforcement Administration	KSP	1,046,965		
16.NA(2)	Federal Bureau of Investigation	KSP	54,213		
16.NA(3)	Federal Methamphetamine Initiative (Note 15)	KSP			
16.NA(4)	Bureau of Alcohol, Tobacco, Firearms & Explosives (ATF) Program	KSP	6,364		
16.NA(5)	Prescription Drug Monitoring Program	CHFS	359,849		
16.NA(6)	District Fugitive Task Force	KSP	3,615		
Total U.S. Department of Justice			\$ 21,880,970	\$	\$ 10,499,204
<u>U.S. Department of Labor</u>					
Direct Programs:					
17.002	Labor Force Statistics	DWI	\$ 940,033	\$	\$
17.005	Compensation and Working Conditions	EPPC	148,763		

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. Department of Labor (Continued)</u>					
Direct Programs (Continued):					
Employment Services Cluster:					
17.207	Employment Service/Wagner-Peyser Funded Activities	DWI	10,741,067		
17.272	Permanent Labor Certification for Foreign Workers	DWI	217,499		
17.801	Disabled Veterans' Outreach Program (DVOP)	DWI	782,884		
17.804	Local Veterans' Employment Representative Program	DWI	1,506,601		
17.225	Unemployment Insurance (Note 2) (Note 6)	DWI	431,924,652		100,253
17.235	Senior Community Service Employment Program	CHFS	1,571,327		657,704
17.245	Trade Adjustment Assistance (Note 2)	DWI	24,967,159		6,398,085
Workforce Investment Act Cluster:					
17.258	WIA Adult Program (Note 2)	DWI	13,548,616		12,940,530
17.259	WIA Youth Activities (Note 2)	DWI MIL	13,065,156		12,282,910
		EDU	372,163		322,329
17.260	WIA Dislocated Workers (Note 2)	DWI EDU	15,022,128 375,000		13,092,802 374,410
17.261	WIA Pilots, Demonstrations, and Research Projects	DWI	50,089		50,089
17.267	Incentive Grants-WIA Section 503 (Note 15)	DWI MIL	118,624		103,668
17.503	Occupational Safety and Health-State Program	EPPC	3,160,390		
17.504	Consultation Agreements	EPPC	26,955		
17.600	Mine Health and Safety Grants	EPPC	606,088		
17.601	Mine Health and Safety Counseling and Technical Assistance	EPPC	132,338		
Total U.S. Department of Labor			\$ 519,277,532	\$	\$ 46,322,780
<u>U.S. Department of Transportation</u>					
Direct Programs:					
Air Transportation Cluster:					
20.106	Airport Improvement Program	TC PARKS	\$ 176,428 24,184	\$	\$
Highway Planning and Construction Cluster:					
20.205	Highway Planning and Construction (Note 2) (Note 7) (Note 15)	TC PARKS	642,853,312		
20.218	National Motor Carrier Safety	KVE TC KSP	4,617,257 750,131 104,596		155,676
20.219	Recreational Trails Program (Note 8)	GOLD PARKS	807,385 6,941		780,109
20.232	Commercial Driver License State Programs (Note 15)	TC			
20.505	Federal Transit-Metropolitan Planning Grants	TC	825,191		825,191
Federal Transit Cluster:					
20.500	Federal Transit-Capital Investment Grants	TC	14,771,510		14,771,510
20.507	Federal Transit-Formula Grants	TC	681,497		681,497

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. Department of Transportation (Continued)</u>					
Direct Programs (Continued):					
20.509	Formula Grants for Other Than Urbanized Areas	TC	11,352,092		10,768,387
20.513	Capital Assistance Program for Elderly Persons and Persons with Disabilities	TC	1,775,663		1,768,440
20.514	Public Transportation Research	TC	45,000		10,000
20.516	Job Access Reverse Commute	TC	76,334		76,334
Highway Safety Cluster:					
20.600	State and Community Highway Safety (Note 5)	KSP	5,673,504		2,250,880
		DCJT	84,158		
		OAG	43,811		
		KVE	9,802		
		TC	8,000		
		AOC	98		
20.601	Alcohol Traffic Safety and Drunk Driving Prevention Incentive Grant(Note 15)	TC			
20.604	Safety Incentive Grants for Use of Seatbelts (Note 15)	KVE	27,739		
		KSP			
20.605	Safety Incentives to Prevent Operation of Motor Vehicles by Intoxicated Persons (Note 15)	TC			
20.700	Pipeline Safety	EPPC	185,708		
20.703	Interagency Hazardous Materials Public Sector Training and Planning Grants	MIL	106,006		
Total U.S. Department of Transportation			\$ 685,006,347	\$	\$ 32,088,024
<u>U.S. Department of Treasury</u>					
Direct Programs:					
21.NA(1)	Internal Revenue Service	KSP	\$ 24,002	\$	\$
Total U.S. Department of Treasury			\$ 24,002	\$	\$
<u>U.S. Appalachian Regional Commission</u>					
Direct Programs:					
23.002	Appalachian Area Development (Note 15)	GOLD	\$	\$	\$
23.011	Appalachian Research, Technical Assistance, and Demonstration Projects	GOLD	498,454		433,770
Total U.S. Appalachian Regional Commission			\$ 498,454	\$	\$ 433,770
<u>U.S. Equal Employment Opportunity Commission</u>					
Direct Programs:					
30.002	Employment Discrimination-State and Local Fair Employment Practices Agency Contracts	HRC	\$ 214,194	\$	\$
Total U.S. Equal Employment Opportunity Commission			\$ 214,194	\$	\$

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. General Services Administration</u>					
Direct Programs:					
39.003	Donation of Federal Surplus Personal Property (Note 14)	FAC	\$	\$ 599,325	\$
39.011	Election Reform Payments (Note 17)	KBE	23,300		
Total U.S. General Services Administration			\$ 23,300	\$ 599,325	\$
<u>National Aeronautics and Space Administration</u>					
Direct Programs:					
43.002	Technology Transfer	COT	\$ 222,273	\$	\$
Total National Aeronautics and Space Administration			\$ 222,273	\$	\$
<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 (Note 15)	KHS KAC	\$ 25,000	\$	\$
45.025	Promotion of the Arts-Partnership Agreements (Note 15)	KAC KHS	612,118		
45.026	Promotion of the Arts-Leadership Initiatives (Note 15)	KAC			
45.161	Promotion of the Humanities-Research	HRC	1,500		
45.310	Grants to States	DLA	2,635,636		872,323
Total U.S. National Foundation on the Arts and Humanities			\$ 3,274,254	\$	\$ 872,323
<u>U.S. Department of Veterans Affairs</u>					
Direct Programs:					
64.005	Grants to States for Construction of State Home Facilities	VA	\$ 59,359	\$	\$
64.203	State Cemetery Grants	VA	6,715,080		
Total U.S. Department of Veterans Affairs			\$ 6,774,439	\$	\$
<u>U.S. Environmental Protection Agency</u>					
Direct Programs:					
66.001	Air Pollution Control Program Support	EPPC	\$ 1,595,228	\$	\$
66.032	State Indoor Radon Grants	CHFS	486,847		373,539
66.034	Surveys, Studies, Investigations, Demonstrations and Special Purpose Activities Relating to the Clean Air Act (Note 14)	EPPC	684,796	177,597	
66.418	Construction Grants for Wastewater Treatment Works	EPPC	275,824		
66.419	Water Pollution Control State, Interstate, and Tribal Program Support (Note 14)	EPPC	1,761,614	15,488	214,234
66.432	State Public Water System Supervision	EPPC	916,412		
66.436	Surveys, Studies, Investigations, Demonstrations, and Training Grants and Cooperative Agreements-Section 104(B)(3) of the Clean Water Act	EPPC	3,448		
66.454	Water Quality Management Planning	EPPC	164,469		113,204
66.458	Capitalization Grants for Clean Water State Revolving Funds	EPPC	290,949		
66.460	Nonpoint Source Implementation Grants	EPPC	3,619,446		2,244,478
66.461	Regional Wetland Program Development Grants	EPPC	68,335		
66.463	Water Quality Cooperative Agreements	EPPC	18,586		18,586
66.467	Wastewater Operator Training Grant Program (Technical Assistance)	EPPC	26,504		
66.468	Capitalization Grants for Drinking Water State Revolving Funds	EPPC	1,999,423		

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. Environmental Protection Agency (Continued)</u>					
Direct Programs (Continued):					
66.471	State Grants to Reimburse Operators of Small Water Systems for Training and Certification Costs	EPPC	113,849		
66.474	Water Protection Grants to the States	EPPC	33,348		
66.606	Surveys, Studies, Investigations and Special Purpose Grants (Note 15)	EPPC			
66.608	Environmental Information Exchange Network Grant Program and Related Assistance (Note 14)	COT	380,416		
		EPPC	40,931	12,000	
66.700	Consolidated Pesticide Enforcement Cooperative Agreements	AGR	599,796		
66.701	Toxic Substances Compliance Monitoring Cooperative Agreements	EPPC	118,286		
66.707	TSCA Title IV State Lead Grants Certification of Lead-Based Paint Professionals	CHFS	247,919		
66.708	Pollution Prevention Grants Program	EPPC	66,945		44,870
66.801	Hazardous Waste Management State Program Support	EPPC	1,779,711		
66.802	Superfund State, Political Subdivision, and Indian Tribe Site-Specific Cooperative Agreements	EPPC	100,428		
66.804	State and Tribal Underground Storage Tanks Program	EPPC	188,400		
66.805	Leaking Underground Storage Tank Trust Fund Program	EPPC	2,070,776		
66.808	Solid Waste Management Assistance Grants	EPPC	17,033		
66.809	Superfund State and Indian Tribe Core Program-Cooperative Agreements	EPPC	142,129		
66.817	State and Tribal Response Program Grants	EPPC	822,677		
66.940	Environmental Policy and State Innovation Grants	EPPC	79,058		
Total U.S. Environmental Protection Agency			<u>\$ 18,713,583</u>	<u>\$ 205,085</u>	<u>\$ 3,008,911</u>
<u>U.S. Department of Energy</u>					
Direct Programs:					
81.039	National Energy Information Center (Note 4)(Note 15)	KOEP EPPC	\$ 8,155	\$	\$
81.041	State Energy Program (Note 4)(Note 15)	KOEP EPPC	487,708		243,569
81.042	Weatherization Assistance for Low-Income Persons	CHFS	4,955,939		4,361,292
81.086	Conservation Research and Development (Note 15)	EPPC			
81.104	Office of Environmental Cleanup and Acceleration	EPPC	44,892		777
81.117	Energy Efficiency and Renewable Energy Information Dissemination, Outreach, Training and Technical Analysis/Assistance (Note 15)	EPPC			
81.119	State Energy Program Special Projects (Note 4)(Note 15)	KOEP EPPC	56,007		56,007
81.502	Paducah Gaseous Diffusion Plant Environmental Monitoring and Oversight	EPPC CHFS	1,103,457 529,925		112,060 216,084
81.NA(1)	Department of Energy	F&W	67,231		
Total U.S. Department of Energy			<u>\$ 7,253,314</u>	<u>\$</u>	<u>\$ 4,989,789</u>
<u>U.S. Department of Education</u>					
Direct Programs:					
84.010	Title I Grants to Local Educational Agencies (Note 2)	EDU	\$ 184,449,118	\$	\$ 182,473,228
84.011	Migrant Education - State Grant Program	EDU	6,534,261		6,437,285
84.013	Title I Program for Neglected and Delinquent Children	JUV CORR	944,315 17,656		477,640

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Education(Continued)					
Direct Programs (Continued):					
Special Education Cluster:					
84.027	Special Education - Grants to States (Note 2)	EDU	151,156,876		148,458,833
84.173	Special Education - Preschool Grants (Note 2)	EDU	10,773,905		10,241,402
84.048	Vocational Education-Basic Grants to States	DWI EDU EPSB	11,561,945 6,795,955 300,000		8,641,187 6,407,992
84.126	Rehabilitation Services-Vocational Rehabilitation Grants to States (Note 2)	DWI	50,726,920		1,270,755
84.128	Rehabilitation Services-Service Projects (Note 15)	DWI			
84.161	Rehabilitation Services-Client Assistance Program	DWI	132,369		
84.169	Independent Living-State Grants	DWI	109,172		34,171
84.177	Rehabilitation Services-Independent Living Services for Older Individuals Who are Blind	DWI	408,987		
84.181	Special Education-Grants for Infants and Families with Disabilities	CHFS	2,625,765		
84.184	Safe and Drug-Free Schools and Communities-National Programs(Note 15)	EDU			
84.186	Safe and Drug-Free Schools and Communities-State Grants	EDU CHFS	4,920,795 1,178,355		4,589,668 1,173,153
84.187	Supported Employment Services for Individuals with Severe Disabilities	DWI	145,324		
84.196	Education for Homeless Children and Youth	EDU	1,169,489		1,169,489
84.213	Even Start - State Educational Agencies	EDU	1,793,803		1,711,978
84.215	Fund for the Improvement of Education (Note 15)	KHS EDU			
84.224	Assistive Technology	DWI	722,794		521,551
84.240	Program of Protection and Advocacy of Individual Rights	PUBAD	208,304		
84.243	Tech-Prep Education	DWI	1,777,613		1,729,854
84.265	Rehabilitation Training-State Vocational Rehabilitation Unit In-Service Training	DWI	230,848		37,046
84.281	Eisenhower Professional Development State Grants (Note 15)	EDU			
84.287	Twenty-First Century Community Learning Centers	EDU	12,321,079		12,263,462
84.298	State Grants for Innovative Programs (Note 15)	EDU	1,777,673		1,746,540
84.318	Education Technology State Grants	EDU	6,436,357		5,832,251
84.323	Special Education-State Personnel Development	EDU	1,613,045		1,511,939
84.326	Special Education - Technical Assistance and Dissemination to Improve Services and Results for Children with Disabilities	EDU	69,969		69,969
84.327	Special Education - Technology and Media Services for Individuals with Disabilities(Note 15)	EDU			
84.330	Advanced Placement Program	EDU	487,006		264,755
84.331	Grants to States for Incarcerated Youth Offenders	CORR	161,149		
84.332	Comprehensive School Reform Demonstration	EDU	3,132,587		3,001,283
84.336	Teacher Quality Enhancement Grants	EPSB	2,158,122		
84.343	Assistive Technology - State Grants for Protection and Advocacy	PUBAD	71,373		
84.346	Vocational Education-Occupational and Employment Information State Grants	DWI	66,425		1,911
84.350	Transition to Teaching	EDU	198,983		156,646
84.352	School Renovation Grants (Note 15)	EDU			
84.357	Reading First State Grants	EDU	16,569,592		14,754,714
84.358	Rural Education	EDU	5,652,766		5,640,266
84.365	English Language Acquisition Grants	EDU	2,527,744		2,444,215
84.366	Mathematics and Science Partnerships	EDU	2,602,440		2,197,199
84.367	Improving Teacher Quality State Grants (Note 2)	EDU	43,979,214		43,314,053

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
<u>U.S. Department of Education (Continued)</u>					
Direct Programs (Continued):					
84.369	Grants for State Assessments and Related Activities	EDU	5,382,261		217,669
84.372	Statewide Data Systems	EDU	374,769		
84.938	Hurricane Education Recovery	EDU	999,654		992,844
Passed Through From the Harlan Independent Board of Education:					
84.215	Fund for the Improvement of Education Pass Through Grantor # - Various (Note 13)	KHS	313,416		
Passed Through From the Letcher County Board of Education:					
84.215	Fund for the Improvement of Education Pass Through Grantor # - Various (Note 13)	KHS	337,408		
Passed Through From Bowling Green State University:					
84.304	Civic Education-Cooperative Education Exchange Program Pass Through Grantor # - Q304B040001 (Note 13)	AOC	8,987		
Passed Through From the Center for Civic Education:					
84.929	We the People Pass Through Grantor # - Various (Note 13)	AOC	77,317		
Total U.S. Department of Education			<u>\$ 546,003,905</u>	<u>\$</u>	<u>\$ 469,784,948</u>
<u>U.S. National Archives and Records Administration</u>					
Direct Programs:					
89.003	National Historical Publications and Records Grants	DLA	\$ 3,526	\$	\$
		KHS	73,840		
Total U.S. National Archives and Records Administration			<u>\$ 77,366</u>	<u>\$</u>	<u>\$</u>
<u>U.S. Election Assistance Commission</u>					
Direct Programs:					
90.401	Help America Vote Act Requirements Payments	KBE	\$ 34,412	\$	\$
Total U.S. Election Assistance Commission			<u>\$ 34,412</u>	<u>\$</u>	<u>\$</u>
<u>U.S. Department of Health and Human Services</u>					
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	70,832		29,700
93.042	Special Programs for the Aging - Title VII, Chapter 2 - Long Term Care Ombudsman Services for Older Individuals	CHFS	204,044		51,816
93.043	Special Programs for the Aging - Title III, Part D - Disease Prevention and Health Promotion Services	CHFS	283,417		228,138
Aging Cluster:					
93.044	Special Programs for the Aging - Title III, Part B - Grants for Supportive Services and Senior Centers	CHFS	4,554,398		2,113,278
93.045	Special Programs for the Aging - Title III, Part C - Nutrition Services	CHFS	6,471,202		2,857,363

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Health and Human Services (Continued)					
Direct Programs (Continued):					
93.053	Nutrition Services Incentive Program	CHFS	1,864,505		891,156
93.048	Special Programs for the Aging-Title IV-and Title II-Discretionary Projects	CHFS	305,682		
93.051	Alzheimer's Disease Demonstration Grants to States	CHFS	254,062		243,561
93.052	National Family Caregiver Support	CHFS	1,772,135		728,450
93.103	Food and Drug Administration-Research	CHFS	3,300		
93.104	Comprehensive Community Mental Health Services for Children with Serious Emotional Disturbances (SED) (Note 15)	CHFS			
93.110	Maternal and Child Health Federal Consolidated Programs	CHFS	287,107		242,141
93.116	Project Grants and Cooperative Agreements for Tuberculosis Control Programs (Note 14)	CHFS	1,081,822	94,127	735,831
93.130	Cooperative Agreements to States/Territories for the Coordination and Development of Primary Care Offices	CHFS	58,131		27,820
93.134	Grants to Increase Organ Donations	CHFS	113,271		112,397
93.136	Injury Prevention and Control Research and State and Community Based Programs	CHFS	2,241,443		25,277
93.138	Protection and Advocacy for Individuals with Mental Illness	PUBAD	485,014		
93.150	Projects for Assistance In Transition from Homelessness (PATH)	CHFS	388,000		388,000
93.197	Childhood Lead Poisoning Prevention Projects - State and Local Childhood Lead Poisoning Prevention and Surveillance of Blood Lead Levels in Children	CHFS	464,313		402,987
93.217	Family Planning - Services	CHFS	5,948,106		5,449,115
93.230	Consolidated Knowledge Development and Application (KD&A) Program (Note 15)	CHFS			
93.234	Traumatic Brain Injury State Demonstration Grant Program	CHFS	75,486		
93.235	Abstinence Education Program	CHFS			
93.238	Cooperative Agreements for State Treatment Outcomes and Performance Pilot Studies Enhancement	CHFS	939,359		884,486
93.242	Mental Health Research Grants	CHFS	21,208		
93.243	Substance Abuse and Mental Health Services-Projects of Regional and National Significance (Note 15)	CHFS	3,532,423		3,136,399
		AOC	147,538		
		JUV	6,589		
		EDU	4,293		
		JUST			
93.251	Universal Newborn Hearing Screening (Note 15)	CHFS			
93.262	Occupational Safety and Health Program	CHFS	210,111		
93.267	State Grants for Protection and Advocacy Services	PUBAD	52,160		
93.268	Immunization Grants (Note 2) (Note 14)	CHFS	3,008,824	17,963,122	1,813,275
93.276	Drug-Free Communities Support Program Grants	KVE	16,656		
93.283	Centers for Disease Control and Prevention-Investigations and Technical Assistance (Note 14)	CHFS	18,905,451	184,885	13,528,016
		MIL	5,902		
93.556	Promoting Safe and Stable Families	CHFS	7,445,248		3,147,833
93.558	Temporary Assistance for Needy Families (Note 2)(Note 15)	CHFS	117,861,180		13,926,259
		DWI	1,823,112		
93.563	Child Support Enforcement (Note 2)	CHFS	40,545,361		24,052,284
		OAG	152,460		
93.568	Low-Income Home Energy Assistance (Note 2)	CHFS	40,509,298		39,834,439
93.569	Community Services Block Grant	CHFS	10,512,367		4,353,353
93.571	Community Services Block Grant Formula and Discretionary Awards	CHFS	14,902		14,902
	Community Food and Nutrition Programs				

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Health and Human Services(Continued)					
Direct Programs (Continued):					
Child Care Cluster:					
93.575	Child Care and Development Block Grant (Note 2)	CHFS	97,323,246		516,380
93.596	Child Care Mandatory and Matching Funds of the Child Care and Development Fund (Note 2)	CHFS	36,738,079		7,629,207
93.576	Refugee and Entrant Assistance - Discretionary Grants (Note 15)	EDU			
93.585	Empowerment Zones Program (Note 15)	FAC			
93.586	State Court Improvement Program	AOC	458,298		
93.590	Community-Based Child Abuse Prevention Grants	CHFS	2,585,787		1,276,494
93.597	Grants to States for Access and Visitation Programs	CHFS	89,510		86,412
93.599	Chafee Education and Training Vouchers Program (ETV)	CHFS	408,195		
93.600	Head Start	EDU	152,298		5,000
93.603	Adoption Incentive Payments	CHFS	1,840,000		
93.617	Voting Access for Individuals with Disabilities-Grants To States	KBE	69,064		69,064
93.618	Voting Access for Individuals with Disabilities-Grants for Protection and Advocacy Systems	PUBAD	96,721		
93.630	Developmental Disabilities Basic Support and Advocacy Grants	CHFS	1,238,776		374,225
		PUBAD	685,759		
		DWI	16,242		
93.643	Children's Justice Grants to States (Note 10)	AOC	191,950		
		OAG	30,615		
		CHFS	28,148		
93.645	Child Welfare Services-State Grants	CHFS	4,393,296		
93.647	Social Services Research and Demonstration (Note 15)	CHFS			
93.658	Foster Care-Title IV-E (Note 2)	CHFS	55,494,552		
		JUV	2,021,793		
		AOC	284,600		
93.659	Adoption Assistance (Note 2)	CHFS	26,106,261		
93.667	Social Services Block Grant (Note 2)	CHFS	17,138,752		168,784
		JUV	7,570,000		
93.669	Child Abuse and Neglect State Grants	CHFS	553,883		12,407
93.671	Family Violence Prevention and Services/Grants for Battered Women's Shelters/Grants to State and Indian Tribes	CHFS	1,332,214		1,197,167
93.674	Chafee Foster Care Independence Program	CHFS	1,358,991		505,480
93.767	State Children's Insurance Program (Note 2)	CHFS	79,346,259		91,622
Medicaid Cluster:					
93.775	State Medicaid Fraud Control Units (Note 2)	OAG	2,106,847		
93.777	State Survey and Certification of Health Care Providers and Suppliers (Note 2)	CHFS	6,747,503		
93.778	Medical Assistance Program (Note 2) (Note 15)	CHFS	3,210,753,101		1,953,965
93.779	Centers for Medicare and Medicaid Services (CMS) Research, Demonstration and Evaluations	CHFS	750,254		338,667
93.781	Seed Grants to States for Qualified High-Risk Pools (Note 15)	EPPC			
93.889	National Bioterrorism Hospital Preparedness Program	CHFS	7,201,545		6,097,741
		MIL	221,195		
93.917	HIV Care Formula Grants	CHFS	6,783,286		2,353,371
93.938	Cooperative Agreements to Support Comprehensive School Health Programs to Prevent the Spread of HIV and Other Important Health Problems	EDU	536,910		466,099
		CHFS	119,568		20,667
93.940	HIV Prevention Activities - Health Department Based (Note 14)	CHFS	2,026,089	11,900	1,568,349

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U.S. Department of Health and Human Services(Continued)					
Direct Programs (Continued):					
93.944	Human Immunodeficiency Virus (HIV)/Acquired Immunodeficiency Virus Syndrome (AIDS) Surveillance	CHFS	100,848		28,601
93.945	Assistance Programs for Chronic Disease Prevention and Control	CHFS	439,365		320,722
93.958	Block Grants for Community Mental Health Services	CHFS	5,626,869		5,625,241
		DWI	63,500		30,000
		CORR	52,000		
93.959	Block Grants for Prevention and Treatment of Substance Abuse (Note 2)	CHFS	21,133,870		20,716,846
		KSP	45,406		
		JUST			
93.977	Preventive Health Services - Sexually Transmitted Diseases Control Grants (Note 14)	CHFS	1,018,632	244,449	226,404
93.988	Cooperative Agreements for State-Based Diabetes Control Programs and Evaluation of Surveillance Systems	CHFS	680,057		624,105
93.991	Preventive Health and Health Services Block Grant	CHFS	1,197,808		976,874
93.994	Maternal and Child Health Services Block Grant to the States	CHFS	12,560,912		8,305,117
Total U.S. Department of Health and Human Services			\$ 3,890,359,566	\$ 18,498,483	\$ 180,803,287
U.S. Corporation for National and Community Service					
Direct Programs:					
94.003	State Commissions	CHFS	\$ 193,425	\$	\$
94.004	Learn and Serve America-School and Community Based Programs	EDU	252,312		234,250
94.006	AmeriCorps	CHFS	2,141,574		2,139,459
94.007	Planning and Program Development Grants	CHFS	60,936		
94.009	Training and Technical Assistance	CHFS	115,362		
Foster Grandparents/Senior Companion Cluster:					
94.011	Foster Grandparent Program	CHFS	562,398		86,226
94.NA(1)	Clinical Laboratory Improvement Act	CHFS	180,891		
Total U.S. Corporation for National and Community Service			\$ 3,506,898	\$	\$ 2,459,935
U.S. Social Security Administration					
Direct Programs:					
Disability Insurance/SSI Cluster:					
96.001	Social Security-Disability Insurance (Note 2)	CHFS	\$ 38,157,972	\$	\$
96.009	Social Security State Grants for Work Incentive Assistance to Disabled Beneficiaries	PUBAD	138,438		
Total U.S. Social Security Administration			\$ 38,296,410	\$	\$
U. S. Department of Homeland Security					
Direct Programs:					
Homeland Security Cluster:					
97.004	State Domestic Preparedness Equipment Support Program (Note 2) (Note 15)	KOHS	\$ 2,456,075	\$	\$ 1,865,187
		DCJT	844,341		181,386
		KSP	677,240		
		MIL	530,113		213,883
		EPPC			

**COMMONWEALTH OF KENTUCKY
SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

CFDA	Program Title	State Agency	Expenditures		Provided to Subrecipient
			Cash	Noncash	
U. S. Department of Homeland Security (Continued)					
Direct Programs (Continued):					
97.067	Homeland Security Grant Program (Note 2) (Note 15)	KOHS	12,218,004		11,011,189
		DCJT	1,559,616		321,723
		MIL	1,323,009		277,137
		KVE	998,000		
		COT	751,994		
		KSP	738,476		
		AGR	222,407		
		JUST	27,595		
		EPPC			
97.008	Urban Areas Security Initiative	KOHS	4,438,584		4,438,583
97.012	Boating Safety Financial Assistance	F&W	1,300,223		
97.017	Pre-Disaster Mitigation (PDM) Competitive Grants	MIL	26,774		26,774
97.023	Community Assistance Program State Support Services Element (CAP-SSSE)	EPPC	132,991		
97.029	Flood Mitigation Assistance (Note 15)	TC			
97.036	Disaster Grants-Public Assistance (Presidentially Declared Disasters) (Note 15)	MIL	4,399,863		4,234,709
		TC	916,529		
		PARKS	16,550		
		KSP			
97.039	Hazardous Mitigation Grant	MIL	1,702,396		1,660,181
97.040	Chemical Stockpile Emergency Preparedness Program (Note 15)	MIL	6,811,023		6,076,362
		CHFS			
97.041	National Dam Safety Program	EPPC	7,914		
97.042	Emergency Management Performance Grants (Note 15)	MIL	2,962,254		1,362,548
		KOHS			
97.045	Cooperating Technical Partners	EPPC	2,209,877		
97.047	Pre-Disaster Mitigation	MIL	74,267		74,267
97.063	Pre-Disaster Mitigation Disaster Resistant Universities (Note 15)	MIL			
97.070	Map Modernization Management Support	EPPC	201,402		67,360
97.077	Homeland Security Testing, Evaluation, and Demonstration of Technologies Related to Nuclear Detection	TC	2,552		
97.078	Buffer Zone Protection Plan (BZPP)	KSP	243,911		
		KOHS	150,601		116,928
97.089	Real ID Program	TC	128,314		
Total U.S. Department of Homeland Security			\$ 48,072,895	\$	\$ 31,928,217
Other Federal Assistance					
Direct Programs:					
NA	Joint Funding Administration (Note 9)	GOLD	\$ 1,000,000	\$	\$ 1,000,000
NA(1)	Tennessee Vally Authority	F&W	1,274		
Total Other Federal Assistance			\$ 1,001,274	\$	\$ 1,000,000
Total All State Agencies			\$ 6,257,451,290	\$ 713,979,782	\$ 1,057,708,315

COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007

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 discretely presented component units, including state Universities, and is presented primarily on the basis of cash disbursements as modified by the application of Kentucky Revised Statute (KRS) 45.229. Consequently, certain expenditures are recorded in the accounts only when cash is disbursed.

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 07. The noncash expenditures presented on this schedule represent the noncash assistance expended using the method or basis of valuation described in Note 14.

The Commonwealth has elected to exclude discretely presented component units, which are presented as part of the Commonwealth reporting entity, from the statewide single audit, except as part of the audit of the basic financial statements. Thus, discretely presented component units are not included in the accompanying Schedule of Expenditures of Federal Awards and reports on internal control and compliance. It should be noted, however, that discretely presented component units 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*.

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

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

Basis of Presentation (Continued)

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

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

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

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

- (a) Federal moneys may be received by a state agency and passed through to another state agency where the moneys are expended. Except for pass-throughs to 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 discretely presented component units report those amounts as expenditures.

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

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

Note 2 - Type A Programs

Type A programs for the Commonwealth represent any program for which total expenditures of federal awards exceeded \$20 million for FY 07. The Commonwealth had the following programs (cash and noncash) that met the Type A program threshold for FY 07, some of which were administered by more than one (1) state agency. The Commonwealth identified clusters among the Type A programs by gray shading. These Type A programs and clusters were:

CFDA	Program Title	Expenditures
Food Stamp Cluster:		
10.551	Food Stamps	\$ 671,445,934
10.561	State Administrative Matching Grants for Food Stamp Program	27,619,379
Child Nutrition Cluster:		
10.553	School Breakfast Program	46,764,396
10.555	National School Lunch Program	135,423,653
10.556	Special Milk Program for Children	79,590
10.559	Summer Food Service Program for Children	9,748,747
10.557	Special Supplemental Nutrition Program for Women, Infants, and Children	111,634,564
10.558	Child and Adult Care Food Program	28,306,984
14.228	Community Development Block Grants/State's Program	31,695,102
17.225	Unemployment Insurance	431,924,652
17.245	Trade Adjustment Assistance	24,967,159
Workforce Investment Cluster:		
17.258	WIA Adult Program	13,548,616
17.259	WIA Youth Activities	13,437,319
17.260	WIA Dislocated Workers	15,397,128
Highway Planning and Construction Cluster:		
20.205	Highway Planning and Construction	642,853,312
84.010	Title I Grants to Local Educational Agencies	184,449,118
Special Education Cluster:		
84.027	Special Education - Grants to States	151,156,876
84.173	Special Education - Preschool Grants	10,773,905

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

Note 2 - Type A Programs (Continued)

CFDA	Program Title	Expenditures
84.126	Rehabilitation Services - Vocational Rehabilitation Grants to States	50,726,920
84.367	Improving Teacher Quality State Grants	43,979,214
93.268	Immunization Grants	20,971,946
93.558	Temporary Assistance for Needy Families	119,684,292
93.563	Child Support Enforcement	40,697,821
93.568	Low-Income Home Energy Assistance	40,509,298
Child Care Cluster:		
93.575	Child Care and Development Block Grant	97,323,246
93.596	Child Care Mandatory and Matching Funds of the Child Care and Development Fund	36,738,079
93.658	Foster Care-Title IV-E	57,800,945
93.659	Adoption Assistance	26,106,261
93.667	Social Services Block Grant	24,708,752
93.767	State Children's Insurance Program	79,346,259
Medicaid Cluster:		
93.775	State Medicaid Fraud Control Units	2,106,847
93.777	State Survey and Certification of Health Care Providers and Suppliers	6,747,503
93.778	Medical Assistance Program	3,210,753,101
93.959	Block Grants for Prevention and Treatment of Substance Abuse	21,179,276
Homeland Security Cluster:		
97.004	State Domestic Preparedness Equipment Support Program	4,507,769
97.067	Homeland Security Grant Program	17,839,101
Disability Insurance/SSI Cluster:		
96.001	Social Security - Disability Insurance	38,157,972
Total Type A Programs		<u>\$ 6,491,111,036</u>

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

Note 3 - Federally Assisted Loan Program

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, 2007 was \$429,461. Student loans and investment earned interest of \$22,094. Outstanding student loans totaled \$64,466. The total grants and scholarships authorized by the USDA in FY 07 totaled \$111,930.

Note 4 - Related to CFDA 81.039, 81.041 and 81.119

The Office of Energy Policy was moved from the Commerce Cabinet to the Governors Office in October 2006.

Note 5 - Related to CFDA 20.600

The Governor's Highway Safety Program was moved from the Kentucky State Police to the Transportation Cabinet in June 2007.

Note 6 - Unemployment Insurance (CFDA 17.225)

The Commonwealth paid out \$402,596,940 in unemployment benefits in FY 07. The amounts shown on the accompanying schedule reflect both the amount expended for benefits from the Commonwealth's Unemployment Insurance Trust Fund and an additional \$29,327,712 of federal funds expended for administration of the program, resulting in a combined total of \$431,924,652 in federal expenditures.

Note 7 - Highway Planning and Construction (CFDA 20.205)

The information reported for this CFDA 20.205 Highway Planning and Construction program represents the activity of all open projects during FY 07. 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.

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

Note 7 - Highway Planning and Construction (CFDA 20.205) (Continued)

Program Income - The Highway Planning and Construction Program earned program income of \$1,331,948 in FY 07. This income was earned in the right-of-way phase through the sale and rental of real property. Income earned in this manner was classified as a negative expenditure, resulting in a reduction to federal expenditures for the current year. The Highway Planning and Construction Program also are comprised of \$4,197,428 for earned program income (interest) attributable to the Garvee Bonds. Last year this figure was inadvertently reported as \$5,893,905, rather than the actual amount of \$3,643,891.

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 \$1,444,869 for FY 07.

Note 8 - 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 9 - Joint Funding Administration

The Joint Funding Administration Program (listed in the schedule under Other Federal Assistance) consists of grants from the following federal agencies:

- U.S. Department of Commerce
- U.S. Department of Housing and Urban Development
- U.S. Appalachian Regional Commission

Note 10 - 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.

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

Note 10 - Research and Development Expenditures (Continued)

CFDA	Program Title	State Agency	Expenditures
10.025	Plant and Animal Disease, Pest Control, and Animal Care	F&W	\$ 68,702
10.028	Wildlife Services	F&W	10,238
15.605	Sport Fish Restoration	F&W	280,977
15.615	Cooperative Endangered Species Conservation Fund	F&W	117,720
15.634	State Wildlife Grants	F&W	403,143
16.585	Drug Court Discretionary Grant Program	AOC	40,315
93.643	Children's Justice Grants to States	AOC	<u>43,076</u>
Total Research and Development Expenditures			<u>\$ 964,171</u>

Note 11 - Community Development Block Grants/State's Program (CFDA 14.228)

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

Note 12 - 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 grant (CFDA 15.611) 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.

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

Note 13 - 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>			
Harlan Independent Board of Education	Pass Through (Various)	KHS	\$ 313,416
Letcher County Board of Education	Pass Through (Various)	KHS	337,408
Total Fund for the Improvement of Education			\$ 650,824
<u>Civic Education-Cooperative Education Exchange Program (CFDA 84.304)</u>			
Bowling Green State University	Pass Through (Q304B040001)	AOC	\$ 8,987
Total Civic Education - Cooperative Education Exchange Program			\$ 8,987
<u>We the People (CFDA 84.929)</u>			
Center for Civic Education	Pass Through (Various)	AOC	\$ 77,317
Total We The People			\$ 77,317

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

Note 14 - Noncash Expenditure Programs

The Commonwealth's noncash programs and a description of the method/basis of valuation follow.

CFDA	Program Title	Amount	Method/Basis of Valuation
10.550	Food Donation	\$ 17,429,759	Commodities issued per ECOS report dated 8/27/07.
10.551	Food Stamps	671,445,934	Electronic Benefit Transfer Issuance.
10.565	Commodity Supplemental Food Program	2,563,211	Quantity issued to recipients valued using April 2007 Commodity File.
10.569	Emergency Food Assistance Program (Food Commodities)	3,046,192	Quantity issued to recipients valued using April 2007 Commodity File.
10.664	Cooperative Forestry Assistance	140,705	Acquisition Cost as indicated by Government Services Administration (GSA).
10.914	Wildlife Habitat Incentive Program	17,499	Per award, \$70,000 per year, \$5,833 per month.
15.250	Regulation of Surface Coal Mining and Surface Effects of Underground Coal Mining	33,589	Inventory of Controlled Property.
39.003	Donation of Federal Surplus Personal Property	599,325	23.3% of federal acquisition cost (\$2,572,211).
66.034	Surveys, Studies, Investigations and Special Purpose Grants	177,597	EPA Contracts with Eastern Research Group, EPA contracts with Research Triangle and National Park Service and EPA contracts for performance audits and data analysis as well as actual cost of filters purchased by EPA for EPPC.

**COMMONWEALTH OF KENTUCKY
NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
FOR THE YEAR ENDED JUNE 30, 2007
(CONTINUED)**

Note 14 - Noncash Expenditure Programs (Continued)

CFDA	Program Title	Amount	Method/Basis of Valuation
66.419	Water Pollution Control Program	15,488	An estimated hourly rate for months: November, December and February.
66.608	Environmental Information Exchange Network Grant Program and Related Assistance	12,000	Work completed by EPA Contractor.
93.116	Project Grants and Cooperative Agreements for Tuberculosis Control Programs	94,127	Per authorized award for personnel.
93.268	Immunization Grants	17,963,122	Per authorized award for personnel, vaccine costs, travel, and other costs and National Immunization Program, CDC Orders Approved Report.
93.283	Centers for Disease Control and Prevention-Investigations and Technical Assistance	184,885	Per authorized award for personnel, travel, and other costs.
93.940	HIV Prevention Activities - Health Department Based	11,900	Per authorized award for personnel costs.
93.977	Preventive Health Services - Sexually Transmitted Diseases Control Grants	<u>244,449</u>	Per authorized award for personnel costs.
	Total Noncash Expenditures	<u>\$ 713,979,782</u>	

**COMMONWEALTH OF KENTUCKY
 NOTES TO THE SCHEDULE OF EXPENDITURES OF FEDERAL AWARDS
 FOR THE YEAR ENDED JUNE 30, 2007
 (CONTINUED)**

Note 15 - Zero Expenditure Programs

These programs had no expenditures related to the respective state agency during FY 07. 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 - 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 USDA Commodity File is as follows:

	<u>Commodity Supplemental Food Program CFDA 10.565</u>
Beginning Inventory, July 1, 2006	\$ 1,054,551
Received	2,424,361
Reporting Price Adjustment	6,386
Issued to Recipients	<u>(2,563,211)</u>
Ending Inventory, June 30, 2007	<u>\$ 922,087</u>

The beginning inventory has been restated from \$588,366 to the amount disclosed due to prior year errors.

Note 17 - Election Reform Payments (CFDA 39.011)

Interest earned must be used for additional program expenditures.

THIS PAGE LEFT BLANK INTENTIONALLY

REPORT ON INTERNAL CONTROL AND COMPLIANCE



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 financial statements of 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, 2007, which collectively comprise the Commonwealth's basic financial statements and have issued our report thereon dated December 18, 2007. Our report was modified to include a reference to other auditors. 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. Other auditors audited the financial statements of several agencies and activities, as described in our report of the Commonwealth's Comprehensive Annual Financial Report. This report does not include the results of the other auditors' testing of internal control over financial reporting or compliance and other matters that are reported on separately by those auditors.

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 opinions 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 would not necessarily identify all deficiencies in internal control over financial reporting that might be significant deficiencies or material weaknesses. However, as discussed below, we identified certain deficiencies in internal control over financial reporting that we consider to be significant deficiencies.



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)

A control deficiency 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 misstatements on a timely basis. A significant deficiency is a control deficiency, or combination of control deficiencies, that adversely affects the entity's ability to initiate, authorize, record, process, or report financial data reliably in accordance with generally accepted accounting principles such that there is more than a remote likelihood that a misstatement of the entity's financial statements that is more than inconsequential will not be prevented or detected by the entity's internal control over financial reporting. We consider the deficiencies described in the accompanying schedule of financial statement findings to be significant deficiencies in internal control over financial reporting, which are identified as findings 07-KST-1, 07-REV-2, 07-CHFS-3, 07-CHFS-4, 07-CHFS-5, 07-CHFS-6, 07-CHFS-7, 07-DMA-8, 07-DWI-9, 07-EDU-10, 07-EDU-11, 07-EDU-12, 07-EDU-13, 07-EDU-14, 07-EDU-15, 07-FAC-16, 07-FAC-17, 07-FAC-18, 07-FAC-19, 07-FAC-20, 07-FAC-21, 07-FAC-22, 07-FAC-23, 07-FAC-24, 07-FAC-25, 07-FAC-26, 07-FAC-27, 07-FAC-28, 07-FAC-29, 07-FAC-30, 07-FAC-31, 07-FAC-32, 07-FAC-33, 07-FAC-34, 07-KOHS-35, 07-KST-36, 07-KST-37, 07-KST-38, 07-OFM-39, 07-OFM-40, 07-OFM-41, 07-OFM-42, 07-REV-43, 07-REV-44, 07-REV-45, 07-REV-46, 07-REV-47, 07-REV-48, 07-REV-49, 07-REV-50, 07-REV-51, 07-REV-52, 07-REV-53, 07-REV-54, 07-TC-55, 07-TC-56, 07-TC-57, 07-TC-58, 07-TC-59, 07-TC-60, 07-TC-61, 07-TC-62, 07-TC-63, 07-TC-64, 07-TC-65, 07-DOC-66, 07-DOC-67, 07-DOC-68, 07-DOC-69, 07-DOC-70, 07-PERS-71, 07-PERS-72, 07-PERS-73, 07-PERS-74, and 07-FAC-75.

A material weakness is a significant deficiency, or combination of significant deficiencies, that results in more than a remote likelihood that a material misstatement of the financial statements will not be prevented or detected by the entity's internal control. Our consideration of the internal control over financial reporting was for the limited purpose described in the first paragraph of this section and would not necessarily identify all deficiencies in the internal control that might be significant deficiencies, and accordingly would not necessarily disclose all significant deficiencies that are also considered to be material weaknesses. However, of the significant deficiencies described above, we consider findings 07-KST-1 and 07-REV-2 in the accompanying schedule of financial statement findings to be material weaknesses.

Compliance and Other Matters

As part of obtaining reasonable assurance about whether the Commonwealth's financial statements for the year ended June 30, 2007, are free of material misstatement, we performed tests of its compliance with certain provisions of laws, regulations, contracts and grant agreements, noncompliance with which could have a direct and material effect on the determination of the 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 required to be reported under *Government Auditing Standards*.

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

Management's responses to the findings identified in our audit are included in the accompanying schedule of financial statement findings. We did not audit their responses and, accordingly, express no opinion on it.

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

Sincerely,

A handwritten signature in cursive script, appearing to read "Crit Luallen".

Crit Luallen
Auditor of Public Accounts

December 18, 2007

FINANCIAL STATEMENT FINDINGS

FINANCIAL STATEMENT FINDINGS

Material Weaknesses Relating to Internal Controls

FINDING 07-KST-1: The Kentucky State Treasury Should Reconcile Commonwealth Bank Accounts With 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, and the retirement of a key employee, Treasury was unable to reconcile for May and June 2006, and therefore the auditor issued a finding during the FY06 audit. Since that time, Treasury has completed partial reconciliations for the months of July, August, and September 2006 but complete reconciliations for every bank account have not been performed.

The retirement of key personnel and the implementation of eMARS in July 2006 played a significant role in Treasury not being able to reconcile. The reconciliation process had to be modified and new, customized reports had to be developed, which are time consuming processes, which delayed the reconciliation.

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. At the time of issuance for the FY 2007 CAFR, reconciliations of the bank accounts managed by the Treasury were seventeen (17) months behind.

Good internal controls dictate that state 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 take appropriate steps to ensure that daily and monthly bank reconciliations are performed timely. We understand that the Commonwealth's change in financial accounting systems from MARS to eMARS 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 FY07 and FY08 reconciliations as soon as possible. Going forward, as future accounting system changes occur, we recommend that 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.

FINANCIAL STATEMENT FINDINGS***Material Weaknesses Relating to Internal Controls*****FINDING 07-KST-1: The Kentucky State Treasury Should Reconcile Commonwealth Bank Accounts With eMARS In A Timely Manner (Continued)**

Management's Response and Corrective Action Plan

A bank reconciliation system was not included in the original eMARS program. The old system was no longer operable because the sources of the data needed for the reconciliation changed completely. Even the system experts did not know all of the sources of that data. Further complicating the problem, much of the queried data has not been accurate. It has been a source of incredible frustration for all involved in both the Treasury Department and the Finance Cabinet.

The Treasury Department has now hired on contract the eMARS Project Director to develop a new reconciliation system. He is probably the only person familiar enough with the intricacies of the eMARS system to be able to do this. The Treasury has also hired on contract a CPA who is focusing entirely on catching up the reconciliations once the new system is developed. This person worked on the MARS reconciliation team after the implementation of that system in 1999, and is extremely familiar with the process. In addition, the Controller's Office has recently sent a team of accountants to assist with the reconciliation process, some of who worked on the MARS reconciliation. In combination with the Treasury Department Accounting Division staff, this overall group brings a wealth of experience and expertise to the task at hand.

The Treasury Department feels confident that the best people available anywhere are now on the job to develop the reconciliation system and catch up the past reconciliations. Progress is being made, and is accelerating. The system is almost in place. Our goal is to have the past reconciliations caught up by spring.

This situation impacts the monthly, complete bank account reconciliation which the Treasury Department traditionally performs. The Treasury Department has been able to perform its daily reconciliations of paid checks and other vital functions. Our expectation is that most issues have been resolved on a daily basis, and that no material issues will emerge that will impact the Commonwealth's financial reporting.

FINANCIAL STATEMENT FINDINGS

Material Weaknesses Relating to Internal Controls

FINDING 07-REV-2: The Department of Revenue Should Improve Procedures Over The Preparation Of The Closing Package To Ensure Financial Statement Data Is Free Of Material Misstatement

The closing package prepared by the Department of Revenue (DOR) contained two significant errors that were not corrected prior to submission to the Finance and Administration Cabinet (FAC) for inclusion in the Commonwealth's financial statements:

- The Revenue Recognition Recap (AFR-32) reporting the General Fund (0100) accounts receivable amount was understated by \$117,457,591 and the Special Revenue Fund (1300) amount was overstated by the same amount.
- The estimated amount to be refunded reported on the AFR-32 was overstated by \$26,783,660.

In addition, one smaller error was noted in the preparation of the closing package:

- The Cash Worksheet (AFR-10) for the General Fund (0100) did not include \$156 as cash on hand for tax type 084-Unhonored Check Fees. This amount was included in the AFR-32 reconciliation and in the agency's supporting documentation.

While DOR corrected the significant errors after the auditor called attention to them, submission to FAC of closing package documents with significant errors indicates an internal control weakness.

The error in the General Fund and Special Revenue Fund accounts receivable was because tax type 076 –Omitted Tangible Property Tax-State was improperly recorded in the Special Revenue Fund. This error would have caused a material misstatement in the Special Revenue Fund accounts receivable balance had it not been detected. The estimated amount to be refunded was in error due to incorrect information being used in the calculation for this estimate. The errors indicate that the closing package forms and related worksheets prepared by DOR were not adequately reviewed to ensure the reported amounts were accurate.

Undetected, these errors would have resulted in the material overstatement of accounts receivable for the Special Revenue Fund of \$117,457,591 and understatement of General Fund accounts receivable by the same amount.

The closing package was submitted to FAC with the assertion that it was “free of material misstatement”, when in fact there were two significant errors included. Good internal controls dictate using a level of care in review of documents commensurate with their importance. Closing package schedules are incorporated into the Commonwealth of Kentucky's Comprehensive Annual Financial Statements (CAFR). The CAFR is a public document with many users, including bond rating agencies, bond analysts, policy analysts, and taxpayers. For this reason, closing package schedules are among the most important financial documents that DOR prepares. Their preparation and review deserve the utmost attention to detail.

FINANCIAL STATEMENT FINDINGS***Material Weaknesses Relating to Internal Controls*****FINDING 07-REV-2: The Department of Revenue Should Improve Procedures Over The Preparation Of The Closing Package To Ensure Financial Statement Data Is Free Of Material Misstatement (Continued)**

Recommendation

We recommend DOR update closing package procedures to include a review by an employee familiar with the closing procedures. This review should include the verification of data used to compile the closing package.

DOR should also consider making comparisons with prior year closing amounts to determine if current amounts appear reasonable.

Management's Response and Corrective Action Plan

Corrective actions have been taken to ensure future accuracy. These actions include, but are not limited to, the following:

The closing package for Accounts Receivable will be crosschecked before submission in the future and the Department of Revenue will routinely make a comparison with prior year(s) to insure accuracy and consistency. A comment has been added to the closing package instructions to insure that dollars are included in the correct fund source categories.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-CHFS-3: The Cabinet For Health And Family Services Should Strengthen The Security Of System Accounts

For security purposes, detailed information concerning the specific servers or user accounts that contributed to this finding is being intentionally omitted from this comment. However, those issues are thoroughly documented and will be sent to the appropriate agency personnel.

During the security vulnerability assessments for FY 2007 for machines controlled by the Cabinet for Health and Family Services (CHFS), our examination revealed various system user accounts with password ages that exceeded the established password policy. Additionally, we noted several accounts that had been disabled.

We obtained NetBIOS account information from one CHFS machine, which was a primary domain controller. To determine if user accounts on this machine were in compliance with established CHFS policies, the auditor used the criterion that account passwords with ages over 31 days were non-compliant. There was only one administrator account on this machine, which had been disabled and had a password age of 523 days. Furthermore, 1,975 out of 9,278 active user accounts, or 21.3 percent, had never been logged into and 511 of these user accounts (non-Guest accounts), or 5.5 percent, had a password age of 33 to 998 days. In addition, we noted eight accounts that were locked out and 2,430 accounts for which the password had expired.

Also, viewable comments associated with this machine were noted which included data that appears to be the last four digits of the user's social security number (SSN). In total, 7,609 out of 9,278 active user accounts, or 82 percent, used this identifier. Even though the CHFS Password Policy (020.305) clearly states that a user's SSN must be provided for validation purposes, this information should not be viewable through general scanning tools. If an account identifier is required then something other than the user's SSN should be used. This issue has been commented on during the past three audits.

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. Providing personal information to anonymous or unauthorized users increases liability that could occur should an unauthorized user obtain that information.

Intruders often use inactive accounts to break into a network. If an account has not been 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. An account should be deleted if it is not going to be reinstated. Personal data should not be readily available. Established password policies should be consistently applied and enforced.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-CHFS-3: The Cabinet For Health And Family Services Should Strengthen The Security Of System Accounts (Continued)

Recommendation

We recommend CHFS review all user accounts on all machines to determine which accounts are not in compliance with the established security policies. These accounts should be evaluated to determine if they are still valid accounts and are required for a business related purpose. If not, the accounts should be disabled or deleted depending on the necessity of reinstatement of the account.

In addition, the agency should ensure personal information, including social security numbers, are not used to identify an account. Even though the validation of a user's SSN is part of a formalized policy, this process poses a security risk of providing the personal information to intruders and should be re-evaluated by the agency. If possible, the information should be removed from the comment section of NetBIOS and securely maintained so that only authorized personnel have access.

Management's Response and Corrective Action Plan

With COT assistance, CHFS is reviewing all Active Directory accounts and removing those accounts that no longer have a business purpose. Although many disabled accounts are being removed, there are situations where certain CHFS business units maintain disabled accounts for legitimate business reasons. Some business units in the Cabinet are covered entities under the HIPAA legislation. Certain covered entities keep user logs and disabled domain accounts for specified time periods to maintain an audit trail. CHFS is reviewing the standards for HIPAA compliance in these areas to ensure all business units maintain the records for a common amount of time.

With regard to the last four digits of the user social security number, CHFS is moving that data field to a web database. This will remove the last four digits of the Social from the current more visible location. In the new web-based location, the user access list to this information is strictly limited to only the IT technicians needing the information for a legitimate business purpose. The database will also retain an audit trail of user access to the database.

CHFS requests that APA recognize the use of the last four digits of the social security number as an acceptable form of identification. CHFS uses the last four digits of the users' social security number (SSN) to verify the user in resets/lockouts. This is necessary to confirm a user's identity when that individual calls the helpdesk for a password reset. It is a number that is both reasonable for the user to remember while not having the same identification risks as a full social security number. If the Cabinet is required to change the composition of this identifying factor, it will weaken the ability of the helpdesk to reasonably identify the calling party to ensure authentic identity.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-CHFS-4: The Cabinet For Health and Family Services Should Ensure Adequate Security Is In Place Over Microsoft Outlook Public Folders

During FY 2007, the Auditor of Public Accounts discovered a significant security vulnerability that potentially allowed confidential and other information to be available to thousands of individuals having email access on the Commonwealth's network. This information was available by accessing agency email folders listed under the heading, "public folders." We identified five "public folders" related to the Cabinet For Health and Family Services (CHFS).

Our review of one of these CHFS public folders identified three subfolders in which either sensitive or confidential information was present. The following specific items of concern were noted:

- Three specific folders were noted containing sensitive information.
- Several instances where a calendar appointment had a Transportation Request form within an email attachment. The request form contained the child's name, date of birth, gender, and pickup and drop off locations.
- An email dated January 21, 2004, contained a spreadsheet with various specific computer addresses listed.
- Emails related to Custom Data Processing (CDP) were found within a series of subfolders. The information found within these folders relate to the program changes and budgeting process. No confidential information has been identified, but the information may be considered proprietary by CDP and the Commonwealth.

Further review of the permissions established on two of the CHFS public folders revealed that an anonymous user could alter the contents of the folder and its settings.

It was noted that agency personnel were proactively working with the Commonwealth Office of Technology (COT) to remedy the issues found within Microsoft Outlook prior to the completion of the audit.

The permissions granted to these folders could allow an individual to not only read the content of a folder, but also to potentially create, delete, or modify the content of a folder.

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.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-CHFS-4: The Cabinet For Health and Family Services Should Ensure Adequate Security Is In Place Over Microsoft Outlook Public Folders (Continued)

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 to ensure confidential information is properly secured and that any violations resulting from the inappropriate disclosure of information be reported:

- CHFS should review the CIO Enterprise Policies, such as the CIO-060 Internet and Electronic Mail Acceptable Use Policy, and ensure compliance with requirements.
- CHFS should develop a policy statement and specific procedures related to agency personnel responsibilities applicable to the security of public folders.
- Specified agency personnel should consistently review, on a regular basis, the security control permissions applied to public folders. Further the content within public folders should be reviewed to ensure that all items are appropriate.
- CHFS should report to all appropriate agencies or individuals that confidential information was potentially disclosed. Those requiring notification could include, but not be limited to:
 - Individuals whose social security numbers, health, or other personal information was accessible.
 - State or federal agencies that may require notification of the potential disclosure of confidential information.

Management’s Response and Corrective Action Plan

Upon APA notifying COT and CHFS of Exchange public folders containing sensitive information, the CHFS Cabinet took action. All permissions under the CHFS public folder tree have been reviewed so that none have Cabinet-wide permissions unless there is a specific reason. Additionally, a person in Information Security performed a manual review of all CHFS public folders to look for any containing protected information. None were found outside the ones brought to CHFS attention by APA.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-CHFS-4: The Cabinet For Health and Family Services Should Ensure Adequate Security Is In Place Over Microsoft Outlook Public Folders (Continued)**

Management's Response and Corrective Action Plan (Continued)

For those folders containing protected information, the information and/or folders have been moved. CHFS has complied with the COT directive that no confidential or sensitive information may be stored in Exchange public folders. The folder containing CDP financial information was removed by the business unit. The folder containing travel information with possible protected information has been removed with the workflow transferred to a more protected mechanism. In this case, the CHFS Office of Legal Services reviewed the situation and determined there to be no legal requirement for the Cabinet to provide notice. CHFS has also worked with the IT staff responsible for Exchange public folders setup to ensure that all public folders are locked down to only affected staff during the setup phase.

The policies and standards group within CHFS OIT has added the creation of a public folders policy to the agenda. That policy is currently in draft formation and will go through the standard CHFS policy review process.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-CHFS-5: The Cabinet For Health And Family Services Should Review Supporting Documentation To Ensure Accuracy Of The Closing Package

During our FY06 audit of accounts receivable we noted errors in the closing package. During the FY07 audit of accounts receivable, the FY06 errors were corrected; however, additional errors were noted. Specifically, CHFS:

- Reversed the federal and state percentage of the KCHIP receivable between fund 0100 and fund 1200 for agency 748.
- “Allowance for Uncollectible” was not reported on AFR-30 & 32 for Agency 736, Fund 1200 and 1400.

Errors were not discovered and resolved during the review process by CHFS. The auditor discovered the errors and CHFS submitted corrected AFR forms to the Finance and Administration Cabinet as follows:

- KCHIP receivable amount on the AFR-30 was overstated for fund 0100 and understated for fund 1200 by \$730,956.
- Department for Community Based Services “Allowance for Uncollectible” on the AFR-30 & 32 was understated by \$3,230,062 for Fund 1200 and understated by \$1,842,271 for Fund 1400.

Good internal controls dictate CHFS should ensure the information reported is accurate and reliable.

Recommendation

CHFS should:

- Reevaluate the closing package review process.
- Have knowledgeable personnel review the closing package to ensure mathematical accuracy and supporting documentation agrees to submitted AFR forms.
- Consider verifying all formulas during compilation or review of closing package forms when using Excel spreadsheets.

Management’s Response and Corrective Action Plan

The Cabinet agrees with the recommendations as suggested by the Auditor of Public Accounts. In the future, CHFS will verify all excel worksheets for formula accuracy and will also review supporting documentation to ensure accuracy of the Closing Package.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-CHFS-6: The Cabinet For Health And Family Services Should Ensure Agency Policies Are Followed For Approval Of Leave And Overtime

In our FY06 audit of the Cabinet for Health and Family Services (CHFS) payroll expenditures we noted the following concerns: timesheets did not have approval for all of the overtime or leave time taken on the accompanying leave forms. During our FY07 audit of CHFS payroll expenditures, the FY06 concerns were not corrected. As of 6/30/2007, CHFS had a total of 7,944 employees. For a predetermined pay period, we requested timesheets and supporting documentation for 60 of these employees. CHFS local offices faxed the timesheets and overtime/leave forms to the CHFS Division of Personnel Administration Branch for the auditors to review. During our FY07 audit of CHFS payroll expenditures we noted the following:

- Five (5) timesheets did not have approval for all of the leave taken on the accompanying leave forms.
- Two (2) timesheets did not have approval for all of the overtime worked.

Some employees did not include all overtime worked and or leave taken on overtime/leave forms submitted to the employee's supervisor for approval. The supervisor did not require the employee to get written approval.

Failure to include all leave time requested and/or overtime worked on the appropriate form would indicate lack of supervisor oversight. Without appropriate review, employees could report time or accrue overtime that wasn't earned. In addition, good internal controls dictate that timesheets and supporting forms should be reviewed to prevent errors in recording payroll.

According to the CHFS Employee Handbook, an employee is required to request and receive approval in advance for all compensatory time and overtime worked whenever possible. If an employee must work compensatory time or overtime and cannot receive advance approval, it must be reported to the supervisor as soon as possible after accrual. The employee must provide justification for working the compensatory time or overtime. Please keep in mind that an employee who works compensatory time or overtime without prior approval may be subject to disciplinary action.

Recommendation

CHFS should ensure all leave and overtime is being approved by supervisors. Employees should make sure to include all of their leave hours and all their overtime on the overtime/leave form submitted to their supervisor for approval. CHFS should make sure their policy regarding overtime/leave approval, stated above, is followed by all employees and their supervisors.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-CHFS-6: The Cabinet For Health And Family Services Should Ensure Agency Policies Are Followed For Approval Of Leave And Overtime (Continued)**

Management's Response and Corrective Action Plan

The managers within the Office of Human Resource Management's (OHRM) Division of Personnel Administration will remind executive leadership for their respective departments of the importance of ensuring that all leave and overtime is approved by supervisors. Even though the leave/overtime is approved by the supervisors through signing the timesheet, it is still important for it to be captured on the overtime/leave form. OHRM's management will ask that the message be conveyed to all supervisors within their respective departments.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-CHFS-7: The Cabinet For Health And Family Services Should Improve Its System For Tracking Payments Made On Contracts

During our audit of CHFS' Department for Medicaid Services (DMS), we met with various personnel and reviewed a list of contracts. It came to our attention that the contract monitoring process did not adequately track payments made on contracts. DMS enters into contracts with vendors who administer various parts of the Medicaid program. The vendors process and substantiate Medicaid claims and distribute payments to doctors, hospitals and pharmacies. More than \$5 billion is expended annually through the Medicaid program; around \$3 billion of this is Federal money, \$2 billion paid by the state of Kentucky. One specific problem noted was:

Timely Payment: Four (4) invoices totaling \$1,605,940 were paid up to three months late. This could lead to vendors deciding not to do business with the state because of the difficulty in receiving payments. Additional charges may be assessed for late payments.

The invoice payment process is not efficient; payments/invoices are not being processed within the specified 30 days, a timeframe set forth in KRS 45.453 and KRS 45.454.

Vendors were not paid in a timely manner, and payments will 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

The contract payment process has already seen improvements with the creation of an invoice committee and an update of the contract procedures. We recommend DMS continue to review and improve the contract 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 Record of Control Weakness for SFY 07 noted the Department for Medicaid Services (DMS) as having a problem with timely payment of invoices. DMS acknowledges that there was a problem and that steps were taken to correct the situation. In January 2007 DMS formed a Contract Review Committee (the Committee) as a step to ensure that contract invoices were reviewed, approved and submitted for payment in a timely manner. The Committee and the DMS Financial Management Branch (FMB) both track contract invoices. The Committee keeps a spreadsheet of invoices approved, held or rejected and the FMB keeps a spreadsheet of invoices being reviewed by the Committee and of contract payments made.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-CHFS-7: The Cabinet For Health And Family Services Should Improve Its System For Tracking Payments Made On Contracts (Continued)**

Management's Response and Corrective Action Plan (Continued)

DMS would also like to note that part of the problem recognized by the Auditors (one of the four invoices noted in the Record of Control Weakness report) was due to the delay of a contract being finalized in the eMARS system. The delay of payment to the vendor was unavoidable by DMS. The CHFS Office of Contract Oversight finalized the contract in January 2007, at which time DMS paid the outstanding invoice. Payment could not be made prior to the contract being finalized.

As stated above, the formation of the Committee and the tracking measures taken by the Committee and FMB are now in place to correct the problem of untimely payments. The FMB continues to monitor the processes now in place and will make any and all necessary adjustments to streamline or improve the process as needed.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DMA-8: The Department Of Military Affairs Should Institute Controls To Prevent Material Errors To The Schedule Of Expenditures Of Federal Awards

Internal controls used by the Department of Military Affairs (DMA) to prepare the Schedule of Expenditures of Federal Awards (SEFA) are ineffective. As a result, the SEFA submitted to the Finance and Administration Cabinet for FY 07 contained numerous errors, including a material overstatement of cash expenditures.

Problems were most widespread on the Commonwealth's SEFA schedule SEFA 2 - Schedule of Cash Programs for CFDA 12.401, National Guard Military Operations and Maintenance Projects from the U.S. Department of Defense. The following is a summary of errors noted:

- Ten 100% state-paid projects erroneously appeared in the SEFA as federal cash expenditures, overstating federal expenditures by \$4,788,023.
- An additional 25 projects with 50% state funding and one project with 25% state funding were combined on the SEFA in total as federal expenditures.
- The AYEVS project reported the cash expenditure amount under cash receipts and the cash receipt amount under cash expenditures.
- Cash receipts were incorrect for 39 projects, and cash expenditures were incorrect for 45 projects.
- Seven annual projects from federal fiscal year 2006 (AIEV6, AIFF6, AIOM6, AYGM6, AYID6, AYOM6 and AYSC6) reported zero cumulative receipts and expenditures as of 6/30/06.

The net impact of these errors was that actual cash receipts for CFDA 12.401 were \$12,880,507 but were reported as \$11,132,417; actual cash expenditures were \$13,618,014 but were reported as \$19,763,192.

For the other 17 federal grants reported in the SEFA, incorrect amounts were reported for eight of the 43 projects with cash receipts and 12 of 53 cash expenditures. The SEFA 2 for CFDA 17.259 (WIA Youth Activities from the U.S. Department of Labor) omitted \$96 paid to grantor. Project HSCE6 with cash receipts and expenditures of \$1,045,872 was omitted from the SEFA 2 for CFDA 97.067 (Homeland Security Grant Program from the U.S. Department of Homeland Security). Projects EMPG6 and EMPG7 with \$1,416,441 passed through from the Kentucky Office of Homeland Security and \$2,962,254 in cash expenditures was incorrectly reported under the grant for CFDA 97.067 instead of CFDA 97.042 (Emergency Management Performance Grants from the U.S. Department of Homeland Security). Project EMPG7 incorrectly reported \$908,122 in cash expenditures as "Other Additions" because improper setup prevented expenditures from being billed to the federal government.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DMA-8: The Department Of Military Affairs Should Institute Controls To Prevent Material Errors To The Schedule Of Expenditures Of Federal Awards (Continued)

The likely cause for many of these problems is lack of expertise with specifying criteria when generating reports from the Enhanced Management and Reporting System (eMARS). Several cash receipts amounts were inflated because, in order to capture FY 07 receipts between the end of the fiscal year and hard close on July 13, 2007, the query specified a date range of July 1, 2006 through July 13, 2007 without adding a filter to stipulate only FY07 transactions. Transactions involving the Capital Projects Fund (fund 0200) report the federal and state portions together, but the need to adjust these amounts for the federal/state split was overlooked.

Some errors on the SEFA suggest insufficient care was taken in its preparation and review. Omitting one federal project while including ten others that were 100% state-funded indicates such. To report that seven of the annual CFDA 12.401 projects for FFY06 had zero expenditures and receipts for the first nine months of the federal fiscal year is not credible.

The impact of these errors was material in relation to DMA's SEFA report. Only six of 18 SEFA 2 schedules were correct as submitted. During FY 07 the DMA expended \$40,840,206 from all federal grants, but it reported that federal expenditures were \$44,943,184, which was \$4,102,978 or 10.04% higher than actual.

The Finance and Administration Cabinet (FAC) furnished instructions on completing the SEFA to agencies that receive federal grants. Pages 10-11 of the instructions includes the following guidance:

- 1) Report on this schedule all federal awards received in the form of cash. Federal awards is defined by OMB Circular A-133 as: "...Federal financial assistance and Federal cost-reimbursement contracts that non-Federal entities receive directly from Federal awarding agencies or indirectly from pass-through entities."
- 2) Information contained in the schedule should be reconciled to infoAdvantage, an extract of eMARS. This will ensure the SEFA agrees to the official accounting records of the Commonwealth, which will have been agreed to the Commonwealth's basic financial statements.

This reconciliation should encompass both receipts and expenditures, and should be done on a grant-by-grant basis, if possible.

- 7) Columns A through L should include only the federal portion of program activity (which could occur in different funds). Do not include any state or local matching activity in these columns.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DMA-8: The Department Of Military Affairs Should Institute Controls To Prevent Material Errors To The Schedule Of Expenditures Of Federal Awards (Continued)

Recommendation

DMA should do the following to improve the reliability of its reporting in the Schedule of Expenditures of Federal Awards:

- Schedule training in infoAdvantage reporting for all personnel involved in SEFA preparation.
- Arrange for someone familiar with the CFDA 12.401 grant to participate in SEFA preparation.
- Reconcile the SEFA to infoAdvantage data.
- Review the SEFA before submitting it to the FAC. The review should be performed by one or more people who are sufficiently familiar with DMA's federal projects to be able to judge whether the report is complete and whether any state-funded projects have been improperly included.

Management's Response and Corrective Action Plan

Management's goal for the internal control process, within the Dept. of Military Affairs (DMA), is to obtain reasonable assurance that material misstatements will not occur or will be detected in a timely manner. The department's internal control objective for financial reporting is to provide reasonable assurance that reports of Federal grant awards submitted to the Federal awarding agency or pass-through entity includes all activity of the reporting period, are supported by underlying accounting or performance records, and are fairly presented in accordance with Federal grant program requirements. The department's current internal control environment, effected by executive management, establishes management's full support of ethical, efficient, and effective internal control activities and sets a positive tone for correction of identified deficiencies.

Based on the auditor's findings, DMA management has conducted an analysis of the overall risk environment currently facing the department from this finding and concurs, completely, with the auditor's internal control finding of material misstatements on DMA's SFY2007 Schedule of Expenditures of Federal Awards (SEFA).

This problem has been a continuing one for many, many years and additional resources have previously been requested in the past three biennial budget submissions as well as the current 2008-2010 Biennial Budget Request to address this very problem, but, no additional resources have been provided. Therefore, DMA's corrective action plan must now be funded from either the current additional budget request in the 2008-2010 biennial budget request or from existing assets in order to

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DMA-8: The Department Of Military Affairs Should Institute Controls To Prevent Material Errors To The Schedule Of Expenditures Of Federal Awards (Continued)

Management's Response and Corrective Action Plan (Continued)

insure that further material misstatements will not be made or will be detected and corrected in a timely manner.

The core intent of this plan is to insure that this corrective action places the right people into the right job with the right skills and the right supervision to insure that this material misstatement does not occur again.

ACTION PLAN.

Step 1 is to create a new position as Internal Auditor for the Dept. of Military Affairs. Besides the normal job duties inherent in auditing internal programs and processes, conducting risk assessments, analysis of financial and statistical records, and providing independent and objective assurance activities & training, this new position would be required to use InfoAdvantage and Business Objects (Thick Client) financial software to develop 'federal reports' for the SEFA as well as other federal quarterly financial reports that extracts data from the eMARS Cost Accounting processes in a standardized style and format. These automated reports would then act as 'source documents' in the compilation and preparation of the final SEFA report. This position would be positioned in the Office of Management and Administration which functions in an oversight capacity for all other organizations in the department and would be supervised by the current Staff Assistant in that office who is already responsible for all eMARS processes and financial management affairs, internal control, capital projects financial planning, and operating and capital budget preparation and execution for the department. The new automated reports would then be used by the department's General Accounting reporting authority to compile the SEFA and who would also reconcile the automated reports to original payment source documents to detect any additional automated report problem and then submit the draft SEFA and all validated source documents back to the internal auditor for audit and final approval. Once reviewed and validated as correct, the General Accounting reporting authority may then submit the final approved SEFA report to the Finance Cabinet and the State Auditor's Office as required by law and regulation. This Internal Auditor position would be the signatory for the 'approved by' designation on the SEFA report or, if unavailable at any given time, their supervisor, the DMA-OMA Staff Assistant, would review, approve, and sign the SEFA.

Step 2 is to create another new position as Graduate Accountant to manage and supervise all General Accounting functions, operations, activities, PROCARD administration, records custodian, and who would be the department's designated financial reporting authority for both the SEFA and the CAFR. This position would

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-DMA-8: The Department Of Military Affairs Should Institute Controls To Prevent Material Errors To The Schedule Of Expenditures Of Federal Awards (Continued)**

Management's Response and Corrective Action Plan (Continued)

supervise the existing accountants and PROCARD clerk in the General Accounting branch of the Administrative Services Division in the department and would also be required to know and utilize the specialized cost accounting processes in eMARS.

This new position would also allow this individual to review all quarterly federal grant financial reports prepared by the division level programmatic and administrative personnel prior to the final submission of the report to the federal grantor. This quarterly federal grant financial reporting is another financial reporting area in which we have had prior problems but was not particularly identified in this specific audit finding. This position would be the signatory for the 'prepared by' designation on the SEFA report.

SUMMARY. The separation of duties in the preparation of the SEFA in this action plan will allow for better internal control via a truly independent and comprehensive preparation and review and approval process. The activities of these two new positions, within the revised SEFA preparation process, will also be monitored by two separate management officials who both have a comprehensive stake in the proper functioning and maintenance of all departmental internal controls and not just those related to financial management and reporting. Also, this action plan addresses the auditor's recommendation that the review "should be performed by one or more people who are sufficiently familiar with DMA's federal projects to judge whether the report is complete". Furthermore, the new Internal Auditor position will have the time and capacity to conduct internal training on the use of InfoAdvantage and the 'feeder' reports that this position has developed for department-wide federal grant reporting as was also recommended by the auditor. Additionally, the Graduate Accountant position will have the time and capacity to conduct internal training on the use of the new 'feeder reports' for use by divisional personnel in the preparation of their quarterly federal grant reports. By utilizing the new standardized 'feeder' reports for all federal grant reporting, this action plan will also address the auditor's recommendation that all federal financial reports "reconcile to InfoAdvantage data". However, implementing this plan during the current and projected economic downturn is going to be difficult at best and no specific timeframe can be defined at this time.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DWI-9: The Department For Workforce Investment Should Ensure Adequate Review Of The Closing Package

For FY 07, DWI prepared its' closing package and submitted to FAC. We reviewed the closing package forms and noted the following issues:

- The Employer Tax Contribution receivables estimate was erroneously calculated and Accounts Receivable Tax Report (WFDIARR2) was not reliable and accurate. This overstated the balance by \$1,528,639.
- The Uncollectible Reports estimate calculation, based on 3-year average write-off, was miscalculated. This overstated the allowance for uncollectible balance by \$555,721.
- The Unemployment Insurance Benefits was transposed, understating the balance by \$566,567.
- Several other mathematical errors were noted during the audit.

DWI submitted amended closing package forms, correcting all the issues noted above by the auditor.

The closing package was not thoroughly reviewed and thus several errors were made and went unnoticed prior to the audit. The errors noted in the closing package forms resulted in misstatements to the accounts receivable amounts on the financial statements.

Good internal controls dictate that adequate review procedures should be in place to ensure the closing package contains verifiable and accurate data before submission. Proper review of the closing package could prevent errors.

Recommendation

We recommend DWI implement controls to ensure the closing package forms are prepared accurately before submission. A second review by a knowledgeable person is highly recommended in completing the closing package. The reviewer should ensure the closing package amounts are properly supported and verifiable.

Management's Response and Corrective Action Plan

1. *Procedures are in place to request up-to-date data and percentages from the Accounts Receivable Tax Report (WFDIARR2). The data used will be from the current report's run date.*
2. *DWI is in the process of identifying a person who can review closing package.*
3. *Internal Audit and Security (IAS) will review process to identify areas where verification and supporting documentation is needed.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-10: The Kentucky Department Of Education Should Implement A Comprehensive Information Technology Policy And Ensure Adequate Oversight Authority Is Established

During the audit of system controls at the Kentucky Department of Education (KDE), it was determined that no governance model or oversight authority has yet been established to ensure adequate information technology (IT) control policies and procedures are implemented to secure IT resources of the various KDE Business Units.

As was noted in the FY 2006 audit, the current KDE business approach involves various Business Units. This structure provides the Business Units with input into the IT infrastructure decisions involving its projects. Though the Office of Education Technology (OET) provides certain operating services, the ownership of the infrastructure lies with the Business Units. Along with that ownership, the traditional IT control responsibilities have also been reallocated from OET to the various Business Units.

OET creates 'guidelines' and disseminates best practice information to assist KDE Business Unit personnel with the configuration and settings related to the IT network or the implementation of new technology products. However, OET was not provided the authority to ensure business units complied with those recommendations. OET's authority extended only to its employees. Because of this structure, KDE does not have a Centralized Security Officer (CSO).

Therefore, KDE Business Units are responsible for implementing their own formal IT control polices and procedures for areas such as program change controls, logical security access controls, and disaster recovery. Based on our testing and discussions, however, Business Unit leaders have yet to establish and implement IT controls governing their Business Units. We again tested IT controls within one Business Unit responsible for the operation of Municipal Users Network Information System (MUNIS) and the Support Education Excellence in Kentucky (SEEK) systems. These were the primary systems included in the audit scope. Our testing revealed weaknesses with IT security controls for those systems. The IT security weaknesses identified with these two programs were commented on separately.

Weaknesses noted included a lack of any basic formal IT security control policies within the audited business unit responsible for these systems.

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

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-10: The Kentucky Department of Education Should Implement A Comprehensive Information Technology Policy And Ensure Adequate Oversight Authority Is Established (Continued)

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

In their response to the recommendations made during FY 2006, KDE indicated that they would have to coordinate with the new Commissioner in order to determine the appropriate model for centralized IT governance. Furthermore, KDE is in the process of formalizing several priority policies and procedures related to IT security.

Each of the business units within KDE is responsible for establishing and adhering to its own policies and procedures regarding information technology. Because of the organizational structure of KDE, business units do not report to OET. Therefore, OET cannot require the business units to comply with policies or procedures developed and implemented by this office. This situation resulted in inconsistent and incomplete controls over the KDE network and IT resources. Business units were not required to ensure they had adequate IT resources necessary for the establishment and implementation of formal IT control policies and procedures.

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

Recommendation

We recommend KDE staff continue to coordinate with the new Commissioner in order to establish an appropriate IT governance authority to design and implement standard IT controls and to provide centralized oversight of these controls for all KDE IT resources. We recommend that OET be provided the authority to develop and govern this process. If that cannot be accomplished through OET, then we recommend that

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-EDU-10: The Kentucky Department of Education Should Implement A Comprehensive Information Technology Policy And Ensure Adequate Oversight Authority Is Established (Continued)**

Recommendation (Continued)

any authority that is established for this purpose have the necessary qualifications to ensure established IT control policies and procedures are adequately designed and implemented. We recommend that management of all business units and the applicable system users be properly advised of the responsibility to comply with established IT control policies and procedures.

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

Management's Response and Corrective Action Plan

KDE agrees to coordinate internally, to discuss these recommendation(s) and to determine what further actions may be appropriate, in light of these recommendations.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-11: The Kentucky Department Of Education's Office Of District Support Services Should Update And Consistently Apply Its Change Management Process

As was noted in the FY 2006 audit of KDE system controls, ODSS has a general program change control review and approval process in place; however, KDE had not implemented a formalized procedure specific to ODSS. Further, the current process is not adequately designed to ensure that only authorized changes to key applications are made. Although progress was made toward achieving formalized change control procedures during FY 2007, this continues to be an issue.

ODSS has implemented a Project Scope Statement that documents new agency projects. In addition, a Project Portfolio is being utilized to track all outstanding and completed projects. A Technology Project Manager has been appointed with oversight responsibilities for the change control process, and a librarian has now been assigned to move ODSS changes into the production environment. A separate test server has been designated, as well as a development directory. It was also noted that two additional documents are in the process of being implemented—an application modification request and an application documentation checklist. Moreover, ODSS is in the process of creating an application that will log the request process for application changes from approval and development to user acceptance and production implementation.

Despite the improvements made with regard to the change control process, ODSS has yet to formalize change control procedures to describe the entire process. Furthermore, the current procedures, albeit not formalized, extend to new application development only and do not govern the existing ODSS programs. Additionally, there was an ODSS segregation of duties issue noted concerning this process, which was addressed in a separate comment.

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

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

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

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-11: The Kentucky Department Of Education's Office Of District Support Services Should Update And Consistently Apply Its Change Management Process (Continued)

Recommendation

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

- Develop a formal procedure for the program change control process. This formalized document should include the procedures to adequately identify program specifications and program objectives, to specifically identify changes in code by developing a code comparison listing between the original code and the revised code, to adequately test proposed program code changes, and to verify that all approvals are in place for the program code change before implementation to the production environment. If emergency situations are anticipated that might require this process to be accelerated, then that should be taken into consideration and an alternative process developed that properly applies compensating controls over that accelerated process. Since OET has recently developed a Change Management Policy and Procedure document, ODSS may be able to use this as a model in developing their policies and procedures.
- Complete implementation of the application modification request, application documentation checklist, and the ODSS applications log. The application modification request should have a tracking number so that records in the applications log can be tied to a specific request. The request form should also indicate what changes are to be made and what files/programs are involved, who is requesting the change, testing of the change, and authorization that the change was approved. This process should be included in the overall formalized procedure to ensure all employees involved with the process understand how to properly complete the form.
- Process all new programs or modifications to existing programs through the established program change control process as documented in the formal procedure.
- Ensure all changes comply with established program change control procedural requirements. Requirements should include procedures to ensure that an individual other than the programmer properly reviews and tests all changes for accuracy and that proper approvals are documented authorizing implementation of the change into production before the librarian moves the change to the production environment. After implementation of changes, the librarian should

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-EDU-11: The Kentucky Department Of Education's Office Of District Support Services Should Update And Consistently Apply Its Change Management Process (Continued)**

Recommendation (Continued)

sign and date the change request form to affirm that this process has been completed.

- Establish a centralized location for maintaining all complete change request forms.

Management's Response and Corrective Action Plan

KDE will take corrective actions to develop and implement a formal process for program change control, application modification requests and application document storage by December 31, 2007. ODSS has already implemented Visual SourceSafe as the code repository (provides version control and code comparison abilities).

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-12: The Kentucky Department of Education's Office Of Education Technology Should Formalize And Consistently Apply Logical Security Policies For The KETS Network And MUNIS

During our FY 2007 audit of KDE system controls, as was noted in the previous audit, OET had not developed or implemented a formalized security policy that identifies management and user responsibilities concerning security surrounding the Kentucky Education Technology System (KETS) network.

OET management is responsible for central workstations and servers, as well as related OET employee and contractor network access. Our audit revealed that OET had not implemented a formalized security policy to control system access by these employees and contractors, nor to control access to OET maintained servers by system users within other business units.

The school districts primarily use the MUNIS financial system to manage 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, the KYTRANSFER utility is used in order to place the files in an "outbox" located on their district MUNIS server. From there the KYCOLLECTION utility automatically collects and transports the files to KDE's MUNIS gateway server that OET manages. These reports are then moved to the file transfer protocol (FTP) server for pickup by ODSS staff.

During the course of fieldwork, we identified 12 individually assigned accounts on the FTP server. Of the 12 individually assigned accounts, there were two (2) enabled user accounts that belonged to users who were no longer employed by KDE. One of these accounts was subsequently removed, and the other account was locked; however, the latter was not disabled or removed from the server account list. We also determined there were shared accounts on the FTP and gateway servers, which were addressed in a separate comment.

We also identified five generic accounts that were locked on the FTP server and one generic account that was locked on both the FTP and gateway server that needed to be disabled or totally removed from the respective servers depending upon their future necessity. All six generic accounts identified also had access to multiple security groups on the respective servers. Moreover, we noted that all 15 disabled accounts on the gateway server and 20 of the 21 disabled accounts on the FTP server remained members of one or more security groups on the respective servers. In addition, the server support account was unnecessarily assigned to the MUNIS file administration group on the gateway server. The support account was subsequently removed from the MUNIS file administration group.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-12: The Kentucky Department Of Education's Office Of Education Technology Should Formalize And Consistently Apply Logical Security Policies For The KETS Network And MUNIS (Continued)

Although OET had not implemented a formal security policy, an informal policy was in place requiring OET staff to first obtain authorization from the school district before accessing that district's MUNIS server or software. However, logs were not maintained at KDE/OET to track access to district servers. We also noted that, although OET had implemented Object Access audit logging on its critical servers, there were no procedures in place to periodically monitor the logs. Furthermore, no one was responsible for monitoring the output of the Computer Oracle and Password System (COPS) utility, which was scheduled to run on the gateway server in order to identify files that were replaced and/or permissions that were changed on the RS6000 servers residing at the school districts. The primary output of the COPS utility included two reports—the Cyclic Redundancy Check (CRC) and Set User ID (SUID) reports.

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

Without strong, formalized, logical security controls, the opportunity increases for unauthorized modification to financial and staffing reports as well as the likelihood of errors or losses occurring from incorrect use of data and other resources. 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. Allowing users to share user IDs eliminates the ability to identify specific individuals accessing system resources.

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

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 purged periodically. Finally, system user accounts and audit trails should be reviewed periodically in order to ensure identification and tracking of user activity.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-EDU-12: The Kentucky Department Of Education's Office Of Education Technology Should Formalize And Consistently Apply Logical Security Policies For The KETS Network And MUNIS (Continued)**

Recommendation

We recommend OET develop and implement a formalized security policy to standardize security responsibilities for all OET employees and ensure critical programs and data, as well as the servers housing such data, are properly secured. Specifically, the agency should, at a minimum:

- Develop 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 enabled 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.
- All security group assignments on the OET servers should be evaluated 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.
- Designate personnel to be responsible for monitoring the COPS utility output, which entails the CRC and SUID reports.
- A security log should be established for all authorized KDE employees to log their access to the school districts' MUNIS servers, and these logs should be monitored and periodically reviewed.
- Local Administrator rights should be restricted to only technical and support staff that requires this type of access.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-EDU-12: The Kentucky Department of Education's Office Of Education Technology Should Formalize And Consistently Apply Logical Security Policies For The KETS Network And MUNIS (Continued)**

Management's Response and Corrective Action Plan

KDE agrees to coordinate internally, to discuss these recommendation(s) and to determine what further actions may be appropriate, in light of these recommendations.

OET has specifically requested all service teams to review their security group assignments on the OET servers to ensure assigned users require membership. This review should be complete by September 15. OET will perform a follow-up inspection once the review is complete.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-13: The Kentucky Department Of Education's Office Of District Support Services Should Formalize And Consistently Apply Its Logical Security Policies

During the FY 2007 audit of controls at KDE, it was determined that ODSS did not properly secure the critical financial data associated with the SEEK program. As was also noted during FY 2006, ODSS had not developed or implemented a formalized security policy that identifies management and user responsibilities concerning IT security surrounding the SEEK program and other applications developed and maintained by ODSS. The logical security issues identified during our audit are presented below.

It was noted during FY 2006 that a user ID and the associated password were hard coded into the program code designed to retrieve information from other programs to be utilized in the SEEK application. We again identified the same administrator-level user ID hard coded within the Data Transformation Services package that is used in the transportation portion of the SEEK program. The password, although it had been changed from the prior year, was also hard coded. It should be noted that the production copy of this script was available to all SEEK database users on the ODSS structured query language (SQL) server, and an older copy was stored in the SEEK development directory and was available to all users of that application server. ODSS indicated that they anticipate completion of a new version of the SEEK application within the upcoming fiscal year, which will eliminate hard coded user IDs and passwords.

We tested to ensure that confidentiality forms were on file for the individual users with access to the SEEK database, SEEK application, as well as the SEEK development and SEEK application directories on the ODSS servers. One of the forms was not available; however, ODSS had the user complete the form as of the date of fieldwork. Since ODSS is responsible for determining the access needed by ODSS employees to OET's FTP server and gateway server utilized in the transfer of MUNIS reports, we also tested to ensure that confidentiality forms were on file for the 10 ODSS users with access to the FTP server and the three ODSS users with access to the gateway server. Our testing revealed that confidentiality forms were not on file for two ODSS users with access to the FTP server and one ODSS user with access to the gateway server. ODSS subsequently had two of the three users complete a confidentiality form. It should be noted that the same two employees identified with access to the FTP server and having no confidentiality form on file were also identified during the FY 2006 audit. Furthermore, two former ODSS employees had access to the FTP server.

We noted ODSS had implemented a transaction log for the SEEK application in order to track user activity within the application. In addition, ODSS has auditing enabled for server logins. However, ODSS has no procedures in place to periodically review their security logs. We also noted one unnecessary group with access to the SEEK application directory. This group was initially implemented for generic branch access; however, it was never used and was deemed unnecessary.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-13: The Kentucky Department Of Education's Office Of District Support Services Should Formalize And Consistently Apply Its Logical Security Policies (Continued)

While auditing the logical security controls surrounding the SEEK application, we identified multiple segregation of duties issues where the SEEK programmer had unnecessary access to the SEEK production data. These issues were addressed in a separate comment.

Without strong, formalized, logical security controls, the opportunity increases for unauthorized modification to production files as well as the likelihood of errors or losses occurring from incorrect use of data and other resources. The lack of formal security policies was key in allowing the various security weaknesses noted.

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

Recommendation

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

- Implement procedures to periodically review security logs with special emphasis upon users with high-level privileges so that inappropriate use of resources can be further investigated, if the need arises.
- User authentication should be used in any processes or code requiring authorization rather than maintaining hard coded usernames and passwords in the code. Hard coded usernames and passwords in program code should be eliminated.
- All individual user accounts and groups should be analyzed to determine if they are necessary. If not, they should be removed. This process should be re-performed on a periodic basis.
- Ensure that confidentiality forms are properly authorized and maintained on behalf of all ODSS employees.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-13: The Kentucky Department Of Education's Office Of District Support Services Should Formalize And Consistently Apply Its Logical Security Policies (Continued)

Management's Response and Corrective Action Plan

KDE will implement processes to periodically review security logs and user accesses and improve user authentication by June 30, 2008. ODSS managers will immediately ensure that confidentiality forms for new employees are properly authorized. The forms are maintained by the Division of Human Resources, Office of Internal Administration and Support.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-14: The Kentucky Department Of Education's Office Of District Support Services Should Ensure Proper Segregation Of Duties

As was noted during the FY 2006 audit of KDE system controls, ODSS did not employ proper segregation of duties between the system programming and operation functions. During the FY 2007 audit, we determined that this situation still exists. Specifically, one KDE programmer had unnecessary access to SEEK production application and database.

Security was implemented within the SEEK application whereby users must authenticate to the application, which in turn authenticates to the SEEK database. User roles were also assigned in order to restrict access within the application. It was noted that the KDE programmer, although not being provided with power user credentials within the SEEK application, had been granted the Administrator role in order to perform user maintenance. In addition, the programmer had the ability to modify files within the directory housing the SEEK application. We determined that the KDE programmer also had write capabilities to the SEEK database, which houses the SEEK production data.

ODSS did not appoint a Database Administrator (DBA) to oversee the SQL server housing the SEEK database. Although ODSS recognizes the importance of filling this position, they have not been successful in accomplishing this appointment.

During FY 2007, improvements were made with regard to the ODSS change control procedures, which includes the appointment of a librarian and Technology Project Manager. However, as was noted in FY 2006, the change control procedures have yet to be formalized, which was addressed in a separate comment.

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

Computer programmers should not have direct access to the production version of program source code or be able to directly affect the production environment. The reason for this control is to ensure that the programmer does not intentionally or unintentionally introduce unauthorized or malicious source code into the production environment. Smaller organizations that cannot easily segregate programmer duties from computer operator duties should implement compensatory controls to supervise and monitor programmer activities to ensure only properly tested and authorized programs are migrated into production. Further, the ability to perform user maintenance provides the opportunity to circumvent role assignments by establishing new accounts with high-level privileges for personal use.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-EDU-14: The Kentucky Department Of Education's Office Of District Support Services Should Ensure Proper Segregation Of Duties (Continued)**

Recommendation

We recommend ODSS evaluate the necessity of granting the programmer access to the production data within the SEEK database. If access is required, it should be Read-Only. Additionally, the programmer should be restricted from performing user maintenance for the SEEK application and from modifying or writing to the directory housing the SEEK application. All production programs and data should be secured separately from the development and testing environment in order to maintain proper segregation of duties. ODSS supervisory staff should continue to thoroughly review and document all program changes made by the programmer to ensure they are appropriate prior to processing. Further, a DBA should be appointed to oversee the SQL server housing the SEEK database. The DBA's responsibilities should include the establishment of all current employee access levels and monitoring of access levels on an ongoing basis to ensure access levels facilitate a proper segregation of duties and do not allow inappropriate access to production data. This review should be thoroughly documented for audit purposes.

Management's Response and Corrective Action Plan

KDE, ODSS concurs with the recommendation and will address required changes and improvements through the redesign of the SEEK application, scheduled for completion by June 2008.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-EDU-15: The Kentucky Department Of Education Should Ensure That Security Information Leakage For Agency Computer Devices Is Minimized

During the review of KDE security controls governing Network Neighborhood folders, we determined the Education Cabinet did not restrict critical information divulged by its network machines. There were a total of three machines that were noted with multiple issues as described below.

Review of the EDU domain revealed three workSTations that, when accessed, displayed a printer. Although the printer did not display excessive information through Network Neighborhood, we were able to determine the associated Internet protocol (IP) number and gain connections through alternate means. Consequently, we connected to a Web Image Monitor on all three machines via Port 80 utilizing one or more of the default usernames for the associated printer model and a null password. The Web Image Monitor for the three machines provided excessive information regarding the printer and network, and provided the options to change settings and passwords when logged in as the machine administrator. We were able to logon as the machine administrator and supervisor on two of the three workSTations; however, we were only able to logon as the supervisor on the third machine. The supervisor login, however, provided the option to change the machine administrator password, which would potentially grant access to an intruder to take over the administrator account and change settings, as well. It should be noted that no network settings or passwords were changed during this review.

In addition, we were able to connect to Port 23 and initiate a Telnet session on all three machines noted above via the same default usernames and null passwords that were used for Port 80 access. We were also able to establish an anonymous FTP session via Port 21 on each of the three machines. Although the files displayed during the FTP session were not confidential in nature, we did have the ability to upload files to all three machines.

It was determined that two of the three machines are located within the Department for Workforce Investment, and the third machine belongs to the Education Cabinet Office of Human Resources. Again, these machines all fall under the jurisdiction of the Education Cabinet.

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. The existence of unused open ports and default profiles increase potential security vulnerabilities and is an invitation for intruders to enter the system.

An agency's domain information that is accessible to users of the Kentucky Information Highway through inquiry tools should be kept at a minimum. An agency can set devices to not respond to certain types of inquiries. To minimize the risk of unauthorized access to a

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-EDU-15: The Kentucky Department Of Education Should Ensure That Security Information Leakage For Agency Computer Devices Is Minimized (Continued)**

machine, only necessary business-related ports should be open, default profiles should be avoided, and system software should be kept up to date. Further, information concerning system configuration should not be made publicly available, and anonymous users should never have the ability to change these settings. The default administrator and user accounts should be secured with strong passwords to avoid being compromised. Servers should not allow anonymous or null session access.

Recommendation

We recommend the Education Cabinet security personnel restrict the level of information provided by their LAN machines to anonymous users. This process should include, where feasible, limiting or restricting the type of response machines provide based on certain inquiries. Furthermore, the Education Cabinet should review all domains/workSTations available through the Network Neighborhood to ensure all files are adequately secured. In addition, all open ports should be reviewed on the noted machines to ensure there is a specific business-related purpose requiring the port to be open. If not required, then that port should be closed. If the port is necessary then the most recent patches should be implemented for the service in use, applications should be kept updated, and adequate logical security controls should be implemented to prevent unauthorized access as necessary. Default profiles and anonymous access should be disabled for critical services, and the services maintained should be secured with strong passwords.

Management's Response and Corrective Action Plan

The above devices were identified and the following corrective action taken. Administrator account has a password assigned; the supervisor account has a password assigned. All non-critical protocols have been disabled.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-16: The Finance And Administration Cabinet Should Formalize And Consistently Apply Logical Security Procedures For ePayment Gateway

During the FY 2007 audit of the Finance and Administration Cabinet (FAC), it was determined that informal logical security procedures exist for the ePayment Gateway (ePay); however, these procedures were not adhered to. Specifically, testing revealed instances where access to ePay was established without proper authorization to support the granted profiles.

There are six security profiles within the ePay that can be established, four of which can be attributed to a user - Merchant Administrator, Merchant User, Merchant Viewer, and Report Developer. Access to these profiles is authorized through the ePay User Information form, which is to be submitted by the user's supervisor either electronically via email or hard copy to the ePay Administrator. Review of users with a Merchant Profile (Administrator, User, or Viewer) revealed 16 out of 23 users, or 69.6 percent of the population, did not have supporting documentation on file with FAC to sufficiently authorize access for the user to the ePay application profile. Specific exceptions identified include the following:

- 10 users had an ePay User Information form on file; however, the granted Profile Access and Merchant ID/Location was not marked for 7 of these users. One additional user had been granted Merchant Administrator access; however, the Merchant ID/Location was not specifically identified.
- Supervisor approval was not obtained prior to access being granted for 11 users.
- No documentation (email or user access form) was on file for 1 user.

In addition, review of users with Report Developer access revealed that 10 out of 10 accounts, or 100 percent of the population, did not have supporting documentation on file with FAC to sufficiently authorize access for the user. Six users did not have supervisor approval on file. Additionally, 4 of the 10 users did not have an ePay User Information form on file indicating the Profile Access and Merchant ID/Location required.

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.

Established security policies and procedures should be formalized 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.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-16: The Finance And Administration Cabinet Should Formalize And Consistently Apply Logical Security Procedures For ePayment Gateway (Continued)****Recommendation**

We recommend FAC develop and implement formalized logical security procedures to ensure only authorized access is granted to the ePayment Gateway. These procedures should require that a user's supervisor formally request access to ePay for all users needing this type of access. The supervisor should ensure that the ePayment Gateway User Information form is thoroughly completed so that the ePay Administrator knows what Profile Access and Merchant ID/Location(s) are required. This documentation should be maintained historically by the ePay Administrator for audit purposes.

Management's Response and Corrective Action Plan

Security Requests for access to the ePAY application shall be submitted on the ePAY User Authorization Form. SAS will be responsible for ensuring the following is included on the form: Name, User/Employee ID, E-mail address, and ePAY security permissions (Security Profile/Role and Merchant ID/Location access). Additionally, SAS will verify the form was submitted by the ePAY Merchant Contact/Admin, the user's supervisor or the agency eMARS Security Officer. Authorization Forms (electronic and/or hard copy) shall be maintained in SAS for historical/auditing purposes.

Subsequent changes for existing users may be submitted on the User Authorization Form or by an E-mail request to the SAS ePAY Administrators. The E-mail should clearly state the particular request (i.e. granting the user an additional security role/profile or granting the user access to another merchant ID/Location). As with electronically-submitted Authorization Forms, all E-mail requests shall be maintained in SAS.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-17: The Finance And Administration Cabinet Should Ensure All Reporting From InfoAdvantage Is Accurate And Complete

Our FY 2007 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 seven situations where reporting was not functioning as expected.

- Within the General Accounting universe, we noted a problem with a database join related to the Event Type field that was not properly established when attributed to the JVA (Advanced Journal Voucher) document code. By using the Event Type field in the report or in the filter requirements, the resulting population would only reflect records where the Event Type was populated within the Accounting Journal. The Commonwealth of Kentucky has not required the Event Type to be populated on all transactions. Therefore, this join logic was causing transactions to be excluded from the population when the Event Type was validly blank. This logic was corrected by Finance in November 2006, subsequent to our testing.
- Within the Procurement Awards universe, there is a problem with the information returned when a user develops a report of Solicitation Response documents including specific required fields for the documents. According to the vendor, CGI-AMS, the values for those fields are not being pulled from the document even though the fields exist on the document. Instead the values for these fields are coming from the Award Accounting Line. The user cannot rely upon these results because there is not a direct relationship between the Solicitation Response and the Award Accounting Line tables in infoAdvantage. When the user attempts to create this connection, infoAdvantage will associate all Award Accounting Line table records to the Solicitation Response documents where the Vendor/Customer ID on the Award Accounting Line matches the value on the Solicitation Response document. This association will cause incorrect information to be reported.
- Within the General Accounting universe, there is a problem when the user attempts to add the address information related to a vendor. There is a Left Outer Join established within the General Accounting universe between the Vendor/Customer Code on the Vendor Customer table and that field on the Accounting Journal. However, there is not a join of any type established related to the Vendor/Customer Address ID or the Address Type although the address is established at that level. There are two classes with the universe where a user can get the vendor address: 1) Vendor Master Address and 2) Vendor Address. Within the Vendor Master Address class, the address is established on the Address ID level. The lack of a join at the Address ID level will cause duplicate records to occur when pulling records from the Vendor Master Address class when the vendor in question has more than one Address ID. Within the

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-17: The Finance And Administration Cabinet Should Ensure All Reporting From InfoAdvantage Is Accurate And Complete (Continued)

Vendor Address class, the address is established on the Address ID/Address Type level. The lack of a join on both the Address ID and Address Type will cause duplicate records to occur when pulling records from the Vendor Address class when the vendor in question has either more than one Address ID or more than one Address Type associated with a single Address ID.

- Within the General Accounting universe, there is a problem with the logic underlying queries made to the Basic Accounting Ledger and Detailed Accounting Ledger. When a user extracts data related to the Accounting Journal, the results are restricted to those departments allowed to the requesting user. However, in the case of queries made against the Basic Accounting Ledger and the Detailed Accounting Ledger, the application provides results related to all departments.
- Within the General Accounting universe, the Basic Accounting Ledger and Detailed Accounting Ledger classes have been designed to mimic the FCT2 and FCT3 summary ledgers within the MARS environment. A single Summary table within the eMARS Data Warehouse populates the data elements within these classes. According to Finance, there are known problems with the validity of the data making up the Summary table that will require the table to be rebuilt.
- Within the General Accounting universe, there is no data element for the Payee Vendor field that resides on the PRC (Commodity Based Purchase Request) and PRC2 (Commodity Based Purchase Request ProCard) documents. On these two documents, this field of data is designed to replace the Vendor Customer Code for payment. It is, therefore, necessary for this field to be available within the General Accounting universe to ensure that the user can identify the actual vendor to whom payment was made.
- Within the Accounts Payable universe, there is a Purchase Request (PR) class with subclasses that house information concerning the PR Header (HDR). Originally we thought that the PR HDR Payee subclass would provide the Payee/Vendor Customer Code and associated name and address information. However, we found that the Payee/Vendor Customer Code within the PD HDR Payee subclass is providing the Vendor Customer Code that was originally placed on the Vendor section within the document instead of the Payee Vendor Code on the document header. The remainder of the Payee information being reported is being populated from an Accounts Payable Payment Request table as expected.

Further, due to the lack of information available on the contents and structure of universes, especially those customized for the State, end users may be developing reports that do not provide accurate or complete data. When requesting information concerning the universes

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-17: The Finance And Administration Cabinet Should Ensure All Reporting From InfoAdvantage Is Accurate And Complete (Continued)

within infoAdvantage, we were informed that a data dictionary for this reporting solution had not been created. Currently, a manual that discusses the base line universes and some quick reference documents developed for training purposes are available for end users, but there was not a comprehensive repository developed that could be utilized for reporting purposes. In addition, an end user working within the thin client (Business Objects Info View) or the base line thick client (Business Object) applications is not able to view how the data elements within a given universe are interrelated. Although there is a discussion of how the universes are developed based on the underlying tables within the base line universe manual, this discussion is at a high level and does not go down to the data element level.

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 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 and content. 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 CGI-AMS, 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 that they are functioning as intended for the Commonwealth of Kentucky.

To 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*****FINDING 07-FAC-17: The Finance And Administration Cabinet Should Ensure All Reporting From InfoAdvantage Is Accurate And Complete (Continued)**

Management's Response and Corrective Action Plan

The Finance and Administration Cabinet acknowledges the need to validate reports that are published to Info Advantage for statewide use. We will continue to address all known reporting issues as well as document existing reports. Reviewing joins in universes is a companion activity to documenting our reports. We are investigating automated data dictionary generation capabilities, although utilization of the MRDB data dictionary was poor.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-18: The Finance And Administration Cabinet Should Develop And Implement Formal Policy And Procedures To Govern The Security Of The eMARS Checkwriter Interface Process

The Finance and Administration Cabinet (FAC) has not developed or implemented a formal policy identifying responsibilities of those individuals involved with the Enhanced Management Administrative and Reporting System (eMARS) Checkwriter (CW) interface process. FAC Statewide Accounting Services (SAS) is ultimately responsible for processing of CW files. Further, they are responsible for ensuring access to CW files is reasonable. SAS must ensure that 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 seven CW files that were loaded and certified at the department level by the same user. Although this situation should have been caught by SAS central level certification, these CW files were allowed to process fully through the system.

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 FAC 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. Additionally, FAC should review the feasibility of adding automated edit checks within the system to ensure proper segregation of duties within processing of the CW files.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-18: The Finance And Administration Cabinet Should Develop And Implement Formal Policy And Procedures To Govern The Security Of The eMARS Checkwriter Interface Process (Continued)

Management's Response and Corrective Action Plan

There are three types of roles associated with the processing of checkwriter files in eMARS. Two roles reside in the agencies and one resides in Finance – SAS. One of the agency security roles (AGCY_CW_LOAD) grants a user the authority to load the checkwriter XML files to the Interface Content Manager page. As part of this security the user must be granted access to one or more specific interface/checkwriter files on the INTIDS page. The security officer in each agency has the authority to assign this security role to the user. Additionally, the security officer and/or agency head must send a request (E-mail of paper) to the SAS Security Admin requesting access to the specific interface files.

The second agency role is the AGENCY_CW security role. This role allows a user to certify the checkwriter files (performed on the Checkwriter Header page). The central security role (CEN_CW) grants SAS the authority to centrally certify the checkwriter files (also done on the Checkwriter Header page). The agency security officer also has the authority to assign the AGENCY_CW role to their users.

A user in the agency may be permitted to have both the AGENCY_CW and AGENCY_CW_LOAD security roles. The reason is a single user may be responsible for loading certain checkwriter files and also be responsible for certifying other checkwriter files. However, a user should not load and certify the same checkwriter file. Currently, this is a process monitored by the “central” SAS staff. Before centrally certifying a checkwriter SAS should verify that separate users loaded and certified the checkwriter in the agency. These fields are displayed on the Checkwriter Header page. If a user did both steps SAS will contact the agency and instruct them that they cannot centrally certify the file, and another agency user will have to departmentally certify the file before SAS can apply their certification.

Auditor's Reply

We understand that procedures have been put in place for the security over checkwriters interfaces within eMARS; however, these procedures have not been formalized. Further, our review has shown, as noted in the body of this comment, that these procedures are not being consistently applied. Therefore, we continue to recommend that the procedures governing the security over checkwriter interface process be formalized and the oversight of this process be strengthened.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-19: The Finance And Administration Cabinet Should Strengthen, Formalize, And Consistently Apply Error Handling Procedures For Interface Files

Our audit of the Finance and Administration Cabinet (Finance) revealed that adequate error handling controls had not been implemented concerning the interface file processing within the Enhanced Management Administrative and Reporting System (eMARS) Advantage Financial application. Our examination found that controls surrounding the error handling process were not formalized and procedures in place were inadequate and were not consistently applied. Specifically, there were three areas of concern: 1) Review of the entire interface file process, 2) Review of submission job logs, and 3) Reporting of errors to appropriate agency staff.

First, the Finance Controller's Office (CO) staff members that perform the reviews of interface file processing did not formally log their reviews. There are currently eight staff members performing this review on a daily, rotational basis. The morning following the nightly interface file processing, the designated staff member produces an e-mail that is provided to production staff outlining all interface files that were imported during the previous night's process. There has not been a policy established concerning required information to be included within this e-mail. Therefore, our testing revealed inconsistent content within the emails submitted for this process by the applicable CO staff members.

Second, the review performed by the CO staff members did not consistently include a review of the submission job logs. These logs will indicate if there were problems with the submission of documents within the Document Catalog. Discussions revealed that Finance considers it as the responsibility of the applicable agency to ensure that errors noted within this process are corrected for their interface files. However, we feel the CO staff should review these logs for unusual errors that might be of a concern at the Finance level. We tested the reviews by CO staff for 20 of the 37 dates (54%) for which interface file processing information was available within the Advantage Financial application. Our testing revealed that on 5 of the 20 dates tested, a type of Purchase Order document was showing up in the submission logs but the transactions were not being successfully submitted to the Document Catalog. Subsequent to our notifying the CO staff of this situation, they contacted CGI-AMS and it was determined that these documents were not being submitted due to a problem with the underlying system query language (SQL) programming. The CO staff issued a formal request to CGI-AMS for an appropriate correction to the SQL.

Third, the CO staff members were not consistently maintaining communications with appropriate agency staff concerning interface file import failures or other errors noted within the import process. Further, we noted that these communications were occasionally made through phone calls, which were not logged or otherwise documented.

The eMARS system was brought into production in July 2006. Although the general instructions concerning the interface file processing have been documented within the system documentation, the specific daily review procedures to be performed by CO staff have not

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-19: The Finance And Administration Cabinet Should Strengthen, Formalize, And Consistently Apply Error Handling Procedures For Interface Files (Continued)**

been formalized. This lack of documented procedures has resulted in inconsistent and inadequate processes related to interface file processing.

Formalized procedures are important for ensuring completeness and uniformity especially when the process is disbursed among multiple staff. Further, these procedures should be consistently applied to ensure that all failures within the import process are identified; unusual errors within the submission process are documented; and any failures or errors identified are communicated to agency staff in a systematic and expedient fashion.

Recommendation

We recommend the Controller's Office staff incorporate the following procedures into the interface file error handling process:

- Standardize the content of the nightly cycle e-mail to include, at a minimum, the following pieces of information:
 - 1) Job ID
 - 2) Interface File Name (.xml file)
 - 3) Document Code
 - 4) Number of Documents for Import
 - 5) Number of Documents Successfully Imported
 - 6) Number of Documents Failing Import
 - 7) Description of Error(s) Shown With Import Process
 - 8) Notation of Agency Contact Concerning Any Errors With Import Process
 - 9) Notation of Review of Submission Jobs To Determine If Unusual Errors Requiring Agency Contact
- Require at least cursory review of all logs related to the submission of documents to ensure that unusual errors are not occurring that need to be brought to the attention of agency personnel or CGI-AMS system programmers.
- Require that all communications with agency personnel or CGI-AMS concerning the interface process be maintained for audit review. The standard communication type should be e-mail. If a phone conversation is used to transmit information concerning the interface process, we recommend that a follow-up e-mail also be send to ensure that all parties understand the discovered error.

Further, we recommend that these procedures be formalized in a policy that is distributed to all Controller's Office staff assigned to the interface file processing review.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-19: The Finance And Administration Cabinet Should Strengthen, Formalize, And Consistently Apply Error Handling Procedures For Interface Files (Continued)**

Management's Response and Corrective Action Plan

The nightly note has been standardized. The interface information includes the XML filename, Doc # loaded, Doc # Failed, and Reason for Failure. Our standard practice is to email the person who loaded the file and the fiscal officer when we have failed loads. Contact email will be stored with the nightly note going forward. The disposition of successfully loaded documents are the responsibility of the departmental personnel. They contact us if the mass actions are necessary to be taken on the loaded documents after their evaluation of errors.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-20: The Finance And Administration Cabinet Should Ensure eMARS Production Cycles Are Monitored And Logged, And That Sufficient Policies And Procedures Are Implemented To Govern eMARS Operations

During the FY 2007 audit of the Finance and Administration Cabinet (FAC), it was determined that no formal policies & procedures had been implemented governing the Enhanced Management Administrative and Reporting System (eMARS) system production job monitoring, logging, and problem resolution. Our audit revealed that eMARS production job run documentation was maintained in an inconsistent and/or incomplete manner.

The auditor accumulated information concerning 22 dates of eMARS unavailability between July 17, 2006 and January 12, 2007. For these dates we examined available documentation maintained by the Commonwealth Office of Technology (COT) concerning job runs, completions, abnormal program terminations (abends), and problem resolutions. Certain procedures had been established at COT concerning required COT Operations documentation for job run statistics or production cycle problems/resolutions. However, our discussions and testing revealed that no formal policies and procedures had been implemented concerning formal requirements to document job runs and production cycle problems and resolutions.

Discussions revealed that nightly run sheets are maintained and manually updated throughout the evening as the cycles run. As the jobs and schedules are completed, the operators either sign-off or check-off the job, indicate the start and end time, any errors, and initial the run sheets. COT Operations also maintain an electronic spreadsheet template to list daily abends. The daily Abend Reports are to be filled out each morning at 7:00 AM and emailed to the distribution lists involving various FAC and technology personnel, which contains system status information for each system that the COT Operations supports. Various email strands are also documented between the COT operations team and the supporting financial and technology personnel as to remediation steps to be taken. These communications are also maintained and reviewed by FAC management.

Specifically, our testing of these 22 days of eMARS system unavailability revealed:

- Nightly run sheets could not be provided for two of the dates examined.
- Daily abend reports were not completed for two incidents examined due to downtime occurring during the daytime hours.
- Daily abend reports were not completed for six additional incidents.
- The daily abend report for one date was incomplete as it only included the start time and that jobs were incomplete but did not report the specific problem or abend causes.
- Email correspondence could not be located for one occurrence and the resolution could not be determined.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-20: The Finance And Administration Cabinet Should Ensure eMARS Production Cycles Are Monitored And Logged, And That Sufficient Policies And Procedures Are Implemented To Govern eMARS Operations (Continued)

Further, the documents that were observed did not consistently and completely provide key production run details such as start/stop times, operator on duty, problems/abends encountered, and resolutions taken.

The lack of formalized policies and procedures concerning production job run documentation resulted in incomplete or inconsistent documentation concerning system abends and resolutions. Failure to adequately document system errors or abends and applicable resolutions increases the chances that data is not completely or accurately processed and can increase the time required for resolving future system errors or abends.

Policies and procedures should be formalized to ensure consistent and accurate documentation of production job progress, completion, and resolutions to abends and errors. Production operations documentation is valuable for determining trends and implications of future events. Production job logs should be sufficiently detailed to enable problem reconstruction and examination.

Recommendation

We recommend FAC formalize and disseminate eMARS production operations policies and procedures to be followed by the various eMARS production and support teams. This policy should include expected procedures for production job run logging, procedures to communicate and resolve production problems, and requirements to document the details of unsuccessful runs and system unavailability. This documentation should be consistently developed and maintained centrally and include the issues, personnel, jobs, systems, and details to resolution. The nightly cycle support notes should completely and consistently reflect details for the night's runs including detail on job failures, jobs placed on hold, or canceled, and indication of reason and resolution action taken.

Management's Response and Corrective Action Plan

A formal process and procedure document has been created and disseminated to all Operations Services Personnel detailing the role and responsibilities of Operations staff pertaining to the support of production EMARS systems after-hours. Awareness has been sent out to the Operations staff informing them that all pertinent information concerning any EMARS Abends or errors needs to be documented and included within the Nightly Abend Report. However, issues that are addressed during normal working hours are not and never have been addressed on the Abend Report. This is consistent with all Systems supported by Operations Services. It is the responsibility of COT Production Services staff to communicate and work with agency support staff during

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-20: The Finance And Administration Cabinet Should Ensure eMARS Production Cycles Are Monitored And Logged, And That Sufficient Policies And Procedures Are Implemented To Govern eMARS Operations (Continued)

Management's Response and Corrective Action Plan (Continued)

normal working hours to resolve any outstanding issues. Furthermore, the amount of detailed information contained within the Nightly Abend Report pertaining to EMARS issues is directly dependent upon the information given to the Operations staff by supporting personnel. A copy of this document has been provided to the auditors for audit documentation purposes.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-21: The Finance And Administration Cabinet Should Formalize Procedures Governing System Assurance Processing

Our audit of the Finance and Administration Cabinet (FAC) Advantage Financial System Assurance (SA) processes revealed there are no formalized procedures governing the process. System Assurance jobs were not consistently run. Reports reflecting detail of errors were not available when SA processes resulted in a return code of a non-fatal error. Further, nightly cycle notes utilized to monitor production did not consistently and/or completely reflect the status of SA jobs, applicable reasons for SA jobs not running, or explanation of errors when jobs were noted as containing errors.

There are five jobs currently governing SA internal to the Advantage Financial System:

- Budget Actual Versus Ledgers, Journals and Posting Line Catalog - Ledgers, journals, and posting line catalog are in sync with the budget tables and with certain non-budget tables. Specifically the actual amounts that are summarized by posting code and chart of account elements are compared across these different database tables. *(SA01 - run nightly Monday - Friday)*
- Non-Budgetary Actual Versus Ledgers, Journals and Posting Line Catalog – Similar to above but verifies actual amounts on specific non-budgetary tables. The process verifies that the ledgers, journals, and the posting line catalog are in sync with the Balance Sheet Account (BBALI), Fund Balance (FBALQ), and Cash Balance (CBALQ) tables. Specifically amounts that are summarized by posting code and chart of account elements are compared across these different database tables. *(SA02 - run nightly Monday - Friday)*
- Debits equal Credits - Debits and credits are equal within a balanced journal/balanced ledger since the last time the process was run. *(SA03 – run nightly Monday - Friday)*
- Disbursements Request Table (DISRQ) Versus the Accounting Lines in Payment Request (PR) and Accounting Based Spending (ABS) Documents - A two-step process that ensures the integrity of all records on the Disbursements Request Table (DISRQ) by comparing its records with the accounting line records for Payment Request (PR) and Accounting-Based Spending (ABS) documents.

The first part of the process ensures that the open accounting lines in the PR and ABS documents are present on the DISRQ table. *(SA04 - run weekly after Friday processing)*

The second part of the process ensures that the amount in the Outstanding Payments field is the same in the DISRQ table and in the accounting lines of the PR or ABS documents. *(SA05 - run weekly after Friday processing)*

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-21: The Finance And Administration Cabinet Should Formalize Procedures Governing System Assurance Processing (Continued)**

Following processing of each job an entry is viewable on-line via the Enhanced Management Administrative and Reporting System (eMARS) BATJOB page for 60 days, including weekends and holidays where the processes are not run. Excluding weekends and holidays the 'Budget Actual versus Ledgers, Journals, and Posting Line Catalog' (SA01), and the 'Non-Budgetary Actual versus Ledgers, Journals, and Posting Line Catalog' (SA02), system assurance processes were not run on the following run dates:

12/5/06 (for 12/4/06 nightly cycle)
12/14/06 (for 12/13/06 nightly cycle)
12/20/06 (for 12/19/06 nightly cycle)
1/11/07 (for 1/10/07 nightly cycle)
1/23/07 (for 1/22/07 nightly cycle)

Follow-up with Finance indicated that there are times when the SA jobs are suspended or canceled to allow the system availability by 7:00 am. At times nightly cycle support staff will receive an email reflecting instructions on when to suspend jobs or cancel them but this email does not appear to be standard practice and there is no evidence that it was consistently followed for the dates reflected above. Though the SA jobs are executed via CA-Scheduler at COT, there is not a formal procedure in place to assist in determining the guidelines for when the jobs should be suspended or canceled.

Review of the SA01 process revealed that of the 37 days viewable on-line there were 35 days that returned a code of non-fatal error and had a job log entry reflecting an Out of Sync Condition, only 18 of these days had a report available to reflect the specific errors. No report was available for the remaining 17 days. System assurance reports are available for viewing on-line through eMARS in the same manner as noted above for the jobs. Our review of the system entries revealed that generation of the report reflecting the status and errors with SA01 processing did not begin until 12/28/06.

Review for the SA02 report revealed that of the 34 days viewable on-line there were 22 days that returned a code of successful and 12 days that returned a non-fatal code and had a job log entry reflecting an Out of Sync Condition. Reports reflecting details of error were associated with only five of the 12 instances. No report was available for the remaining seven. Our review of the system entries revealed that generation of the report reflecting the status and errors with SA02 process did not begin until 1/9/07.

The origination date of two errors within the SA01 and SA02 jobs was undetectable as a result of the SA jobs and reports not being consistently executed. Further, there is a rotation schedule reflecting who is responsible for monitoring eMARS nightly cycle processing each night. After each cycle, a nightly cycle note is compiled addressing certain subject matters. Our discussions with the Finance and Administration Cabinet management revealed that these

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-21: The Finance And Administration Cabinet Should Formalize Procedures Governing System Assurance Processing (Continued)**

nightly cycle notes are not required to be completed in a specific format or to include specific subject matters. The notes do, however, have to contain common subject matters including System Assurance exceptions.

Since the SA processing status information was only available on-line for 60 days, the auditor reviewed hard copy cycle notes distributed to report on nightly cycle processing for the tested dates outside of that 60 day period. The cycle notes for three of the ten such dates tested did not reflect the status of the SA jobs. For one date the nightly cycle notes indicated that the SA jobs were not run but there was no indication as to the reason. On two dates the nightly cycle notes reflected the SA01 job failed but did not provide the status of the remaining four SA jobs (SA02-SA05) and there was no indication as to the reason for the failure. There was one date where the nightly cycle note indicated the jobs run successfully when in fact they were not run at all.

Failure to formalize procedures for governing system assurance jobs and resulting reports may result in system assurance processes being neglected and ultimately hinder the integrity of data.

Formalized procedures are important to ensure system assurance processes are completely and accurately executed and any noted issues are resolved in a timely manner. These procedures should be consistently applied to ensure that adequate documentation is maintained for all instances where the system assurance process is suspended or canceled and to ensure that all errors are responded to accordingly.

Recommendation

We recommend FAC work with the Commonwealth Office of Technology (COT) to formalize procedures for processing System Assurance jobs. These procedures should include explanations as to when System Assurance jobs should be suspended or canceled and should include error resolution requirements. These formalized procedures should be distributed to all personnel responsible for nightly cycle processing and nightly cycle support. We also recommend that FAC work with COT to ensure that resulting system assurance reports are produced and maintained on a consistent basis.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-21: The Finance And Administration Cabinet Should Formalize Procedures Governing System Assurance Processing (Continued)**

Management's Response and Corrective Action Plan

We continue to have issues with the systems assurance reports recording false positives. Because of the unreliable results on our system assurance reports, we have made the call on many nights when we have troubles to bypass them to take time out of the cycle. Once our reports are reliable, we will not routinely suspend these reports in the nightly cycle. The SA reports can also be run in full or incremental modes, so if a night is missed the full mode picks up any missed items. The call to suspend the reports is with the CGI-AMS and Commonwealth functional person on call. PDF files of the systems assurance reports will be maintained on the eMARS server by the functional person on call to avoid the loss of historical reports.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-22: The Finance And Administration Cabinet Should Develop And Implement Formal Policy And Procedures To Govern The Security Of The eMARS Production Databases

During the FY 2007 audit of the Finance and Administration Cabinet, it was determined that logical security procedures exist for granting access to the Enhanced Management Administrative and Reporting System (eMARS) production databases; however, these procedures were not formalized nor consistently applied. 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 Remedy application. Out of a total of 39 individual users with access to the eMARS production databases, there were 28 users (or approximately 72%) that either did not have a complete COT-F181 form or an email on file to authorize the request. The emails that were on file were not well organized so that they could be retrieved quickly for audit purposes.

Various security concerns were noted with the user accounts established with access to the eMARS production databases, as follows:

1. There were seven instances where a user had two accounts present within the production databases. After informing Commonwealth Office of Technology (COT) staff, the unnecessary account was subsequently removed for all seven users.
2. There were two users with unnecessary roles granting greater than Read access to the base tables in the ePayment Gateway database. Access rights for one of these users was subsequently reduced to Read Only.
3. There was one user with an unnecessary role granting greater than Read access to the base tables in the Finance and Administration and Vendor Self Service databases.
4. There were two users with unnecessary roles granting greater than Read access to the base tables in all three databases: ePayment Gateway, Finance and Administration, and Vendor Self Service. Access rights for one of these users was subsequently reduced to Read Only for two of the three databases—Finance and Administration and Vendor Self Service.
5. Specific to the four users with access to the ePayment Gateway database noted above, they also have administrator rights with the ePayment Gateway application and can process transactions therein.
6. Regarding the three Finance and Administration users noted above, they also have been granted the administrator role within the eMARS application and can approve documents therein.
7. There were 21 unduplicated user accounts with unnecessary access to the RESOURCE role within the Finance and Administration, Vendor Self Service, and infoAdvantage databases. The RESOURCE role is typically used by designers only and is not required for all database users. After informing COT staff of this situation, these users were subsequently removed from the RESOURCE role.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-22: The Finance And Administration Cabinet Should Develop And Implement Formal Policy And Procedures To Govern The Security Of The eMARS Production Databases (Continued)

8. The PUBLIC account was granted greater than Read privileges to five production tables within the Finance and Administration database. The PUBLIC account is a default Oracle account whose rights are automatically inherited by all database users. After informing COT staff of this situation, these privileges were subsequently revoked for the PUBLIC account.

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. When users have the ability to initiate and approve transactions within the application, an improper segregation of duties results when they also have the ability to directly effect changes to the base tables on the database servers.

Established security policies and procedures should be 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 system resources as required for completion of assigned job functions. A proper segregation of duties requires that system users that have authority to initiate and approve documents should not be provided direct access to related databases that could allow them the ability to alter receipts or payment data.

Recommendation

We recommend FAC develop and implement formalized logical security procedures to ensure that only authorized access is granted to the ePayment Gateway, Finance and Administration, Vendor Self Service, and infoAdvantage production databases. These procedures should require that the COT-F181 forms are complete and signed. Furthermore, emails accompanying the COT-F181 forms should be retained for audit purposes or some other means should be established as proof of the originating approval. In addition, all production database accounts should be monitored to ensure that no unnecessary accounts exist and that the roles and privileges assigned to each user are appropriate. In order to avoid an improper segregation of duties, users with the ability to create and approve documents within the ePayment Gateway and eMARS applications should be restricted to Read-Only access within the production databases.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-22: The Finance And Administration Cabinet Should Develop And Implement Formal Policy And Procedures To Govern The Security Of The eMARS Production Databases (Continued)**

Management's Response and Corrective Action Plan

We have reviewed the users with access to the production databases and verified the following: a user has only one ID in each database and the access (view, update, and/or delete) is correctly assigned. For new users to obtain database access an F-181 form must be completed and a Remedy ticket must be logged (and subsequently assigned to the COT DBA Support team).

The form will include the user ID, name of user, type of access requested and the reason for the request. The F-181 form and Remedy ticket will be completed by either Jennifer Robertson, Donald Sweasy or Diana Holberg.

Additionally, SAS will conduct a periodic review (quarterly) to ensure only authorized users have been granted access to the production databases.

There are two users in SAS (Jennifer Robertson and Donald Sweasy) who currently have update access in the application and in the production database. There are a number of tasks these two users do in the online application that requires them to have UPDATE access. Also, there are issues/problems that occur that sometimes cannot be fixed in the online application and require database updates. These updates are usually needed to fix problems in the functional areas where these two users have a considerable knowledge base.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-23: The Finance And Administration Cabinet's Password Policy Should Be Consistently Applied To All eMARS Production Databases

During the FY 2007 audit of the Finance and Administration Cabinet (FAC), it was determined that the password policies established for the Enhanced Management Administrative and Reporting System (eMARS) production databases user profiles do not provide adequate protection of the databases and are not in compliance with the Commonwealth Office for Technology (COT) standards.

There are two user profiles utilized for the eMARS production databases: a default profile and a user profile. The default profile was designed to be the most restrictive profile; however, the current password lifetime for the default profile is unlimited, which is not in compliance.

The user profile, on the other hand, was designed as the profile for users that require non-expiring passwords. Non-expiring passwords are requested through submission of the COT-F085 Security Exemption Request Form. Only one of the tested 64 user accounts with an established user profile in the eMARS production databases had a properly completed and authorized COT-F085 form on file. Furthermore, one of the 63 user accounts without a properly approved authorization form on file was a database administrator account. Finally, we noted that none of these user profiles established with production database access had any of the password complexity rules implemented to control the strength of the passwords used.

Additionally, it was determined that clear-text passwords are stored and transmitted within scripts used during the creation of the infoAdvantage database from the Finance and Administration database. InfoAdvantage is used for reporting purposes for eMARS transactions.

If password policies are inconsistently applied, the agency could potentially be vulnerable to unauthorized access or disruption of service caused by an intruder. Passwords for sensitive database access should be established using strict, complex password rules. Passwords that are stored and transmitted over the State network within clear-text increase the risk that those associated critical user accounts could be compromised.

Passwords are a significant feature to guard against unauthorized system access. The purpose of a password policy is to establish a control standard to create strong passwords, to protect those passwords, and to ensure passwords are changed within a specified time period.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-23: The Finance And Administration Cabinet's Password Policy Should Be Consistently Applied To All eMARS Production Databases (Continued)

Recommendation

We recommend FAC review the list of users granted a profile with a non-expiring password to ensure that there is a business-related purpose for the exemption and that a complete and authorized COT-F085 form is on file on behalf of each user. FAC should also review the established user profiles within the eMARS production databases to ensure that the accounts with non-expiring passwords are segregated from the other user accounts so that different password rules can be applied to each group of users.

Authorized users with non-expiring passwords, despite having no maximum password age, should be forced to create strong passwords through implementation of complexity rules. All other users should have a password lifetime in compliance with the 31-day COT standard. FAC should also ensure that a method is established to allow all passwords within the truncate and append scripts to be stored and transmitted in an encrypted manner.

Management's Response and Corrective Action Plan

COT has made some changes and there are 3 profiles now

- 1. Default--Used for users with most restrictive privileges.*
- 2. Users_profile--Used for All other users.*
- 3. User_profile--Used for application ids and/or userids requiring non-expiring password only.*

*The **default profile** has the password verification turned on. The history of the all passwords are kept for 1800 days and the accounts are locked after 3 unsuccessful attempts for unlimited days.*

*The **Users profile** has password verification turned on. The password expires every 30 days and has 5 day grace period before the account is locked. The password history is kept for 360 days . The account will be locked after 3 unsuccessful attempts for unlimited days.*

*The **User_profile** has users with exempted passwords. We create these ids with strong passwords.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-24: The Finance And Administration Cabinet Should Strengthen Input Validation Controls Over eMARS Machines

During the security vulnerability assessments for FY 2007, our examination discovered java script files that, when reviewed, showed that client-side input validation controls were in place on two critical machines related to the Enhanced Management Administrative and Reporting System (eMARS) administered by the Finance and Administration Cabinet (FAC). Through this review, we identified specific validation procedures being performed on the client-side of communications with these machines. Our testing revealed that a client could circumvent the client-side input validation controls when communicating with both machines. Further, our testing revealed that these validation procedures are not being performed on the server-side to ensure that input received from the client is acceptable and valid.

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.

If a web service allows client-side material to be submitted without first verifying its type, size, format and content, there is an increased risk that the web service, the host operating system, and other hosts on the network could be the target of attack such as cross-site scripting or denial of service attacks.

To minimize the risks that improper input validation causes, the client must not be able to easily circumvent those safeguards. While input validation can be implemented at the client-side, they must be reiterated at the server-side.

Recommendation

We recommend Finance review the input validation at both the client-side and server-side related to eMARS and applicable critical machines to ensure that the controls are enforced at least as stringently on the server-side as on the client-side. If these controls are not available on the server-side, then Finance should work with CGI to implement comparable controls on the server-side.

Management's Response and Corrective Action Plan

CGI-AMS will be consulted on this matter and will work with COT to implement any needed changes.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-25: The Finance And Administration Cabinet Should Improve Logical Security Over The UNIX Servers

During the FY 2007 audit of the Finance and Administration Cabinet (FAC), it was determined that improvements should be established over the logical security controls of eMARS UNIX servers. We tested the security controls established for three UNIX servers determined to be critical to Enhanced Management Administrative and Reporting System (eMARS) processing. Various security related control weaknesses were noted during the audit as detailed below.

Security Policy and Procedures Documentation

We examined two documents used by FAC's Commonwealth Office of Technology (COT) to address UNIX security policy and procedure communication and guidance. These two documents were entitled Standard Password Restrictions for AIX/Solaris and Creating a New AIX User (Non-SP). Our examination of these documents revealed:

- The documents had not been reviewed and/or updated by COT since 2004.
- The policy documents did not adequately address user responsibilities nor did they specify proper procedures for documentation required for access authorizations, prohibitions against password sharing, requirements for the use of single user ID's, and procedures for requesting deviations from established policy.

User Access Accountability and Authorization

Four issues were noted from an examination of user accounts and documented access authorizations.

- Documentation for user access authorizations was inadequate for the three servers. We tested access authorization forms for the thirteen (13) active users on each of the three servers. Only two authorization forms were provided by COT for the thirteen tested active users. Neither of these forms was properly completed. No authorization forms were provided for the remaining eleven (11) active users.
- One user ID (UID) was found with active access to one tested server according to the password file (/etc/passwd) and the security password file (/etc/security/passwd). However, our examination revealed this user did not require the access and no authorization for the access was provided.
- One UID was noted that is a UNIX Team administrator level account used for system support and is directed to the root home directory. Per COT, this account was created to allow the UNIX Team an alternate way to gain access if for some reason they were unable to access their regular account. The password was shared and any user utilizing this account gains superuser (root) privileges and may perform superuser

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-25: The Finance And Administration Cabinet Should Improve Logical Security Over The UNIX Servers (Continued)

(root) tasks without leaving an adequate audit trail as to who performed the task. This issue creates the potential for unauthorized activity through this account.

- In most cases, to disable a user from server access, COT would remove the UID from the password file, but refrain from disabling the UID residual user files by removing them from the security password file. Our testing revealed users that were no longer active users but are still listed as active within the security password file for each of the three tested UNIX servers. Two of these servers were found with eleven (11) users that should be disabled (4 of which were locked out), while one server contained twelve (12) users that should be disabled (4 of which were locked out).

Additionally, nine (9) users were found within each of the three servers tested that contained disabled passwords on the security password file. These nine (9) users appeared as active on the password file, and should be removed or disabled from that file.

Lastly, two of the three servers tested contained seventeen (17) system accounts with active passwords on the security password file but were not found on the password file. The other server tested contained eighteen (18) system accounts with active passwords that were not included on the password file. These systems accounts with active passwords should be reviewed for necessity, and disabled on the security password file if unnecessary.

Default Security Options

The last password change date was reviewed for all active users to determine if the password has 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 that reveal that these noted users are not being required to comply with established password policies:

- Three (3) users on one server were found to have logged on although they had not changed their password within the 35-day policy.
- Four (4) users on each of the other two servers were found to have logged on although they had not changed their password within the 35-day policy. Three of these users are the same users noted for the server above.

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 issues:

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-25: The Finance And Administration Cabinet Should Improve Logical Security Over The UNIX Servers (Continued)

	Option policy	Deviations
<i>servers:</i>	su = true, except for <i>root</i>	All three server default options were set as <i>su=false</i>
	rlogin=false for <i>root</i>	One server allowed remote login to root
<i>user files:</i>	histsize=15 passwords	Five users accounted for no password history (histsize = 0)
	minother=3 new characters required for new password	One user account required no new password characters (minother = 0)
	maxexpired = 1 week	One user accounted at unlimited (- 1) maximum number of weeks after maxage (35 days) that an expired password can be changed by a user
	maxage = 5 weeks (35 days)	Two users accounts required no maximum password age (maxage=0); One users max password age was set to 15 weeks

We noted that the file permissions for the /etc/inittab system file, which was noted on all servers, did not comply with industry best practices. The /etc/inittab system file is responsible for processes when the system is booted. Industry best practice recommends the permissions to this file be set to read/write for only the owner (-rw-----). Our review revealed that the current setup allows the owner read/write access, and, against industry best practice, provides read access to groups and others (-rw-r--r--).

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. Access should only be granted to system resources as required for completion of assigned job functions and user account settings should be established using industry best practices.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-25: The Finance And Administration Cabinet Should Improve Logical Security Over The UNIX Servers (Continued)

Recommendation

We recommend FAC management ensure that COT develop and implement formalized UNIX logical security policy and procedures that address user responsibility and accountability, ensure secure user and password default options, prohibit account sharing, and establish proper procedures for handling incidents and deviations from the implemented security policy. These security policies and procedures should ensure that a COT-F181 form is required for all user access to the critical eMARS UNIX servers. These forms should be appropriately completed, authorized, and maintained. All UNIX server user accounts should be monitored on a regular basis to ensure unnecessary accounts are disabled in the password file and the residual files, and to ensure the established user security options conform to policy and industry best practices.

Management's Response and Corrective Action Plan

Security Policy and Procedures Documentation

A review of the Standard Password Restrictions for AIX/Solaris and the Creating a New AIX User (Non-SP) documents revealed that these were for internal use and are not adopted COT policies. Security Services has requested that the UNIX Team review the internal working documents and update them to industry best standards.

User Access Accountability and Authorization

The UNIX Team will follow the already established procedures requiring an F-181 before granting access for users.

Default Security Options

The UNIX Team has set the user accounts to expire in the 35-day policy recommendation. Any user accounts that need an extension to this policy will require a security exemption to be filled out and approved by Security Services.

Regarding the following specific security options:

- The "su " option – The document stating this setting was an internal working document and not an adopted COT policy. The UNIX Team will review and update the document to the industry best practices.*
- The "rlogin" option – COT has corrected this issue.*
- The histsize option – COT management will ensure that COT User ID/Password Policy is followed in the future.*
- The minother option – COT UNIX Team will review these settings and correct them to meet the User ID/Password Policy.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-25: The Finance And Administration Cabinet Should Improve Logical Security Over The UNIX Servers (Continued)

Management's Response and Corrective Action Plan (Continued)

- *The maxexpired option – COT UNIX Team will review these settings and correct them to meet the User ID/Password Policy.*
- *The maxage option – COT UNIX Team will review these settings and correct them to meet the User ID/Password Policy.*

Related to the iniitab user account, the COT UNIX Team will make the recommended changes.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-26: The Finance And Administration Cabinet Should Strengthen System Assurance Procedures Between Production And The Data Warehouse**

Our audit of the Finance and Administration Cabinet (FAC) system assurance processes governing the Enhanced Management Administrative and Reporting System (eMARS) revealed out of balance conditions between eMARS production data and the data warehouse that is updated with production data and ultimately used for financial reporting by multiple agencies.

Production data updates the eMARS data warehouse that is used for reporting by both the Finance Cabinet and Departments statewide. In addition to the data warehouse there are production ledgers that are used for reporting. One example is the ledger customized by the Finance and Administration Cabinet to represent the Commonwealth's trial balance, O_FIN.LDGR_003. This custom ledger and the data warehouse are both updated with the data from the same production ledger, O_FIN.JRNL.ACTG.

Review of the summary trial balance data extracted from the production ledger O_FIN.LDGR_003 and summary trial balance data extracted from the General Accounting Universe within the data warehouse revealed discrepant amounts within 34 of 46 funds. There were several instances where the entry within the production table was not found in the data warehouse. Discrepancies within 24 of the funds were inter-fund discrepancies between closing classifications and/or balance sheet class amounts that ultimately zeroed out in total by fund. The remaining 10 funds were discrepant in total by fund for over negative \$110 million.

Follow-up with the Finance and Administration Cabinet indicated this was an out of sync issue that they are aware of and that during the time of our fieldwork had taken action to investigate and request remedy; however no action had taken place to date.

Weak system assurance processes governing production and reporting data hinders the integrity of data relied upon for reporting used for management decision purposes.

Strong system assurance processes assure that data is complete and accurate and that any noted issues are resolved and corrections to data are made in a timely manner.

Recommendation

System assurance procedures within and between eMARS production data and the data warehouse should be strengthened to ensure the data is properly synchronized and in balance. Further, we recommend Finance identify all instances where the data warehouse is out of sync with production and make adjustments to the warehouse data accordingly.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-26: The Finance And Administration Cabinet Should Strengthen System Assurance Procedures Between Production And The Data Warehouse (Continued)**

Management's Response and Corrective Action Plan

The O_FIN.LDGR_003 has still yet to be re-built, but is not currently in use. We still intend to re-build it as it is a convenient source for the trial balance. We have just accepted a patch re-building the Summary Table A in the DW keeping them it sync with the DW Journal. A discrepancy with Summary Table B is under investigation. Discrepancies between the production journal and the DW journal has been identified and is recorded as an incident. We are awaiting an infoadvantage baseline systems assurance process to be delivered.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-27: The Finance And Administration Cabinet Should Develop And Formalize Guidance Concerning Approval Rules Related To The eMARS Applications

Our audit of the Finance and Administration Cabinet (Finance) revealed that there are instances where the security surrounding documents within the Enhanced Management Administrative and Reporting System (eMARS) Advantage Financial application would allow an individual to place an approval on a document that he/she created or submitted. This security feature is established on the approval rule associated with each document code, which can be customized to place the restriction at the department, or lower, organizational level. At the time of our review, there were 2,594 different approval rules where the “Self-approval?” field within the approval rule was set to “no restriction,” which would allow the creator or submitter of the document to also approve the document to the extent that the user’s access rights would allow. There were 52 individual document codes that had at least one approval rule established that would allow self-approval without restriction.

There are three valid settings that can be placed within the “Self-approval?” field: “no restriction”, “submitter restricted”, and “creator/submitter restricted.” Although Finance does not allow the “no restriction” setting to be used on document codes related to payments, there is no formal policy or guidance discussing under what circumstances each of the valid settings would be appropriate or specifically disallowed.

Failure to properly restrict authority to processing eMARS documents, either intentional or through a lack of understanding of security controls, increases the risk of unauthorized access, modification to computer data or the submission of fraudulent transactions.

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 systems. Further, management should ensure that a proper segregation of duties is in place regarding the origination and approval of documents.

Recommendation

We recommend Finance develop and formalize guidance to address the “Self-approval?” field on the approval rules and the associated valid values for this field. This guidance should also address situations where the “no restriction”, “submitter restricted”, and “creator/submitter restricted” options would be appropriate and specifically disallowed. Further, we recommend that Finance review the current approval rules where the “Self-approval” value is set to “no restriction” to determine if these documents need to be more strictly controlled. If situations are discovered where the “no restriction” option is not appropriate, Finance should work with agencies to revise the affected approval rules.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-27: The Finance And Administration Cabinet Should Develop And Formalize Guidance Concerning Approval Rules Related To The eMARS Applications (Continued)**

Management's Response and Corrective Action Plan

*The "self-approval" field is set to either **submitter-restricted** or **creator/submitter restricted** for all payment documents in the application (GAX, GAX2, GAX3, TP, PRC, PRCI, IN, MD). This means the last person to "touch" a document while in EDIT mode...Draft phase...will not be allowed to approve a document that they submit. They won't even be allowed to remove it from the Role Worklist.*

Currently, the payment documents are the only documents where we have enforced the "submitter-restriction" on the approval of the documents. The agency heads/agency security officers have determined what restriction, if any, they want to have on their other documents. The majority of the documents currently have the submitter-restriction in place. There are just over 10,000 + approval rules in the application and 68% of them are set up so that the submitter cannot approve documents he submits.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-28: The Finance And Administration Cabinet Should Strengthen The Controls Over The Payee Vendor Field

Our audit of the Finance and Administration Cabinet (Finance) revealed that the PRC (Commodity Based Purchase Request) document within the Enhanced Management Administrative and Reporting System (eMARS) system is designed to allow payment to a vendor other than that related to the Vendor/Customer Code entered onto the document. This document will allow the user to enter a Payee Vendor code, which will supplant the Vendor/Customer Code on the document when an automatic disbursement or electronic transfer of funds is created related to the document. This lax control over the vendor to be paid from the PRC document would even allow the document creator to enter his or her own eMARS ID in the Payee field, which would cause the payment to be issued to the document creator.

Through discussions with personnel from other departments, our examination discovered an instance of this situation occurring within the new eMARS system. Within the example noted, the user had created the document with the accurate Vendor/Customer Code and related it appropriately to the associated master agreement. However, the user then inadvertently placed his/her eMARS user id in the Payee Vendor field on the Document Header. System edits were not implemented to ensure that the changed payee information appeared valid or reasonable. Once the document was validated and went through the appropriate approvals, an electronic funds transfer was issued to the user's bank account. In this instance, the user contacted department management to report the error.

The allowance of the Vendor Customer to be supplanted by the Payee Vendor within the PRC document heightens the risk of errors and the risk that valid transactions could be altered to perpetrate a fraud. Even if the alteration is unintentional, the allowance of this change in payee can cause serious problems with ensuring timeliness of payment to vendors and inefficiencies resulting from required error correction processes.

Document edits should be in place to ensure payments are issued to the appropriate vendor.

Recommendation

We recommend Finance work with CGI to remove the Payee Vendor field on the PRC document. Further, a review of all PRC documents should be performed to ensure that the responsible department could support any payees that were changed from the original vendor. Any instances of potential fraud should be reported to the appropriate department management.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-28: The Finance And Administration Cabinet Should Strengthen The Controls Over The Payee Vendor Field (Continued)**

Management's Response and Corrective Action Plan

The payee functionality is baseline for certain procurement documents. Based on the way our vendor file was converted, it is necessary to be able to pay different vendor numbers than are on the face of the contract. While different payment addresses are the primary need, multi-vendor contracts such as tire contracts requiring many different vendors to be paid off the contract is an issue. Any change to this functionality would have to be submitted to the CGI-AMS Client Advisory Committee for consideration.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-29: The Finance And Administration Cabinet Should Ensure eMARS Fixed Assets Are Converted Completely And Accurately

Our FY 2007 audit of the Finance and Administration Cabinet (Finance) revealed that adequate documentation was not readily available to support the conversion of the Fixed Assets Balance Sheet Accounts (BSA) from the Management Administrative and Reporting System (MARS) to the enhanced Management Administrative and Reporting System (eMARS). Using the file that contains ending account balances in MARS, the auditor was able to reconcile numerous MARS BSAs that were converted to an eMARS BSA Class. However, Fixed Assets BSAs were converted separately through Pervasive Data Integrator (PDI) maps. Finance could not provide documentation supporting the conversion of Fixed Asset balances during the course of fieldwork. Therefore, a determination could not be made as to whether these balances were converted completely and accurately.

Without adequate documentation to support fixed-asset data conversions from MARS to eMARS, Finance and others relying on the data are not be assured the conversion was properly completed without applying additional efforts, which results in inefficiencies and an increased possibility that data was improperly converted.

The data conversion process should ensure that Chart of Accounts (COA) elements and closing balances have been converted completely and accurately from the MARS system into the new eMARS system with minimal disruption to agencies. To ensure balances are converted completely and accurately, documentation of the conversion and reconciliation process should be maintained to support the balances converted and testing performed to ensure completeness and accuracy of the data within the new system.

Recommendation

We recommend Finance perform reconciliation procedures to ensure the Fixed Asset balances as reported in MARS were completely and accurately converted to eMARS. The data and documentation used to perform this reconciliation should be maintained for audit purposes.

Management's Response and Corrective Action Plan

All CAFR reportable real property is being reconciled on an agency by agency basis. A spreadsheet log of FY 2006 property that did not convert is being maintained with the document numbers. CAFR reportable personal property is being compared from ending balance to converted balance and we have covered most of the departments and expect to be complete by mid September 2007.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-30: The Finance And Administration Cabinet Should Develop And Implement A Policy Governing The Security Of Microsoft Outlook Public Folders

During FY 2007, the Auditor of Public Accounts discovered a significant security vulnerability that potentially allowed confidential and other information to be available to thousands of individuals having email access on the state's network. This information was available by accessing agency email folders listed under the heading, "public folders." We identified two "public folders" related to agencies within the Finance and Administration Cabinet (Finance).

Our review of one of these Finance public folders identified eight subfolders in which either sensitive or confidential information was present. The following specific items of concern were noted:

- Within one of the subfolders we found three emails that had file attachments with the social security numbers of employees listed.
- Within one of the subfolders we found an email that had an attachment that appears to be a listing of the employees of a certain state agency. This listing included employee IDs and social security numbers.
- Within two of the subfolders we found emails listing a user's eMARS ID and the associated reset password.
- Within three of the subfolders we found emails listing a user's Procurement Desktop (PD) user ID and the associated reset password.
- Within one of the subfolders we found four emails providing the password reset for a VISA Procurement Card user account.

As soon as these items were found, we notified Finance management. Although attempts were made by the agency and the Commonwealth Office of Technology (COT) to remediate the situation, it took Finance nearly two weeks to adequately secure all of these subfolders. This delay was caused by uncertainty as to who was responsible for administering the security over the folders and how to specifically secure the public folders.

The review of the second Finance public folder, which is related to COT, revealed several subfolders where the permissions for the Default or Anonymous settings were established as other than "None." The following settings for subfolders were noted:

- One contact list and one email folder with the permissions of Owner. As the folder owner, the user could create, read, and delete items, edit items, and create subfolders.
- Four email folders with the permissions of Publishing Author. As the publishing author, the user could create and read items, create subfolders and edit or delete items that the user owns.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-30: The Finance And Administration Cabinet Should Develop And Implement A Policy Governing The Security Of Microsoft Outlook Public Folders (Continued)

- One calendar with the permissions of Custom. With the custom permission, the user could read, create and delete appointments.
- One calendar with the permissions of Contributor. As a contributor, the user could create appointments.
- One email folder and one calendar with the permissions of Reviewer. As a reviewer, the user could read items only.

As soon as these items were found, we notified the COT management. Remediation of those items that were improperly secured took place within four days of notification.

The permissions granted to these folders could allow an individual to not only read the content of a folder, but also to potentially create, delete, or modify the content of a folder.

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 immediately to ensure confidential information is properly secured and that any violations resulting from the inappropriate disclosure of information be reported:

- Finance should review the CIO Enterprise Policies, such as the CIO-060 Internet and Electronic Mail Acceptable Use Policy, and ensure compliance with requirements.
- Finance should develop a policy statement and specific procedures related to agency personnel responsibilities related to the security of public folders.
- Finance should designate specific agency personnel to administer the security access control permissions applied to public folders.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-30: The Finance And Administration Cabinet Should Develop And Implement A Policy Governing The Security Of Microsoft Outlook Public Folders (Continued)**

Recommendation (Continued)

- Specified agency personnel should consistently review, on a regular basis, the security control permissions applied to public folders. Further the content within public folders should be reviewed to ensure that all items are appropriate.
- Finance should report to all appropriate agencies or individuals that confidential information was potentially disclosed. Those requiring notification could include, but not be limited to:
 - Individuals whose social security numbers, health, or other personal information was accessible.
 - State or federal agencies that may require notification of the potential disclosure of confidential information.

Management's Response and Corrective Action Plan

As a result of this discovery COT sent out two directives regarding the use, setup, and maintenance of Outlook/Exchange Public Folders. These directives required immediate remediation of sensitive or confidential data available through public folders and established high level guidelines as well as requested agencies develop their own internal procedures to aid in the prevention of accidental disclosure of information.

Finance CRC Remediation Steps

- *Establish alternatives to using public folders*
- *Clear all existing public folders of outdated information*
- *Notify staff of the appropriate use of the folders*
- *Assign two members of our management staff as owners of these folders responsible for overseeing proper use of these folders*

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-31: The Finance And Administration Cabinet Should Monitor Contracts To Ensure Vendor Compliance With Terms Specified In The Contract**

An audit finding was issued during the FY06 audit as a result of FAC's noncompliance with the post-award requirements of the Pepsi Cola North America contract. The auditor requested documentation of the vendors' compliance with the post-award requirements to review the post-award monitoring process in place for FY07 and to determine if recommendations of the 2006 finding had been implemented. After repeated inquiry, the Finance and Administration Cabinet did not provide the auditor with documentation indicating that post-award requirements had been met for the contract.

This is the second year that auditors could not verify that FAC had monitored the contract. Despite this FAC has renewed the contract each year.

The specific post-award requirements of the Pepsi contract are:

- Section 30.030: documentation that the marketing requirements of the contract were followed and properly implemented.
- Section 30.040: verification or documentation provided for the required In-Kind Services. The proposed cost to the commonwealth for these services is stated in the contract as no less than \$725,000 per year.
- Section 30.140: requires an agency participation list, volume report for scholarships awarded, and product usage report (specific details below).

FAC did not provide requested documentation that the vendors had complied with the above post-award requirements.

Since no documentation of the above post-ward requirements was provided to auditors, we conclude that the documentation may not exist, and that FAC has not adequately ensured that the vendors provided services stipulated in the contract. Further, the contract was renewed for an additional year during FY07 presumably without considering whether the vendors complied with the requirements of the contract, or reviewing documentation to determine whether the Commonwealth received expected benefits from the vendors.

Section 30.030 of the contract states:

Vendors shall invest monies annually in a marketing program with the Commonwealth of Kentucky. Each Vendor will have staff dedicated to working with the Commonwealth to promote the Vendor's Product and the Kentucky Unbridled Spirit Brand.

All marketing programs will be designed, implemented and mutually decided upon to create an increased demand for the Product and to extend the branding message of the state.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-31: The Finance And Administration Cabinet Should Monitor Contracts To Ensure Vendor Compliance With Terms Specified In The Contract (Continued)**

For these considerations, each Vendor will be allowed to refer to itself in all marketing, public relations, sales efforts during the life of the contract, as the Contract Holder for Soft Drinks of the Executive Branch of State Government.

The Commerce Cabinet agrees to provide the vendors (collectively) with \$40,000 worth of lodging at various state resort parks based on availability at any time during the year. Each drive away lodging package includes a three (3) day two (2) night stay. Additional drive away packages can be purchased at the published Commonwealth employee rate at the time of purchase.

Section 30.040 of the contract states:

Together the Vendors shall provide the following in-kind services to the Commonwealth, totaling approximately \$729,500 PER YEAR, but in no case would the approximation be less than \$725,000.

Radio and television spots associated with the University of Kentucky, University of Louisville and Western Kentucky University during football and basketball seasons. Estimated value = \$35,000

The Unbridles Spirit Logo will be advertised on the back of 150 delivery trucks a minimum of once a year. Estimated value \$32,5000

The Unbridled Spirit Logo will be placed on point of sale material, such as pole signs and shelf signage, in high-traffic retail locations. Estimated value = \$2,000

The Unbridled Spirit Logo will be placed on various products (cans, bottles, etc.) To be distributed throughout the commonwealth at various times during the year. Estimated value = \$650,000

The vendor will co-partner with a restaurant associate to provide coupons linked with the Kentucky state parks. Estimated value = \$10,000

Section 30.140 of the contract states:

One of the most important tools to monitor the contract's size and usage is by comprehensive reporting. This reporting will include each vendor's figures to include state agencies and political subs referencing the contract.

Below is a list of the reports that the Office of Material and Procurement Services requires each Vendor to provide an the frequency schedules:

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-31: The Finance And Administration Cabinet Should Monitor Contracts To Ensure Vendor Compliance With Terms Specified In The Contract (Continued)

AGENCY LIST

This report shall be a comprehensive list of all of the agencies and locations that are using the Soft Drink contract. This list shall include the name of the agency, the location, the county that it is located in and the account number of other identifying number used in billing. This report needs to be in Microsoft Excel format with each of the above as columns so that the Commonwealth personnel using these reports can sort the data in various ways for use in tracking agency participation. This report is required on a QUARTERLY basis until such time as the frequency may be changed. This report needs to be sent to the Commonwealth buyer on the 1st day of the second month following the quarter in question.

VOLUME REPORT

This report shall be a comprehensive list of data from each Vendor. This report shall include the following data elements: amount of scholarships provided during the year broken out by Governor's Scholars Program and the Office for the Blind; a list of the In-Kind Services provided during the year with a monetary dollar amount tied to them; the total amount of Commissions paid to the Commonwealth broken down by the agency and location and the means by which it was calculated so that the Commonwealth can reconcile that amount. The above report elements can be in a Microsoft Word document.

PRODUCT USAGE

To be created in Microsoft Excel format. The report shall show the total amount paid for Product by the Commonwealth to be broken down by the following columnar headings:

Agency name

Agency location (address)

County located in

Specific use areas such as a specific State Park broken out by dining room, golf course, boat dock, campground, etc.

Product category such as 12 ounce CSD, 2 liter CSD, etc.

Usage per each category above in case quantities

Dollar amount paid for those cases

Each of the Product Usage reports shall show a grand total of how many cases per Product category is being purchased, and a total dollar amount the Commonwealth is spending on Product. This report shall be submitted to the commonwealth buyer on a QUARTERLY basis in

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-31: The Finance And Administration Cabinet Should Monitor Contracts To Ensure Vendor Compliance With Terms Specified In The Contract (Continued)**

Microsoft Excel format for ease of rearranging the data and distribution to other Commonwealth personnel.

Recommendation

We recommend FAC:

- Contact the vendor and request submission of the reports required by section 30.0140;
- Contact the Commerce Cabinet to determine if the drive away lodging program was implemented and evaluate the success of the program;
- Implement a system to monitor contracts for appropriate delivery of services, including development of policies and procedures to communicate monitoring requirements to user agencies for agency-specific contracts;
- Consider including penalties such as the withholding of payment or fines as a consequence for failure to comply with post award requirements.

Management's Response and Corrective Action Plan

- *Contact the vendor and request submission of the reports required by section 30.0140;*
 - *The in-kind services report was received from Pepsi on October 4, 2007. Pepsi reports \$783,666.76 worth of in-kind services being provided for the 2007 reporting period. This amount exceeds the contract requirement that the vendors shall provide in-kind services to the Commonwealth, totaling approximately \$729,500 PER YEAR, but in no case would the approximation be less than \$725,000.*

Scholarship checks for the Governor's Scholars Program (\$30,000) and the Office for the Blind (\$20,000) were received November 20, 2007.

The vendor representative is coordinating with the bottlers to compile data needed for the remainder of the reports required by section 30.140. The Office of Procurement Services' buyer will continue to monitor this activity.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-31: The Finance And Administration Cabinet Should Monitor Contracts To Ensure Vendor Compliance With Terms Specified In The Contract (Continued)****Management's Response and Corrective Action Plan (Continued)**

- *Contact the Commerce Cabinet to determine if the drive away lodging program was implemented and evaluate the success of the program;*
 - *The Commerce Cabinet provided the spreadsheet below. The Drive Away program generated 981 stays for 1975 nights from November 1, 2005 through November 15, 2007. Commerce also reports that the program worked quite well. The original timing was a little off, because they ran the offer at different times in different places. However, we feel we got full value from the program.*

<i>Park Name</i>	<i>Stay</i>	<i>Nights</i>
<i>Barren River State Resort Park</i>	<i>69</i>	<i>141</i>
<i>Blue Lick State Resort Park</i>	<i>39</i>	<i>75</i>
<i>Buckhorn Lake State Resort Park</i>	<i>27</i>	<i>56</i>
<i>Carter Caves State Resort Park</i>	<i>76</i>	<i>153</i>
<i>Cumberland Falls State Resort Park</i>	<i>93</i>	<i>185</i>
<i>Dale Hollow State Resort Park</i>	<i>65</i>	<i>130</i>
<i>General Butler State Resort Park</i>	<i>71</i>	<i>140</i>
<i>Greenbo Lake State Resort Park</i>	<i>46</i>	<i>99</i>
<i>Jenny Wiley State Resort Park</i>	<i>7</i>	<i>14</i>
<i>Kenlake State Resort Park</i>	<i>48</i>	<i>98</i>
<i>Kentucky Dam State Resort Park</i>	<i>60</i>	<i>129</i>
<i>Lake Barkley State Resort Park</i>	<i>69</i>	<i>143</i>
<i>Lake Cumberland State Resort Park</i>	<i>161</i>	<i>319</i>
<i>Natural Bridge State Resort Park</i>	<i>52</i>	<i>98</i>
<i>Pennyrile State Resort Park</i>	<i>8</i>	<i>17</i>
<i>Pine Mountain State Resort Park</i>	<i>39</i>	<i>75</i>
<i>Rough River State Resort Park</i>	<i>51</i>	<i>103</i>
	<i>981</i>	<i>1975</i>

- *Implement a system to monitor contracts for appropriate delivery of services, including development of policies and procedures to communicate monitoring requirements to user agencies for agency-specific contracts.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-31: The Finance And Administration Cabinet Should Monitor Contracts To Ensure Vendor Compliance With Terms Specified In The Contract (Continued)

Management's Response and Corrective Action Plan (Continued)

- *Policy and procedure for monitoring contracts currently exist. FAP-11-51-00 of the Finance and Administration Cabinet, Manual of Policies and Procedures addresses using agency contract administration:*

FAP 111-51-00

CONTRACT ADMINISTRATION

1. ***General:*** *The Office of Material and Procurement Services shall rely on the using agency to ensure the contract is being completed or executed as written. If any post-contract problem, deviation, change, or delay arises that is not provided for in the contract, the matter shall first be handled between the using agency and vendor.*

If the using agency cannot reach a satisfactory resolution with the vendor, the agency shall refer the matter to the Office of Material and Procurement Services in accordance with the provisions of FAP 111-42-00, Vendor Complaints.

2. ***Authorities:*** *An using agency shall not allow any change to the terms of a contract without proper authorization from the issuing agency. Agencies shall document problems that may require contract changes, price adjustments, quantity variations, alternate items or delinquent deliveries, and forward the documents to the issuing agency. The issuing agency shall then initiate any necessary action or contract change with the vendor.*

- *OPS relies heavily on using agencies to monitor vendor performance and reporting problems that can not be resolved by the using agency. Agencies can document a vendor's performance on the Vendor Performance Evaluation (PE) document in emars. The data entered on PE documents is used to determine if vendors should receive future awards or have their existing Master Agreements renewed. Users can rate a vendor's performance (Unsatisfactory, Poor, Fair, Good, Excellent or Not applicable) based on the criteria that was loaded for the document. This process was communicated to users in training sessions during eMARS implementation.*

To this point, the using agencies have not reported any material deviations in contract performance by Pepsi.

- *Consider including penalties such as the withholding of payment or fines as a consequence for failure to comply with post award requirements.*

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-31: The Finance And Administration Cabinet Should Monitor Contracts To Ensure Vendor Compliance With Terms Specified In The Contract (Continued)**

Management's Response and Corrective Action Plan (Continued)

- *Penalties such as the withholding of payment as well as others have been used in the past on some contracts. Additionally, 200 KAR 5:312. Termination of contracts, addresses termination of contracts because of the contractor's failure to perform its contractual duties and 200 KAR 5:315 Disciplinary action for failure to perform, addresses actions that can be taken against the vendor for failure to comply with contract terms and conditions or failure to complete performance within the time specified in the contract.*

OPS has utilized the provisions referenced above and will continue to utilize them when circumstances warrant such action.

Auditor's Reply

The In-Kind report and Scholarship information referred to in FAC's response are not for the time frame requested by the auditor for the FY 2007 audit (July 1, 2006 through June 30, 2007) and do not indicate compliance with the contract's requirements for FY 2007. To date FAC has not provided these or any other requested reports related to the Pepsi contract to the auditor.

While APA recognizes FAC's reliance on using agencies to monitor performance, this does not diminish their responsibility to ensure that vendors comply with central reporting requirements. FAC should ensure that using agencies are periodically trained about post award monitoring, utilizing the Vendor Performance Evaluation, resolving conflicts and reporting problems to FAC that may require further action.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-32: The Finance And Administration Cabinet Should Ensure Contracts Are Not Improperly Extended Beyond The Renewal Periods Specified In The Original Contract**

During our testing of the Office of Material and Procurement Services (OMPS) compliance with the contract awards process, we noted four exceptions resulting from contract modifications used to initiate major changes outside of the scope of the original contracts:

- Contract C-01090447 with Motorola Inc was awarded May 1, 2001. The contract called for an initial period of one year from the date of the award, with the option to renew the contract for four additional one-year periods. Including the allowable renewal periods, this contract should have expired April 30, 2006. However this contract's expiration date was modified through July 13, 2007.
- Contract M-00062705 with FleetOne was awarded December 1, 2000. The contract called for an initial period of two years, with the option to renew up to three additional one-year periods. This contract should have expired November 30, 2005. However, this contract's expiration date was modified through August 31, 2007.
- Contract C-00348479 with Image Entry/Source Corp was awarded January 1, 2001. The contract called for an initial two-year period, with the option to renew up to two additional two-year periods. This contract should have expired December 31, 2006. However this contract's expiration date was modified to December 31, 2007.
- Contract C-01363732 with IDMS Inc. was awarded April 5, 2001. The contract called for an initial period to end June 30, 2003, with the option to renew for up to three additional one-year periods. This contract should have expired June 30, 2006. However this contracts expiration date was modified to June 30, 2007.

OMPS improperly extended these contracts beyond the extension contract renewal periods specified in the contracts. Furthermore, OMPS use of contract Modifications in effect created changes in contract terms outside the original scope, in violation of FAP 110-10-00.

Because these contracts were extended beyond the allowable renewal periods, the Commonwealth did not re-bid or renegotiate these contracts timely.

FAP 111-11-00 states:

1. A Modification shall be used to make corrections or changes to a solicitation or contract. A Modification shall not be used to:
 - a. initiate a major changes outside the original scope of the contract; or
 - b. effect a new buy that normally would be placed by competitive bid.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-32: The Finance And Administration Cabinet Should Ensure Contracts Are Not Improperly Extended Beyond The Renewal Periods Specified In The Original Contract (Continued)

The contract with FleetOne (Contract Number: M-0062705) reads in part:

1. The initial term of the contract shall be from December 1, 2000 through December 21, 2002. . . .
2. Upon expiration of the initial term of the Contract, the Contract may be renewed for up to three (3) one-year periods.

The contract with Motorola (Contract Number: C-01090447) reads in part:

1. The contract will be for the initial period of ONE (1) year from the date of award (5/1/2001).
2. This contract may be extended at the completion of the initial contract period for FOUR (4) additional one-year periods.

The contract with Image Entry/Source Corp (Contract Number: C-00348479) reads in part:

1. The contracts will be for the initial period of two (2) years from the date of award.
2. The contract may be extended at the completion of the initial contract period for two (2) additional two (2) year periods.

The contract with IDMS Inc (Contract Number: C-01363732) reads in part:

1. This contract will be for the initial period of date of award until June 30, 2003.
2. This contract may be extended at the completion of the initial contract period for three (3) additional one-year periods.

Recommendation

OMPS should review active contracts to ensure that no other contracts have been improperly extended beyond the renewal periods specified in the clauses of the original contract. OMPS should refrain from such practices in the future without authorization from the Secretary of Finance justifying the extension.

Management's Response and Corrective Action Plan

The Office of Procurement Services concurs with the findings of the APA in regard to renewal of master agreements beyond the number of periods specified in the solicitation. This practice is unacceptable as a regular course of action, and should be utilized only in extreme circumstances in which it is not possible to resolicit for a successor to be selected prior to expiration of the final renewal period. The recommendation made in this Record of Noncompliance has been fully implemented.

It has been a priority since January of 2007 to firstly, identify all master agreements that were in that status of renewal beyond the maximum number authorized and secondly to identify those agreements that were in the final authorized period.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-32: The Finance And Administration Cabinet Should Ensure Contracts Are Not Improperly Extended Beyond The Renewal Periods Specified In The Original Contract (Continued)**

Management's Response and Corrective Action Plan (Continued)

The office has been working diligently to resolicit those procurements already extended beyond the authorized life. Tremendous progress has been made, and it continues to be a top priority. The office is acting under a directive that there are to be no further extensions for any master agreement unless it is a matter of emergency as defined by statute or upon approval of the Secretary of the Finance and Administration Cabinet. Those that expire will be permitted to lapse. Those agreements in the final authorized period have been scheduled for reprourement in a timely manner to allow for the succeeding contracts to be in place upon expiration.

Of the four agreements cited, the first three have been resolicited and awarded during 2007. An RFP is currently being developed for the fourth item for Filenet services.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-33: The Finance And Administration Cabinet Should Improve Procedures Related To The Entity Removal Process Related To The CAFR Compilation

During our audit of the Commonwealth's Comprehensive Annual Financial Report (CAFR), we reviewed prior period adjustments to determine whether any beginning fund balance restatements indicated possible control deficiencies. We noted restatements impacting several funds due to mistakes made in the removal process in the previous year-end CAFR compilation process. Removals are adjustments entered into the Commonwealth's financial accounting system for the purpose of removing financial data of certain entities to avoid duplicate reporting in the CAFR. Rather than extract the financial activity for these entities from the Commonwealth's financial accounting system for CAFR reporting, the information for those entities is compiled from separately audited financial statements. The most significant restatements of beginning fund equity related to the errors in the removal process included:

- An increase approximately \$19,521,455 in the Capital Projects Fund;
- A decrease of approximately \$13,116,141 in the Federal Fund; and
- An increase in the Special Benefits Fund of \$4,840,000.

The prior period errors appear to be due to oversight in preparation of the removals, with the most significant errors being related to a single entity. Because these errors went undetected in the prior year, it indicates a control weakness in the FAC Reporting Team's compilation and review process.

Errors related to removals cause misstatements in one of two ways. First, if certain entity information is overlooked and not removed from the financial accounting system, the error creates a doubling up effect in the financial statements due to entity information reported in both the financial accounting system reports used in the CAFR compilation and also entered from the entity's separately audited financial statements. Errors may also occur if removals are performed, but capture an incorrect dollar amount or fail to capture all accounts impacted by the entity's transactions.

Proper internal controls dictate procedures be in place to ensure all financial data obtained from separately audited financial statements be removed from the Commonwealth's financial accounting system to avoid double reporting the same transactions. Also, procedures for removals should ensure that removals capture all applicable transactions for each removal entity.

Recommendation

We recommend FAC Reporting Team improve procedures related to removals to ensure that all amounts identified are complete and accurate.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-33: The Finance And Administration Cabinet Should Improve Procedures Related To The Entity Removal Process Related To The CAFR Compilation (Continued)

Management's Response and Corrective Action Plan

We are adding additional steps to the removal process to assure that the accounts removed by the reporting team, for each removal entity, are the appropriate accounts for that agency. We will add steps to assure that the accounts removed, have been included in the audited financial statements of that entity.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-34: The Finance And Administration Cabinet Should Strengthen Policies And Procedures Related To Approvals and Tracking Of State-Owned Take Home Vehicles**

We requested detailed information from the Finance and Administration Cabinet (FAC) regarding the agency requests and the approvals granted for all state take-home vehicles as of May 1, 2007, made pursuant to KRS 44.045(2). This statute stipulates that state-owned vehicles be assigned to individuals only upon the approval by the secretary of FAC of a written request made by the head of the agency. FAC was unable to provide the details of approvals granted to agencies upon our initial request.

FAC did take measures following the auditor's request to update its records by directing all agencies to submit a report of permanently assigned state take-home vehicles. Unfortunately, it took several weeks to gather and compile a complete inventory of the vehicles assigned to individuals, raising concerns as to whether the use of state take-home vehicles has been properly monitored.

Also, we noted the Kentucky Revised Statutes still authorize the Kentucky Transportation Cabinet (KYTC) to promulgate administrative regulations governing the use of state-owned vehicles, even though the responsibility was transferred from KYTC to FAC in 2006 under Executive Order 2006-679. The lag in updating the statutes and administrative regulations for this reorganization is confusing as to the specific responsibilities of FAC for inventorying and monitoring the state-owned vehicles after the reorganization.

Also, reviewing former KYTC policies and procedures regarding the use of state-owned vehicles, there appear to be current practices in place not addressed under these written procedures, such as policies for agencies that own or lease vehicles outside of the Commonwealth's fleet. These policies do not appear to have been updated for several years.

It appears that FAC oversight led to a failure to consistently track approvals granted for state-take home vehicles assigned to individuals. Changes to statutes and administrative regulations often lag behind reorganizations approved under Executive Order. We understand that FAC and the Division of Fleet Management has worked toward having the Executive Order passed into law in order to promote their ability to begin changing the administrative regulations.

Policies and procedures related to state-owned vehicles should be periodically reviewed to ensure that they address existing practice in order to provide guidance to agencies for a broad range of questions. The failure of FAC to maintain accurate records of approvals granted for assignments of state-take home vehicles increases the risk that the vehicles can be misused for other than official purposes.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-34: The Finance And Administration Cabinet Should Strengthen Policies And Procedures Related To Approvals and Tracking Of State-Owned Take Home Vehicles (Continued)**

Outdated statutes and administrative regulations that do not reflect actual government operations interfere with agencies ability to operate as intended. With the written statutory authority to promulgate administrative regulations and current administrative regulations on record currently referencing the authority of another Cabinet, the outdated information confuses the lines of authority between the KYTC and FAC in regards to the management and monitoring of state-owned vehicles.

Also outdated policies and procedures increase the risk of misuse of state-owned vehicles.

KRS 44.045 (2) states, "...The assignment of passenger motor vehicles to specific individuals shall be discouraged but may be made upon approval by the secretary of Finance and Administration Cabinet of a written request to make the assignment by the head of the agency involved."

KRS 44.045 (6) states, "...The secretary of the Transportation Cabinet may adopt administrative regulations pursuant to KRS Chapter 13A necessary to govern the use of those state-owned vehicles acquired pursuant to the provisions of this section". Although the transition of Fleet Management was approved under an Executive Order, this statute does not reflect current operations for the management of state-owned vehicles.

Recommendation

We recommend:

- FAC implement procedures to monitor and track approvals of state-take home vehicles assigned to individuals, the justification of the assignments, and other details of the assignment (agency, individual, etc).
- FAC and Division of Fleet Management continue to request the statutory authority that formally approves the Division's transition from KYTC.
- In the meantime, FAC should establish or update written policies and procedures regarding the use of state-owned vehicles, specifically addressing the approval process, intended and appropriate use of state take-home vehicles, and applicability of those procedures to agencies with independent ownership or leasing arrangements.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-34: The Finance And Administration Cabinet Should Strengthen Policies And Procedures Related To Approvals and Tracking Of State-Owned Take Home Vehicles (Continued)**

Management's Response and Corrective Action Plan

We agree in principle with the recommendations:

The responsibility to approve and monitor the take home vehicles has always been the responsibility of the Finance and Administration Cabinet. We have updated our list of assigned take home vehicles and will in the future update this list annually.

We submitted reorganization bills to the 2006 and 2007 sessions of the General Assembly that would have ratified Executive Orders 2006-679 and/or 2007-502, which moved Fleet management from the Transportation Cabinet to the Finance and Administration Cabinet. We failed to get this legislation passed in either session and will be introducing a reorganization bill for the 2008 session of the General assembly.

We are in the process of updating policy and procedures for take home vehicles and overall use of state owned vehicles. The intent is to file a regulation when the reorganization bill is ratified giving us legal standing to issue a regulation.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-KOHS-35: The Kentucky Office Of Homeland Security Should Improve Controls Over The Preparation Of The Schedule Of Expenditures Of Federal Awards

During the FY 07 audit, we noted that the Kentucky Office of Homeland Security (KOHS) lacked adequate controls over the preparation of their SEFA. The SEFA was materially misstated, and went through four revisions before the final submission. In addition, while reviewing the SEFA, we noted \$472,278 of federal expenditures improperly recorded under CFDA 97.094 in eMARS that should have been recorded under CFDA 97.004.

Errors in the amount of expenditures and amounts passed through to other entities reported on the SEFA resulted from a lack of understanding of the SEFA instructions. Federal expenditures recorded under the wrong CFDA in eMARS appear to result from the grant being set up incorrectly.

Failing to have adequate internal controls over the SEFA preparation resulted in material misstatements in the earlier SEFA versions. Although many of the errors were corrected in subsequent versions, they initially were undetected by the agency's management until identified by the auditor. Also, pass through amounts related to the Department of Military Affairs were materially incorrect in the final SEFA disclosures.

Failing to record grant expenditures under the correct CFDA in the Commonwealth's accounting system could result in erroneous management decisions based on incorrect information, as well as inaccurate financial and/or federal reporting.

Management is responsible for implementing internal controls over the financial reporting process to ensure that financial and/or federal reports are fairly stated in all reasonable respects. As a part of this, good internal controls dictate that grants be set up properly in the accounting system.

Recommendation

We recommend the following:

1. The SEFA preparer review the SEFA instructions prior to its preparation. Should there be any questions, these should be directed to and resolved with the Finance and Administration Cabinet (FAC) prior to submission.
2. The KOHS implement supervisory level review procedures to help ensure accuracy and completeness prior to submission.
3. All CFDA numbers, titles, and federal grantors reported in the SEFA should be compared with the grant listing at <http://www.cfda.gov>.
4. KOHS should review the grants recorded in the accounting system to ensure that they are set up properly. Should any problems be found, this should be corrected immediately. Management should also determine if the improper grant setup has any impact upon prior financial or federal reports and take corrective actions accordingly.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-KOHS-35: The Kentucky Office Of Homeland Security Should Improve Controls Over The Preparation Of The Schedule Of Expenditures Of Federal Awards (Continued)

Recommendation (Continued)

5. Subgrant agreements with other agencies should be reviewed prior to submission of the SEFA to ensure that amounts passed through to those agencies are reported under the correct CFDA and recorded for the correct amount.
6. KOHS should maintain all documentation to support expenditure/pass through amounts reported on the SEFA and the expenditures on this document should be reconciled with eMARS.

Management's Response and Corrective Action Plan

KOHS will implement procedures according to recommendations as follows:

1. *The SEFA preparer review the SEFA instructions prior to its preparation. Should there be any questions, these should be directed to and resolved with the Finance and Administration Cabinet (FAC) prior to submission.*

KOHS SEFA preparer did review the instructions but apparently did not resolve misunderstandings prior to preparation. In future SEFA submissions preparer will make every effort to resolve issues prior to submission.

2. *The KOHS implement supervisory level review procedures to help ensure accuracy and completeness prior to submission.*

KOHS has re-structured the organization of the office and will ensure that the SEFA prepared will be reviewed by the Deputy Director for Grants and Financial Services prior to Executive Director's Signature.

3. *All CFDA numbers, titles, and federal grantors reported in the SEFA should be compared with the grant listing at <http://www.cfda.gov>.*

KOHS believes this was done and will continue to do so.

4. *KOHS should review the grants recorded in the accounting system to ensure that they are set up properly. Should any problems be found, this should be corrected immediately. Management should also determine if the improper grant setup has any impact upon prior financial or federal reports and take corrective actions accordingly.*

KOHS will review the grant set up in eMARS and make every effort to ensure that any grants with improper grant setup will be corrected accordingly.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-KOHS-35: The Kentucky Office Of Homeland Security Should Improve Controls Over The Preparation Of The Schedule Of Expenditures Of Federal Awards (Continued)**

Management's Response and Corrective Action Plan (Continued)

5. *Subgrant agreements with other agencies should be reviewed prior to submission of the SEFA to ensure that amounts passed through to those agencies are reported under the correct CFDA and recorded for the correct amount.*

KOHS will make every effort to ensure that funds passed through to other state agencies are recorded properly. However we note that other state agencies must cooperate and make eMARS corrections when required as this has not always been the case in the past.

6. *KOHS should maintain all documentation to support expenditure/pass through amounts reported on the SEFA and the expenditures on this document should be reconciled with eMARS.*

KOHS will require state agencies to submit documentation of expenditures of pass through amounts on a monthly basis as well as an annual SEFA amount. KOHS staff will reconcile these amounts with eMARS.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-KST-36: The Kentucky State Treasury Should Segregate Duties Within The Cash Receipts Function And The Computer Application Access/Modification Processes**

While performing tests of controls over receipts and disbursements during the FY 06 audit, we noted that the Kentucky State Treasury's Director of Computer and Technical Services is the only employee who is authorized to and has access to make programming changes to Treasury's software. In addition, the person in this position also has read, write, and change authority for live data from the Commonwealth's financial accounting system (MARS in FY 06; eMARS in FY 07), which would indicate inadequate segregation of duties between the programming and operation functions. This finding was communicated to Treasury at the conclusion of the FY 06 audit; however, no improvements were noted in this area in FY 07.

In addition, during this year's audit, it came to our attention that the Deposit Room Supervisor potentially has the ability to change deposit information in eMARS without any third party review, approve the changed transaction, post it within eMARS, and also reconcile the deposit to the bank statement. This also suggests an inadequate segregation of duties within the deposit room responsibilities.

Although the IT weakness existed during FY 06 and FY 07 and the Deposit Room weakness existed during FY 07, nothing came to our attention that would suggest any transactions were questionable, were falsely recorded, or were not appropriate as a result of this weakness.

These weaknesses result from an inadequate design of internal controls at Treasury, part of which may be due to inadequate staffing in the IT function.

Given the access capabilities of the Director of Computer and Technical Services, it is possible that live eMARS data could be modified and unauthorized activity could occur and go undetected.

Given the responsibilities of the Deposit Room Supervisor, the lack of segregated duties related to handling deposits, posting transactions, and preparing reconciliations increases the risk of theft and/or undetected errors.

Employing strong segregation of duty controls over computer programming and operations and deposit room functions decreases the opportunity for unauthorized modification to transactions, files and programs, and decreases the likelihood of errors or losses occurring because of incorrect use of data, programs, and other resources.

Proper internal controls dictate that duties of software programmers be segregated to prohibit the same individual from having access to live eMARS data, source code of programs (such as the reconciliation software), the compiler, and programming documentation. Proper internal controls also dictate that one individual should not have custody of cash, be able to approve/post transactions, and reconcile the activity to the accounting system.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-KST-36: The Kentucky State Treasury Should Segregate Duties Within The Cash Receipts Function And The Computer Application Access/Modification Processes (Continued)**

Recommendation

We recommend Treasury not allow programmers to process eMARS transactions, or implement sufficient compensating controls to supervise programmer activities. We also recommend that Treasury consider rotating the responsibility of reconciling the deposit room deposits with other personnel. These actions should be taken in order to reduce the risk of misstatements due to error or fraud.

Management's Response and Corrective Action Plan

The Treasury Department would love to have the budget and the employee cap level to allow the segregation of duties recommended by the auditor. Unfortunately, it does not, and does not foresee any changes in this situation in the immediate future.

The segregation proposed for the IT Division actually is not workable. The person in that position must have all of the authority that is described in the audit comment in order to accomplish what needs to be done. If a second programmer were possible in that area, that programmer, too, would need this same authority to work in both the Treasury Department programs and the eMARS data. Separation of the duties is not feasible, for everything interrelates. The Treasurer's Office is seeking budgetary approval for a second programmer position, but with the current budgetary situation it is doubtful that it will be approved.

The Treasury Deposit Room staff members do rotate duties on a regular basis so that one person does not always perform the same responsibilities. This lessens the chance that an employee could make a change to a deposit and have it go undetected. In addition, the individual state agencies making deposits through the Treasurer's Office maintain their own records of deposits and compare them to the deposits that are posted in eMARS. Any irregularities between the documents submitted and the documents that are actually posted will show up on this reconciliation. Actions performed on a CR document are recorded in eMARS under the "View Log" function, so there is a permanent record of anyone who touches the document. Unfortunately, the budgetary resources are not available to provide the type of textbook separation of responsibilities envisioned by the Auditor for the deposit process.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-KST-36: The Kentucky State Treasury Should Segregate Duties Within The Cash Receipts Function And The Computer Application Access/Modification Processes (Continued)**

Auditor's Reply

In response to Treasury's concern that incompatible functions of the IT Division Director cannot be segregated, we would like to note that these functions have been successfully segregated in other agencies with internal systems that utilize eMARS data or upload into eMARS. Considering Treasury's specific needs, if program modifications require change access to eMARS data, adequate compensating controls should be in place to document and authorize a limited-time access, and ensure after the modification that no inappropriate or unauthorized data manipulation occurred.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-KST-37: The Kentucky State Treasury And The Finance And Administration Cabinet Should Implement Internal Controls Over The Approval Process To Prevent Users From Bypassing Approvals On Transactions Within eMARS

During the FY 07 Kentucky State Treasury audit, we noted numerous instances where Treasury employees bypassed approvals of transactions in the accounting system. In addition, other agency auditors noted that:

- Treasury bypassed approvals on 13 cash receipt documents out of the 27 tested (48%) for one agency. On two of these items, Treasury bypassed approvals before the agency applied the 2nd agency level approval.
- Of the 15 items tested at another agency, 12 approvals were bypassed by Treasury (80%).
- Similar results were noted in other agency audits.

We also noted where Finance and Administration (FAC) employees bypassed approvals on 9 out of 11 (81.8%) journal voucher documents that write off old outstanding checks. Given the extent of the bypassed approvals at Treasury and FAC, this would suggest that bypassing approvals is a routine task at least for certain functions within both agencies.

Treasury and FAC employees bypass approvals for various reasons including: 1) some agencies are not timely in applying all levels of approval prior to submitting documents for deposit, 2) the deposit room staff will change a deposit when necessary as a result of deposit errors and staff at the agency level are not available or do not respond, 3) to clean up worklists, 4) as a matter of convenience as it is easier to bypass approvals than to follow the normal system routines, and 5) due to a belief that multiple reviews/approvals are not necessary on non-payment documents.

When approvals are bypassed, internal controls over the accounting system, financial reporting, and safeguarding of cash are circumvented and the audit trail showing the employees involved in the approval process is lost. Furthermore, without other compensating controls, employees who have the authority to bypass approvals have the ability to change the cash balance and revenue recorded within the accounting system, which could result in inaccurate postings, improper accounting strings, and etc.

Bypassing approvals also takes away the ability for agency level supervisors to review transactions to ensure they post correctly.

Good internal controls dictate that transactions be properly reviewed and approved prior to posting within the accounting system.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-KST-37: The Kentucky State Treasury And The Finance And Administration Cabinet Should Implement Internal Controls Over The Approval Process To Prevent Users From Bypassing Approvals On Transactions Within eMARS (Continued)

Recommendation

We recommend employees at Treasury and FAC improve internal controls by implementing controls to avoid bypassed approvals. These procedures should give adequate consideration to ensuring appropriate audit trails are maintained and that agency management have the appropriate authority and notification of transactions hitting their accounts. Furthermore, in those cases that Treasury employees note that a particular agency is not approving their documents appropriately, Treasury could consider contacting the agency head to make them aware of the situation. Should there continue to be problems, Treasury could communicate concerns to the FAC for further evaluation.

Management's Response and Corrective Action Plan

Treasury's Response

There are at least two issues involved with this comment.

If you examine the CR approvals that have been bypassed, you will probably find that 95%+ of them involve CR documents for electronic deposits. This occurs because of a serious flaw in the eMARS approval system that primarily impacts the Treasury Department Accounting Branch.

When the Treasury Department receives notification from Farmers Bank that an electronic deposit has been received, it is the responsibility of the Accounting Branch personnel to match that deposit amount with an eMARS Cash Receipt (CR) document for EFT transactions. In some cases the electronic deposit may indicate the name of the receiving department, but in many cases the only information that the Treasury has is the dollar amount that was received. The Treasury accountants must look for a CR for this amount.

The normal process to approve a CR would be to go to the CR EFT worklist to look for a pending CR. However, in this case the worklist is useless to the Treasury personnel because it does not show the dollar value of the documents. Using the worklist, the Treasury staff members would have to open each CR document until they found one for the proper amount. This would be unacceptably time consuming. To be able to view the dollar amount of the pending CR documents, the Treasury accountants must use instead the Document Catalog. Here they can identify the correct document that matches the deposit without having to open each individual

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-KST-37: The Kentucky State Treasury And The Finance And Administration Cabinet Should Implement Internal Controls Over The Approval Process To Prevent Users From Bypassing Approvals On Transactions Within eMARS (Continued)

Management's Response and Corrective Action Plan (Continued)

Treasury's Response (Continued)

document. With the document located in the Document Catalog, the Treasury staff can then go ahead and approve the document for posting.

The problem is that documents approved from the Document Catalog all post as "bypassed approval" documents. Even if all of the agency approvals were on, and the Treasury approval was all that was lacking, the document still processes as "Bypassed Approval." In reality, it is probable that no approvals have actually been bypassed, and the document was sitting in the CR worklist waiting for approval.

If the Treasury Accounting Division personnel cannot approve the CR documents from the Document Catalog once they are located, the only option is for them to record the CR number, close out of the Document Catalog, open the CR Worklist, search for the CR by the document number that they have just learned, and then apply the approval. This is the method prescribed by eMARS. However, it was obviously not designed for use in an environment where dozens or even hundreds of CR documents must be identified by document amount and approved each day. If this process were to be used, it would increase processing time for each CR document that is approved by at least 3 to 4 times. With dozens of CR documents waiting to be approved each day, and most agencies needing the funds transferred through the EFT process immediately so that they can release pending payments, the Treasury personnel do not have the time that would be required to follow this process and keep it timely. A minimum of one additional person would have to be added to keep up with production.

To avoid having to identify and release deposit documents from the Document Catalog, the CR dollar amounts need to be added to the CR EFT Worklist viewed by the Treasury Department Accounting personnel. We have made this request, but we have been unable to get this major programming change put into effect in eMARS. It apparently will require extensive and very costly reprogramming to which the eMARS overseers have thus far been unwilling to agree. The Treasury accountants have had to resort to the "workaround" that enables them to identify and release the pending CRs for EFT deposits in a timely manner.

Approving CR documents from the Document Catalog rather than the CR approval Worklist does mean that a document may be approved by the Treasury that does not yet have all agency approvals on it. The approval status of a document cannot be readily determined by viewing it in the Document Worklist.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-KST-37: The Kentucky State Treasury And The Finance And Administration Cabinet Should Implement Internal Controls Over The Approval Process To Prevent Users From Bypassing Approvals On Transactions Within eMARS (Continued)

Management's Response and Corrective Action Plan (Continued)

Treasury's Response (Continued)

It is important to understand that the CR documents for electronic deposits do not involve any physical checks or cash. The money is already in the bank in the state's bank account. There is no risk in misappropriating these funds through the manipulation of a CR document.

The only three options that we see to correct this situation are:

- Have the dollar amount of the CRs displayed in the deposit Worklist. The Treasury Department has not been successful in having this done.*
- Hire additional personnel to identify and approve the EFT CR documents. The current budget crisis and the budgetary personnel cap will not allow this to happen.*
- Identify and approve the EFT CR documents in the eMARS Document Catalog. This seems to be the only avenue open to the Treasury staff that will allow them to keep up with the timely approvals of deposit documents for electronic transfers. When documents are approved in the Document Catalog, though, they are recorded as "Bypass Approval" transactions, even though it is highly likely that no approvals have actually been bypassed.*

The "View Log" function in eMARS does record the bypass action and the employee who has applied that approval. A record does exist of the transaction.

*The Treasury Deposit Room personnel, who deal with physical deposits rather than electronic ones, have the advantage of having Deposit Transmittal Sheets submitted with the deposits that identify the CR documents on which the deposits are being posted. They, therefore, do not have to go out and search for CR documents using only the deposit amount. Because of this, they are able to work almost exclusively from the document Worklist. The documents appearing on the Treasury Deposit Room Worklist by definition have already received all necessary agency approvals. There are, however, a few instances in which the Treasury Deposit Room personnel find it necessary to make changes on and add approvals to CR documents to complete the processing of deposits that are being held by them. They **ONLY** change a CR after rejecting it back to and e-mailing the agency to fix any errors that are discovered.*

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-KST-37: The Kentucky State Treasury And The Finance And Administration Cabinet Should Implement Internal Controls Over The Approval Process To Prevent Users From Bypassing Approvals On Transactions Within eMARS (Continued)**

Management's Response and Corrective Action Plan (Continued)**Treasury's Response (Continued)**

If they receive no response from the agency and they are in a bind to get the deposit processed because the money has already gone to the bank, they will make a necessary change. It is the Deposit Room policy NOT to change a CR if anything is wrong with the cash. The agency is always made aware of the change, no matter what it is. The employee making the change is recorded in the "View Log" function in eMARS. These instances in which the Deposit Room personnel make changes on their CRs are rare, however. The Deposit Room staff is under constant security surveillance by five cameras which video every action in that room.

It is essential that the Treasury Deposit Room and Accounting Branch personnel have the authority to bypass approvals when necessary. The Treasury Department is a central agency in the eMARS accounting process. As a critical central agency, the employees must have the necessary authority to correct agency errors to get the state's money to the bank in a timely manner. To the degree that the Auditor perceives a risk in allowing this authority, we maintain that it is a risk that must be taken for the efficient operation of the office. It is a "managed risk." The likelihood that agency personnel could manipulate deposit documents to embezzle funds without being detected is very low. Most agencies do monitor their accounts and their deposits, and they will notice if a deposit does not post correctly.

To summarize, most of the "Bypassed Approval" deposit documents are for electronic deposits already in the bank, where there is no risk of misappropriation of funds. The use of this procedure has become routine because of a serious shortcoming of the eMARS system. Bypasses on physical deposit documents processed through the Deposit Room are rare, and usually occur after agencies fail to respond to requests for action. "Time Is Money" with the deposits, and sometimes Treasury action becomes necessary to keep the process timely. It is extremely necessary that the Treasury Department retain this authority as a central player in the state accounting process.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls***

FINDING 07-KST-37: The Kentucky State Treasury And The Finance And Administration Cabinet Should Implement Internal Controls Over The Approval Process To Prevent Users From Bypassing Approvals On Transactions Within eMARS (Continued)

Management's Response and Corrective Action Plan (Continued)**FAC's Response**

We agree that approvals should be recorded in the system for our internal transactions and agency requested overrides. While we intend to require approvals on internal transactions, we reserve the ability to bypass approvals as unique situations present themselves.

Auditor's Reply

We recommend Treasury work with FAC to further investigate the options presented in Treasury's response, or develop alternative solutions to reduce the necessity for the bypassed approvals.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-KST-38: The Kentucky State Treasury Should Improve Internal Controls Over The Processing Of NSF Documents

We reviewed a random sample of 40 non-sufficient funds (NSF) transactions that were processed by the Kentucky State Treasury during FY 07. During this test, we could find no evidence that: the NSF documents were 1) appropriately approved, 2) were communicated to the applicable agency for collection, and 3) that they correctly reverse the original cash receipt document.

The cause of the concerns noted above is the majority of the approvals of NSF documents within eMARS were bypassed and documentation supporting the NSF transactions (both the original transaction and communication to the applicable agency) was not maintained.

When approvals of NSF documents are bypassed, internal controls over the cash balance and revenue recorded in eMARS are circumvented and the audit trail showing the employees involved in the approval process is lost. Furthermore, without other compensating controls, employees who have the authority to bypass approvals on NSF documents have the ability to change the cash balance and revenue recorded within the accounting system, which could result in inaccurate postings, improper accounting strings, and etc.

When Treasury does not maintain supporting documentation for NSF documents, we cannot confirm that the NSF documents were communicated to the originating agency for collection and also that the NSF document correctly reverses the accounting string on the original cash receipt.

Good internal controls dictate that adequate supporting documentation be maintained for NSF documents and that these transactions be approved appropriately within the accounting system. Also, agencies in which the original revenue originated should be part of either the NSF approval process or should be notified of the transaction since it involves cash reductions in its funds.

Recommendation

We recommend Treasury: 1) not bypass approvals when approving NSF documents, 2) establish a system of communication with the agencies that ensures agencies can identify the nature and timing of NSF transactions impacting their accounts, and 3) maintain documentation of the accounting string of the original transaction as well as the letter, email, or other form of communication with the originating agency showing that the original cash transaction was returned.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-KST-38: The Kentucky State Treasury Should Improve Internal Controls Over The Processing Of NSF Documents (Continued)

Management's Response and Corrective Action Plan

The Treasurer's Office is puzzled by and does not understand or agree with this audit finding.

The Treasurer's Office processes two types of NSF transactions – returned checks and returned electronic transactions. In both instances, money has been removed from the state's bank account. The items are charged back by Farmers Bank to the State Treasurer. The Treasurer charges the items back to the agency through which they were deposited.

The agencies do not have the option of accepting or not accepting the charge-backs. The money no longer exists in the state's accounts. The credit for that deposit is removed from the depositing agency. There is no agency approval necessary on the CRNSF documents. The charge-backs are made upon receipt from Farmers Bank.

The CRNSF documents for returned checks are prepared by an employee outside of the Treasury Accounting Branch. For this reason, there is an approval required by an Accounting Branch employee to verify all of the information. For speed and convenience, the Accounting Branch employees usually process these under the "bypass approval" option. There are no other approvals needed beyond theirs, so they are not really bypassing any approvals. Using this option cuts out several more steps and saves valuable time. There is a complete record of these transactions in the "View Log" tab in eMARS. There is also a serious deficiency in the eMARS system in that the documents listed in the eMARS Worklist do not show monetary amounts. The amounts of the documents are only shown on documents listed in the Document Catalog. For this reason, Treasury Accounting Branch personnel are forced to work from the Document Catalog rather than the Document Worklist to identify their documents. Approvals done from the Document Catalog generally show a "Bypass Approval" designation.

The Treasury employees send a complete record of these NSF transactions to the designated personnel in each agency. For NSF checks, the agencies receive the actual charged-back check (or official copy, if applicable) and a copy of the CRNSF document. This shows them that the charge-back has occurred, and to what CR it was applied. For charged-back electronic deposits, the designated agency representatives receive a copy of the CRNSF and the bank debit ticket showing where the money was removed.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-KST-38: The Kentucky State Treasury Should Improve Internal Controls Over The Processing Of NSF Documents (Continued)**

Management's Response and Corrective Action Plan (Continued)

The Treasury Department does not keep copies of the NSF checks, but we can obtain a duplicate copy from Farmers Bank any time one is needed. We do keep a copy of the CRNSF document that was created, and the listing from Farmers Bank showing every check that was charged back on a particular day. For charged-back electronic transactions, we keep copies of the CRNSF and the bank debit ticket. We consider this to be complete and adequate documentation.

For NSF checks, the charge-back is done to the original CR on which the check was processed. The charge is made to the first line on the CR large enough to accept the charge. It is true that it may not be the actual accounting line on which the deposit was made originally. If it is not the correct line, it is the agency's responsibility to make the distribution to the correct line. This is the process, which was originally developed with the implementation of MARS in 1999. It was agreed upon by the system planners, and was conveyed to all agencies at that time. With the volume of returned checks, it is not feasible to investigate every check to determine the exact accounting line on which the check was processed before making the charge-back. There is not adequate time or personnel to do this. It also requires an agency response, which oftentimes does not occur.

For returned electronic transactions, the Division of Statewide Accounting provides the Treasury with the exact accounting string to which the charge-back should be applied. That information is provided to the designated agency personnel with a copy of the CRNSF and the bank debit.

We feel strongly that all recommendations of the auditor are already being met. The auditor apparently did not have a clear understanding of the process when making these recommendations.

Auditor's Reply

The Treasurer's office states that approvals are bypassed on CRNSF documents "for speed and convenience." Bypassing internal controls over the approval process as a matter of convenience, without effective compensating controls in place, is not an acceptable accounting practice. Unfortunately, complete records of the approval process are not always available in the "View Log" tab in eMARS.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-KST-38: The Kentucky State Treasury Should Improve Internal Controls Over The Processing Of NSF Documents (Continued)**

Auditor's Reply (Continued)

Although Treasury sends a record of the NSF transactions to designated personnel at the agency level, Treasury does not keep copies of the information sent making it difficult to determine the existence and timeliness of that communication. FAP 120-21-00 states, "An agency shall maintain the original source document that initiated a transaction and shall maintain a system of tracking that allows for auditing the original source document back to the electronic system." Since CR NSF documents are created in eMARS, in order to comply with this policy, Treasury's should maintain adequate accounting records (such as copies of the check charged back and correspondence/documents provided to the agency level) to support this newly created accounting document.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-OFM-39: The Office Of Financial Management Should Formalize And Consistently Apply The Program Modification Process**

As was noted during the previous seven audits of the Commonwealth's Cash and Investments System, the Office of Financial Management (OFM) has an informal program modification process in place; yet, this informal process was not consistently used nor had it been formalized in standards or procedure statements specific to the agency. Furthermore, no training routine has been implemented so that users are made aware of new programs or changes to the existing programs. We examined changes to the investment processing programs made since our testing in FY 2006. Although some improvements were made during FY 2006, our examination revealed that the program modification process had deteriorated significantly within FY 2007.

OFM continues to maintain a Program Change Request (PCR) form to document change requests and authorizations, yet it has not been updated to reflect the migration to enhanced Management Administrative and Reporting System (eMARS). Further, the PCR log developed in FY 2006 to track all change requests for the investment programs is no longer being used. The last entry in this log is dated November 7, 2006. The log revealed a total of 23 PCRs issued since completion of our FY 2006 testing. Three of these PCRs listed on the log did not include the date requested, date completed, or a proper description.

Only two of the 23 logged PCRs, or approximately 8.7 percent, were appropriately filed and properly authorized. One of these requests, although marked as completed on the form, was not noted as completed on the PCR log. In addition to the two PCRs provided, OFM also furnished a set of screen prints that corresponded to a change made to include a new pool in the processing. No PCR document was created to support this change nor was documentation of proper support available.

Microsoft Access is utilized as the primary software for the Cash and Investments System programs. We performed program code comparisons in order to identify all changes made to the investment processing programs since audit testing performed in FY 2006. This examination revealed a total of 196 changes to the programs that could have affected the programs' processing output. Only 15 of the 196 changes, or approximately 7.65 percent, were authorized within a PCR on file with OFM. Additionally, there were a total of 89 changes to the investment processing programs that likely would have no impact upon the program's processing output. Only four of the 89 changes, or approximately 4.5 percent, were authorized within a PCR on file with OFM. Although many of these changes could be classified as general maintenance, OFM does not have a general maintenance definition available or a specific PCR on file for general maintenance changes.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-OFM-39: The Office Of Financial Management Should Formalize And Consistently Apply The Program Modification Process (Continued)

It should be noted that the OFM programmer also had excessive access to the investment programs and data libraries. The programmer had the ability to make, approve, and move changes into production as well as the ability to update the LanBatch job scheduler during FY 2007. These security issues are addressed in a separate comment regarding segregation of duties (see 07-OFM-41).

In addition to the Access based programs, during FY 2007 a new set of programs were developed in Visual Basic that extracted information from the month end process and created a file formatted for eMARS processing to distribute the investment interest earned for each month. Since these programs have been in use, three main changes were made to the processing. No documentation related to these changes was maintained by OFM. No formal program change procedures were established related to these Visual Basic programs and the programmer had not performed any informal change control procedures.

Over the last several years OFM has continued to lose staff resources critical to the processing and maintenance of the Cash and Investments System. This scarcity of resources has resulted in a loss of knowledgebase as well as manpower and subsequently, a deficient program modification control process. The lack of continuity of resources and an inconsistently applied program modification control process is especially disturbing given that this system affects all investment activity for the Commonwealth. This concern is further warranted due to the fact that OFM has found it necessary to complete three major redesigns of this system during the last seven years.

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

Discussions with the agency revealed that a major cause for the lack of compliance with program modification controls within OFM during the fiscal year was primarily due to staff turnover and the lack of staff.

The program modification process should be formalized, distributed, and understood by all applicable agency personnel. This process should be consistently applied to all code changes to existing programs and the development of new programs.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-OFM-39: The Office Of Financial Management Should Formalize And Consistently Apply The Program Modification Process (Continued)**

Recommendation

Despite some improvements during the last two fiscal years, program modification control procedures have all but completely disintegrated during FY 2007. Therefore, we are strongly recommending OFM seriously consider requesting the Commonwealth Office of Technology (COT) take over the program modification process related to the OFM's investment processing programs.

If, however, OFM intends to maintain the program modification process completely within their agency, then we advocate the following recommendations in order to improve the current process.

We recommend that OFM formalize, implement, and consistently apply control procedures over the Cash and Investments System program modification process. Specifically, the agency should, at a minimum:

- Develop a formal procedure manual for the program modification process. This manual should include the procedures to adequately document program specifications and understanding of program objectives, to specifically identify changes in code by maintaining both the pre-modified copy of the database and the revised copy, to properly complete and maintain the PCR form historically, to document all PCRs thoroughly on the PCR log, to adequately test proposed program code changes, and to verify that all approvals are in place for the program code change before implementation to the production environment. If emergency situations are anticipated that might require this process to be accelerated, then that should be taken into consideration and an alternative process developed that properly applies compensating controls over that accelerated process.
- Consistently apply the formalized program modification process.
- Incorporate the Visual Basic programs into the central program modification process.
- Establish the requirement that an individual other than the programmer review all changes for accuracy.
- Establish the requirement that proper approvals are documented authorizing implementation of the change prior to the librarian moving the altered program to the production environment.
- Establish the requirement that an independent librarian without programming responsibilities is appointed to implement changes in production. After implementation of changes, the librarian should sign and date the PCR form to affirm that this process has been completed.
- Update the PCR Source field to reflect the migration to eMARS.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-OFM-39: The Office Of Financial Management Should Formalize And Consistently Apply The Program Modification Process (Continued)

Recommendation (Continued)

- Develop a 'general maintenance' PCR, which specifically identifies changes that would fall under 'general maintenance' and gives the programmer an overarching authorization for such changes.
- If there are changes that relate to a 'general maintenance' PCR form, ensure that the programmer provides supporting documentation for the request of the program changes, inclusive of an e-mail or other communication of the issues to be resolved, identification of the specific program code that was changed to satisfy the request, and approval from a person other than the programmer to move the changes into production. All personnel involved with authorizations of the PCR form should be made aware of the responsibilities they are assuming with their authorizations on these forms.
- Implement a training course whereby all users are trained on the operation of the investment processing programs. The training course should include all existing programs and should be updated when new programs are added or when existing programs are altered so that users will be properly informed of these changes.

Management's Response and Corrective Action Plan

The Office of Financial Management (OFM) agrees that the informal program modification process was not consistently applied during FY 07. Since July 2006, OFM has not had a programmer on staff and instead has relied on the support of the Commonwealth Office of Technology (COT). The departure of several key staff over recent years has depleted OFM's knowledge base of the processing system and has impacted the program change process. OFM appreciates the detailed recommendation and is working with COT to document and formalize the process.

System redesigns were in part necessitated by changes in the state accounting system. Most of the program modifications in FY07 relate to the change over from MARS to eMARS including the use of Visual Basic to create an XML file to allow for an upload of monthly data into eMARS.

Staff, utilizing in-house and outside resources, is currently evaluating the system and its components and is looking to further secure, document and streamline the process. COT recently completed an assessment of the system and we will begin detailed documentation of the processing programs including program modification in January 2008. Staff can then rely on the documentation to understand the program, make changes and diminish the effect of future staff turnover.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-OFM-40: The Office Of Financial Management Should Strengthen Logical Security Controls Over Investment Data And Resources

As noted during the previous three audits of the Commonwealth's Cash and Investments System, the Office of Financial Management (OFM) did not properly secure the critical financial data associated with the calculation and distribution of earnings from Commonwealth investments. Further, OFM has not implemented a formalized security policy that identifies management and user responsibilities concerning IT security surrounding the Cash and Investments System.

Our examination revealed that the OFM computer programmer from the prior year terminated employment with OFM in June 2006. Due to staffing limitations, the individual that assumed the duties as programmer also had full access to the production library during the FY 2007. In addition to this access, the individual also had full access to the Complete Asset Management, Reporting, and Accounting (CAMRA) application and data files. This security setting allowed the new programmer unlimited access to all the current investment related databases and programs used in production.

Currently, informal procedures are in place to request access to the CAMRA application and the libraries that hold the investment programs and data. However, these procedures are not formalized or consistently applied. Our examination revealed

- Five user accounts with access to the CAMRA application were granted a higher level of security than "read only."
- Two user accounts had "full control" access to the production libraries that house critical programs and data.

OFM was unable to provide either formal or informal access requests to support proper authorization for establishment of the associated access levels for these user accounts.

In addition, four user accounts were provided access levels allowing users the ability to modify programs and data files within the production libraries. The employees using these accounts are part of the normal investment process. However, since these libraries should be strictly secured on an as needed basis, access for this many individuals who do not perform a librarian function appears to be excessive.

During the review of the operations logs available for FY 2007, we discovered notes that indicated the previous programmer had been granted access to the production libraries after transferring to another agency in June 2006. OFM was unable to provide supporting documentation for approval of this person's system access to the production libraries.

Finally, for FY 2007, new programs were developed in Visual Basic that extracted information from the month end process and created a file formatted for eMARS processing to distribute the interest earned for each month. The production programs and the output files are all maintained on the programmer's personal office computer, which is not backed up on a regular basis.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-OFM-40: The Office Of Financial Management Should Strengthen Logical Security Controls Over Investment Data And Resources (Continued)

Without strong, formalized, logical security controls, the opportunity increases for unauthorized modification to production files as well as the likelihood of errors or losses occurring from incorrect use of data and other resources.

Formalized 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 for performing assigned duties and should be properly documented. Granting users system access that would allow the ability to alter or delete programs or financial data prior to or subsequent to processing increases the risk of financial misstatements or fraudulent reporting.

We are aware that OFM has retained contact with the previous programmer due to her knowledge of the production system. However, any outside use of the agency's system should be strictly controlled. This control should include documentation of the granting and revocation of access to the system.

Recommendation

We recommend OFM develop and implement a formalized security policy that standardizes security responsibilities for all employees and ensures critical programs and data are properly secured. OFM should ensure that programmers are not allowed access to the production library or to the CAMRA software and related data files. Management should monitor all current employee's access levels to determine whether access levels ensure a proper segregation of duties and do not allow inappropriate access to production data. This review should be thoroughly documented for audit purposes.

Further, we recommend that OFM ensure all production programs and files are located on a machine that can be properly secured and is included in a backup schedule.

Management's Response and Corrective Action Plan

The Office of Financial Management (OFM) agrees with the recommendations to strengthen IT security. Since July 2006, OFM has not had a programmer on staff and instead has relied on the support of the Commonwealth Office of Technology (COT). The departure of several key staff over recent years has depleted OFM's knowledge base of the processing system and has impacted the monitoring of the system's IT security.

OFM is working with COT and the CAMRA vendor to limit user access to necessary levels. OFM's previous programmer is now employed by the Controller's Office and

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-OFM-40: The Office Of Financial Management Should Strengthen Logical Security Controls Over Investment Data And Resources (Continued)**

Management's Response and Corrective Action Plan (Continued)

is assigned to OFM on an as needed basis therefore she retained her access to the system. Management will monitor employee access. Staff will secure the Visual Basic program and files and provide for routine backups.

Staff, utilizing in-house and outside resources, is currently evaluating the system and its components and is looking to further secure, document and streamline the process. COT recently completed an assessment of the system, including security issues, and we will begin detailed documentation of the processing programs in January 2008. Staff can then rely on the documentation to understand the program, make changes and diminish the effect of future staff turnover.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-OFM-41: The Office Of Financial Management Should Improve Segregation Of Duty Controls

As noted in the previous five audits, OFM did not employ a proper segregation of duties between the computer programming and operation functions. During the FY 2007, the programmer was also functioning as the operator for the Microsoft Access programs used within the Commonwealth's Cash and Investments System. These duties included running automated daily programs and manually running the macros within the month end programs on a routine basis. The programmer also made program changes and placed modified programs directly into the production environment. In addition, the programmer has the ability to alter the automated scheduling application.

Currently, this same individual has been established as the Administrator within the Complete Asset Management, Reporting, and Accounting (CAMRA) application. Further, this individual is the only person whose authorization is required to request access be granted to the CAMRA application. These duties in combination would allow this individual to establish user accounts, revoke user accounts, and alter user access rights without any additional oversight being necessary.

Finally, for FY 2007, new programs were developed in Visual Basic that extracted information from the month end process and created a file formatted for eMARS processing to distribute the interest earned for each month. Related to these programs, a single individual is the owner, programmer, and operator. These duties in combination will allow this individual to create, alter, and execute programs without any additional oversight.

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

Recommendation

We recommend OFM redistribute the programming, librarian, and operation duties related to the Access and Visual Basic programs among staff, so that the same individual is not performing more than one of these jobs. OFM should ensure that system users with access levels allowing them to alter the automated scheduling

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-OFM-41: The Office Of Financial Management Should Improve Segregation Of Duty Controls (Continued)**

Recommendation (Continued)

application cannot also create or move programs into production that are to be executed by the scheduler. Further, OFM should ensure that the same individual responsible for the administration of the CAMRA system is not also the person solely capable of approving user access within that system.

Management's Response and Corrective Action Plan

The Office of Financial Management (OFM) continues to be limited in the segregation of duties due to our small staff size. Since July 2006, OFM has not had a programmer on staff and instead has relied on the support of the Commonwealth Office of Technology (COT). The departure of several key staff over recent years has further reduced staff size, which impacts the practicality of segregation of duties. OFM agrees to redistribute duties and where segregation is not completely feasible, OFM will implement compensatory controls to ensure a secure environment.

As for the oversight of the Visual Basic program, the monthly data is reviewed by other staff persons before the owner/programmer/operator runs the program to create the XML file. The file is then given back to other staff persons to upload and approve in eMARS. Execution of the Visual Basic program alone has no effect on the system or eMARS.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-OFM-42: The Office Of Financial Management Should Ensure Contracts Are Recorded On The Appropriate eMARS Documents And All Payments Are Attributed To Those Documents**

During our FY 2007 audit of contracts issued by the Office of Financial Management (OFM) concerning information technology services, we identified payments made to Bloomberg Limited Partnership (LP) for the lease of a router/data service unit (DSU) and real-time investment data, which exceeded the associated master agreement (MA) commodity line service contract amount. In addition, there was an additional payment to Bloomberg LP for router/DSU rental, which was not directly attributed to the MA.

The Bloomberg MA reported a service contract amount of \$46,200 on the commodity line related to the lease of a router/DSU. At the time of our review, the Enhanced Management Administrative and Reporting System (eMARS) showed a total of four payments attributed to the router/DSU commodity line, which totaled \$73,455. In addition, there was one payment in the amount of \$1,200 that was not directly attributed to the MA; however, the commodity line description stated that it was for router/DSU rental. Inclusive of this payment, a total of \$74,655 was disbursed related to this commodity line from the MA, which represents an over-expenditure of the service contract amount of \$28,455.

Communication with the Office of Material and Procurement Services (OMPS) revealed that the MA document within eMARS was designed to be used for open-ended contracts, where expenditures may be controlled at the document header level, but can not be controlled at the commodity line. The contract (CT) document within eMARS was intended for fixed agreements with maximum expenditure restrictions. According to OMPS, the Bloomberg contract, being fixed in nature, should have been recorded on a CT document instead of an open-ended MA document. Despite the fact that the incorrect document code allowed the over-expenditure to occur, OMPS stated that OFM is still responsible for monitoring expenditures to ensure that they fall within the contract parameters.

When payments are not properly categorized or attributed to contracts, the agency runs the risk of over-expending established limitations or paying for unauthorized services.

Agencies are responsible for ensuring that they do not over-expend their funds. According to the Finance and Administration Cabinet Policy statement FAP 111-45-00 entitled Payment Documents, "An agency shall select the appropriate payment method for all goods and services...All payments referencing contracts and awards established in the state's procurement system shall be made in the state's procurement system and reference the appropriate award."

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-OFM-42: The Office Of Financial Management Should Ensure Contracts Are Recorded On The Appropriate eMARS Documents And All Payments Are Attributed To Those Documents (Continued)**

Recommendation

We recommend OFM review all transactions associated with the Bloomberg MA to ensure that payments were valid and correctly attributed to the commodity lines. If payments were appropriately attributed to the router/DSU commodity line, which has been shown to be over-expended, then the agency should review the underlying contract to determine if these charges are in violation of the agreement and whether OFM is entitled to a refund from Bloomberg.

The payment discovered related to the rental of a router/DSU, but not referenced to the Bloomberg MA, should be corrected to properly reference the appropriate contract within eMARS.

Further, we recommend that OFM work with OMPS to create a CT document within eMARS to replace the current MA. This new document will allow OFM to control the contract at the commodity line. OFM should then ensure that all future payments associated with the contract are properly attributed to the CT document and its commodity lines.

Management's Response and Corrective Action Plan

The Office of Financial Management (OFM) agrees with the recommendations. Bloomberg invoices are approved by OFM and then forwarded to OMPS for entry into eMARS. OFM has implemented a monitoring process whereby OFM will identify the expenditure amount for each commodity line level on each invoice. OMPS can then correctly account for contract expenditures at the commodity line level using the appropriate document type. OFM will periodically reconcile Bloomberg invoice items to eMARS activity reports to verify proper entry.

OFM will also review past eMARS transactions associated with Bloomberg to ensure payments were valid and that Bloomberg was not overpaid. Any recording discrepancies will be forwarded to OMPS for correction in eMARS.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-43: The Department Of Revenue Should Ensure Access To Production Libraries Is Limited

As noted during the prior year audit, our audit of logical access controls for the Department of Revenue (DOR) revealed that DOR had not adequately restricted access to its Job Control Language (JCL) and Production Libraries. Our testing revealed twenty-five (25) Commonwealth Office of Technology (COT) computer operators were provided 'alter' access to thirty-two (32) DOR JCL and Production Libraries. While the group account is used to log into the mainframe, these employees are required to use their individual user IDs to access the DOR libraries for tracking purposes. However, since these employees have established access to the mainframe through the group account, the access rights for that account would take precedence.

In addition, it was noted that fourteen (14) COT computer operators were granted 'alter' access to four DOR Production libraries through assignment to another group account. This group monitors and supports the DOR mainframe batch functions, and its members perform job restarts and manipulate job cards for restarts when production problems occur after hours. However, again these are COT employees that should not need to be granted 'alter' access levels to production libraries to perform assigned job duties.

Although the COT computer operators are responsible for migrating programs into production from libraries for DOR, they use a software application for this purpose that only requires 'read' access to a library to migrate the program into production. Also, another production library was established as a staging area that approved COT employees can access in order to phase jobs into production. Therefore, these computer operators do not need 'alter' access to any of the DOR production libraries. This is the second year we identified this issue and recommended that COT employee access to DOR production libraries be appropriately restricted. In the prior year audit, COT management concluded that further analysis of this situation was necessary prior to making any changes to the process. However, one year later no progress has been made toward improvement in this control. Only under emergency situations should this type of access be granted to COT employees, and then it should be closely monitored.

Merging DOR and COT within the Finance and Administration Cabinet has resulted in many information technology employees previously located within the Revenue Cabinet being transferred to COT. This group of employees appears to have retained alter access to these production libraries out of convenience for COT. Failure to properly restrict access to the DOR JCL and Production Libraries increases the likelihood that unauthorized changes to programs, JCL, or data could occur.

Organization of the information technology functions should be structured such that the highest possible segregation of duties is achieved. Access to production load libraries should be restricted to ensure only properly authorized programs are available to be migrated into

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-43: The Department Of Revenue Should Ensure Access To Production Libraries Is Limited (Continued)**

production environments. Users should only be granted the minimum access necessary to complete an assigned task to ensure a strong security environment.

Optimally, a librarian function is established as the only user allowed to move programs into a load library to ensure proper logical access security. This prevents computer operators from having authority to introduce unauthorized programs into the library and subsequently into the production environment. If computer operators are allowed more than 'read' access to load or production libraries for emergency purposes, then providing such access levels should be temporary, the reason well documented, and activities should be closely supervised. Circumstances of an emergency nature requiring elevated access privileges should be documented and closely monitored at the appropriate supervisory level. All activity should be subject to supervisory control and system log entries should be substantiated by a formal request to make system changes or modify system access privileges.

Recommendation

We recommend DOR and COT management work together to ensure the computer operator access to DOR production libraries is limited to the minimal access necessary for the operators to perform their job. Only in emergency conditions, under close supervision while documenting actions taken, should COT operators be provided greater than 'read' access to the DOR production libraries. Once the action taken is completed, access should be revoked or reduced to read access immediately.

Management's Response and Corrective Action Plan

COT and the DOR will review the access given to the operators and set them to the level of access needed to perform their job functions.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-44: The Department of Revenue Should Ensure KY-OSCAR Access Forms Are Properly Completed

Our FY 2007 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 proper procedures for granting access to Kentucky's On-Line System for Collection of Accounts Receivable (KY-OSCAR).

According to DOR security policy and procedure #6.5.2, DOR requires supervisors or managers to complete the Authorization to Access Department of Revenue Cabinet Confidential Computer Information and KY-OSCAR User ID Request forms to request system access. The DOR Security Office reviews the first form to ensure it properly indicates access to KY-OSCAR and ensures the user has submitted a KY-OSCAR User ID Request form. Once approved by the DOR Security Office, the KY-OSCAR User ID Request form is then forwarded to the Systems Administration Branch within the Division of Collections for processing. Review of these two forms revealed that guidelines have been established for the proper completion of the first form; however, no guidelines have been provided to users to assist with completing the KY-OSCAR User ID request form.

Testing of 11 KY-OSCAR User ID Request forms revealed the following:

- Eight (8) of the forms, or 73% of the population, were not approved by the Security Office prior to being forwarded to the Division of Collections.
- Three (3) forms, or 27% of the population, did not indicate the capability level. The capability level determines exactly what access levels the users are provided within OSCAR.
- One (1) form, or 9% of the population, did not include a listing of the user's supervisors. This information should be listed to indicate the chain of command and for work list routing purposes.
- Four (4) of the forms, or 36% of the population, did not have the signature of a supervisor, indicating that a supervisor approved the request.
- Three (3) forms, or 27% of the population, did not have signatures of the person in the Division of Collections who established the Userid. This should be completed to show that the ID was actually established.

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. Further, the level of system access granted to users should be restricted to only areas necessary for an employee to perform assigned job duties. All access request forms should be completed appropriately. Signatures should be provided to show the request for access was properly reviewed and approved by management.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-44: The Department of Revenue Should Ensure KY-OSCAR Access Forms Are Properly Completed (Continued)**

Recommendation

We recommend DOR update the KY-OSCAR User ID Request form to include detailed instructions on how to complete the form and identify those fields that are required in order to grant access. If this is not feasible, then DOR should expand upon security procedure #6.5.2 to include such guidelines. A designated employee within the Security Office and Systems Administration Branch should review and approve each access request prior to granting access.

Management's Response and Corrective Action Plan

DOR will review the KY-OSCAR User ID Request form and the Security Procedure #6.5.2 to determine how best to communicate applicable guidelines. DOR will also ensure that approvals are granted prior to granting requested access.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-45: The Department of Revenue Should Work With COT To Strengthen Controls Governing Data Processing Of Taxpayer Accounts

As noted in the prior year audit, the Department of Revenue (DOR) did not implement an adequate process for balancing the Tax Receipt System to the Commonwealth's Management Administrative and Reporting System (MARS). Our examination revealed that the REREPI08 report used by DOR to post electronic payments to the Tax Receipts System, to balance the electronic receipts with MARS, and to post receipts to taxpayer accounts through the Compliance and Receivables System (CARS) was not developed in a manner that would allow that report to be used effectively by DOR.

Testing revealed that the REREPI08 report does not reflect dollars refunded to taxpayers and also revealed varying delays between postings to MARS (creation and posting of the C1E document indicating actual receipts of funds), and the time those funds are reported on the REREPI08 report, which indirectly leads to a delay in posting to taxpayer accounts. It was also noted that the REREPI08 report does not include a data field common to the electronic payment gateway, the Tax Receipts System, and MARS that could be used to track and identify variances between the systems. The reconciliation and timing issues were determined as not affecting posting of payments to CARS.

We acknowledge that DOR has been working with the Commonwealth's Office of Technology (COT) to resolve issues surrounding the processing of electronic tax payments and that some progress has been made in identifying the source of the discrepancies between tax receipts processed by DOR and the tax receipts posted in MARS. A Duplicate Transactions report has been implemented in attempt to solve the issue of duplicates posted. Also, an Audit Trail report can be accessed upon request. In addition, an ePay Reconciliation report has been created to assist with monthly reconciliation and posting in a timelier manner, but it has not been placed into production thus far. As of the end of FY 2007, DOR continues to use the same REREPI08 report for posting to the Tax Receipts System, processing data through CARS, and to attempt to reconcile with MARS.

The process of using the REREPI08 report as a tool for posting tax payments to the Revenue Tax System and to balance with MARS is inaccurate and inefficient. This report currently does not reflect the actual posting of settled receipts as captured in MARS. Timing and other issues cause variances between this report and postings within MARS that cannot be accurately identified and explained. Further, the failure to properly investigate and reconcile variances resulting from this process illustrates a lack of due diligence and effects the integrity of data that could lead to inaccurate tax notices and penalties. At a minimum, using the REREPI08 report for posting to the Tax Receipt System could result in the unnecessary expense of researching and correcting errors regarding taxpayer accounts.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-45: The Department of Revenue Should Work With COT To Strengthen Controls Governing Data Processing Of Taxpayer Accounts (Continued)**

The agency should establish procedures for assuring that data input is reconciled to the relevant control totals. Proper procedures should be established to resolve variances or errors noted using control total balancing to ensure the complete and accurate posting of transactions to the system. Transactions should be input and processed within critical systems in a timely fashion.

Recommendation

We recommend DOR continue to work with COT to identify all sources of the discrepancies between the Tax Receipts System and MARS, to identify any effect on associated taxpayer accounts, and to make any and all corrections to taxpayer accounts if necessary. Further, we recommend that DOR continue to pursue methods to generate a new report or to alter the current REREPI08 report so that a more functional report is available for posting tax receipts to the Revenue Tax System and CARS. This report should include a data field that assists in reconciling the amounts posted from the report with those posted within MARS. Based on our examination the Merchant Order Number within the ePayment table and the transaction sequence number that is currently being used within the REREPI08 report are key linking fields. DOR should also ensure to implement the ePay Reconciliation report that has been created, which will aid in the reconciliation of these systems. Finally, DOR should determine causes for delays between posting in MARS and posting within DOR systems and ensure corrective actions are taken as necessary to alleviate any posting delays.

Management's Response and Corrective Action Plan

We agree with your comments. It is the Department of Revenue's desire to have a tight accounting process. We have and will continue to work with COT in an effort to improve this process. Further, we will attempt to resolve any issues still outstanding with the e-tax system as we implement CTS.

The reconciliation reports were recently put in production, so there has not been time to determine the benefits they will provide. Although these reports do not alter the payment posting process, the reports should allow for detailed identification and documentation of the discrepancies between the REREPI08 report and the EPAY CR's (CIE's).

A preliminary review shows that the reversals listed on the reconciliation review report during the 2007 calendar year were primarily the result of duplicated payments. Further review of Revenue's tax databases shows that the reversals have been properly reflected with adjustments to any tax bills and journal vouchers of the tax databases.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-46: The Department of Revenue Should Ensure All Agency Web Servers Have Updated Software And Security Patches Installed

During the security vulnerability assessments for FY 2007, our examination revealed web service vulnerabilities with 30 machines controlled by the Department of Revenue (DOR). Some of these machines have more than one issue involved.

Our testing identified one web service machine that had been defaced by a Turkish hacker. As soon as this issue was found, we notified DOR and Commonwealth Office of Technology (COT) management. Further testing was performed to ensure no other DOR web service machines had been defaced. No further web page defacements were noted within the Revenue IP series tested for this audit. Additional testing of the defaced machine would be required to conclude whether or not any other applications or servers were affected. At the time of fieldwork, COT also performed a review of this issue. On October 2, 2007, COT provided formal documentation to support the fact that their testing did not reveal any additional issues or concerns.

Also, 25 websites were found that either did not display a web page or were under construction. When no default website or login request is present, normally this means that no application/web service is running and the port is not needed. This exposure would be enticing to a hacker, so the necessity of these ports should be determined.

Furthermore, seven machines were determined to be running outdated software. Vulnerabilities associated with these machines include buffer overflow attacks and execution of arbitrary code using default servlets or robots. These vulnerabilities can potentially be exploited, leading to exposure of sensitive system information or misuse of the services the web server provides.

Web service vulnerabilities such as those noted herein could allow the stability of the network to be compromised as these machines become more susceptible to unauthorized intrusion. Installed web services without a specific business purpose may subject the network to buffer overflow issues, execution of arbitrary commands to circumvent network security, and unnecessary access to view network server volume files.

To assist in securing a network adequately, it is necessary to ensure all required web services have the most current security patch installed and that any unnecessary web service that does not have a known business function be disabled.

Recommendation

We recommend DOR take the necessary actions to ensure that web services on each identified machine are appropriately updated or patched. DOR should work with COT to ensure all machines are adequately secured. We also recommend that DOR management ensure that COT completes an adequate review of the machine related to the web service defacement, and that COT provide DOR and the auditor with the

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-46: The Department of Revenue Should Ensure All Agency Web Servers Have Updated Software And Security Patches Installed (Continued)**

results of that review. This is necessary in order to gain assurance that no further penetration occurred on this machine or within the critical applications residing thereon.

Management's Response and Corrective Action Plan

With the overall goal to ensure that all machines are adequately secured, DOR will work with COT to ensure that web services on each identified machine are appropriately updated or patched. In addition, DOR will work with COT to ensure that a review of the defaced machine is completed and then considered for appropriate action.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-47: The Department of Revenue Should Strengthen The Security Of System Accounts

During the security vulnerability assessments for FY 2007 for machines controlled by the Department of Revenue (DOR), our examination revealed various system user accounts with password ages that exceeded the established password policy. Additionally, we noted several accounts that had been disabled.

We obtained NetBIOS account information from two DOR machines, one of which was a Primary Domain Controller (PDC). To determine if user accounts on these machines were in compliance with established DOR policies, the auditor used the criterion that account passwords with ages over 31 days were non-compliant, which is the established agency policy. With respect to the PDC, there were 29 accounts that met this criterion. These accounts had password ages between 32 and 237 days. Also, there were 29 user accounts that were disabled and one account that was locked out. In addition, there were 57 accounts with expired passwords. One additional machine was noncompliant with the agency's password uniqueness policy.

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 has not been 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. An account should be deleted if it is not going to be reinstated. Established password policies should be consistently applied and enforced.

Recommendation

We recommend DOR review all user accounts on all machines to determine which accounts are not in compliance with the established security policies. These accounts should be evaluated to determine if they are still valid accounts and are required for a business related purpose. If not, the accounts should be disabled or deleted depending on the necessity of reinstatement of the account.

Management's Response and Corrective Action Plan

DOR will work with COT to determine which accounts are not in compliance with the established securities policies. If these accounts do not have a business related purpose, the accounts will be disabled or deleted.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-48: The Department of Revenue Should Disable The Simple Network Management Protocol Service On All Machines**

During the FY 2007 security vulnerability assessments of machines controlled by the Department of Revenue (DOR), the auditor identified one machine that had the Simple Network Management Protocol (SNMP) service available and would allow an anonymous user to logon with the community name “public”. The “public” community name is the default public account for this service.

Information provided by the SNMP service concerning a machine’s functions could be useful to an intruder in developing an attack.

SNMP services should be properly implemented to ensure excessive information is not provided to unauthorized users. The default community name should be changed to increase security of the service.

Recommendation

We recommend DOR either disconnect the SNMP service on the noted machine or change the “public” community name to a more sophisticated name on all servers. Further, any new machines should be checked for the SNMP service to ensure the “public” community name has been changed.

Management’s Response and Corrective Action Plan

The SNMP public community name on this device has been changed from the default. The information is no longer viewable.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-49: The Department of Revenue Should Comply With KRS 131.175 And End The Practice Of Waiving Interest Due**

During our FY 07 Department of Revenue (DOR) audit, we noted Finance and Administration Cabinet's (FAC) Office of Legal Services for Revenue waived interest and penalties assessed on Omitted Intangible Property Tax in apparent violation of state law. We also noted that the methodology used by DOR to establish these refunds created an additional unintended effect by computing and paying additional interest on top of the amounts to be refunded.

Prior to January 1, 2006 (when it was abolished), intangible tax was a property tax assessed on various investment assets. Taxpayers were supposed to file an annual return listing taxable intangible property. When DOR compliance efforts indicated failure to file the required return, the taxpayer was assessed for tax, penalty, and interest. Omitted Intangible Tax generally includes substantial interest because the taxpayer's failure to file creates a significant delay between the tax due date and payment date. Apparently, receipt of numerous taxpayer complaints motivated DOR to refund penalty and interest with additional interest.

To force the system to calculate refunds of the penalties and interest, DOR entered a false payment date, of January 31, 1999. This date was arbitrarily selected since it would be early enough to cause the system to refund penalties and interest since the date was prior to all of the various payment due dates. Entering the false date also inadvertently caused the system to pay additional interest on the refund amount. Refunds issued on March 29, 2007 included 267 items using this false payment date. As an example of its impact, one taxpayer was refunded \$2,467 interest and penalties previously paid. Because the payment date had been backdated, this taxpayer also received additional interest of \$477.

DOR states that these refunds have been issued as part of a settlement. While KRS 131.020 grants DOR the authority to negotiate with taxpayers and settle tax controversies, DOR has not presented the auditor with any supporting documentation related to an Omitted Intangible Tax settlement.

The Commissioner of DOR has authority to waive penalties, but not interest. Taxpayers are responsible for showing reasonable cause for waiver of penalties. KRS 131.175 states, "Notwithstanding any other provisions of KRS Chapters 131 to 143A, for all taxes payable directly to the Department of Revenue, the sheriff or the county clerk, the commissioner shall have authority to waive the penalty, but not interest, where it is shown to the satisfaction of the department that failure to file or pay timely is due to reasonable cause."

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-49: The Department of Revenue Should Comply With KRS 131.175 And End The Practice Of Waiving Interest Due (Continued)**

Also, KRS 131.030 (3) states,

The Department of Revenue shall have all the powers and duties necessary to consider and settle tax cases under KRS 131.110 and refund claims made under KRS 134.580. The Department of Revenue is encouraged to settle controversies on a fair and equitable basis and shall be authorized to settle tax controversies based on the hazards of litigation applicable to them.

Recommendation

The Department of Revenue should immediately cease refunding interest on Omitted Intangible Tax. DOR should waive penalties only when the taxpayer requests the waiver and shows reasonable cause, which should be appropriately documented. Legal Services should conduct a refresher course for its staff on the statutory requirements related to penalties, interest payable, and interest receivable, and disseminate this information to all levels of DOR management.

Management's Response and Corrective Action Plan

As requested by the previous administration, DOR issued Omitted Intangible Property Tax refunds as part of a global settlement under KRS 131.020 which grants DOR the authority to negotiate with taxpayers and settle tax controversies. However, the current administration agrees with the recommendation. DOR along with Protest Resolution, Finance and Administration Cabinet, will resolve the remaining Omitted Intangible Property Tax cases based upon additional hazards of litigation that may apply. In addition, Legal Service, Finance and Administration Cabinet, conducted a refresher course for its staff on 1/16/08 on the statutory requirements related to penalties, interest payable, and interest receivable and this information was disseminated to DOR management on 1/25/08.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-50: The Department of Revenue And Office Of State Budget Director Should Ensure Tax Receipts Belonging To County Governments Are Properly Accounted For In The Fiduciary Fund At Year End

The Department of Revenue (DOR) collects several types of property taxes, some entirely or in part on behalf of local governments. Both state and local property tax receipts are deposited into the General Fund. Periodically DOR distributes tax receipts to local governments after first making a transfer to the Special Deposit Trust Fund using journal vouchers. Several previous audits have noted inconsistency in the timing of the year's last journal voucher transfers from the General Fund to the Special Deposit Trust Fund. The transfer occurred before June 30 in 2000, 2001, 2004, 2005, 2006, and 2007, but after June 30 in 1997, 1998, 1999, 2002, and 2003. Local governments receive the fiscal year's last payment in August of the following fiscal year.

Concerning this issue, Department of Revenue states,

The Department of Revenue's policy is to record the fiscal fourth quarter property tax transfers by the end of the fiscal year, unless unforeseen circumstances preclude us from doing so. In the event of an unforeseen circumstance, the Department of Revenue will work with the Finance and Administration Cabinet and the Office of State Budget Director to determine the best way to proceed.

The example supplied for an "unforeseen circumstance" was a revenue shortfall. This indicates that management continues to contemplate reporting local government property tax receipts as part of the fund balance for the General Fund, which would be improper revenue recognition and manipulation of financial reporting. During previous audits, the APA recommended that DOR implement measures to prohibit this from occurring. Because the policy above is not a formal written policy, nor does it prohibit the improper recognition of the local property tax revenue in the General Fund, this finding is being repeated.

The MIXERS tax system is not set up to credit local government property tax revenue to the Special Deposit Trust Fund when received. Revenue from four tax types [General Property Tax-Real (R251), General Property Tax-Tangible (R252), Public Service Companies Tax (R260), and Apportioned Vehicle Property Tax (R266)] is instead credited to the General Fund upon receipt. Multiple journal vouchers transfer a share of the tax revenue from the General Fund to the Special Deposit Trust Fund as tax type General Property Tax-Tangible Motor (R253). This tax revenue is then distributed to local governments. A similar transfer takes place for tax type Omitted Tangible Property Tax (R265) from the General Fund to the Special Deposit Trust Fund, although the tax type does not change.

Because MIXERS does not credit the local government share of property taxes to the Special Deposit Trust Fund upon receipt, these fiduciary funds are mingled with governmental funds (the General Fund). Whenever the transfer is made after June 30, receipts and fund balance for the General Fund are overstated, while fiduciary assets and liabilities for the Special Deposit Trust Fund are understated.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-50: The Department of Revenue And Office Of State Budget Director Should Ensure Tax Receipts Belonging To County Governments Are Properly Accounted For In The Fiduciary Fund At Year End (Continued)

In response to the FY04 finding DOR and the Office of the State Budget Director (OSBD) adopted a policy to vary the timing of the transfers according to year-end budgetary considerations; in other words, to include money that is the property of local governments in General Fund receipts in order to show a balanced budget or trigger surplus spending. This is improper revenue recognition and a violation of Generally Accepted Accounting Principles (GAAP). Adopting a policy that allows this encourages management to manipulate financial reporting.

As written, the policy adopted by the Office of the State Budget Director could result in inaccurate and inconsistent financial reporting. Depending on the timing of the transfer in any given year, the General Fund and Special Deposit Trust Fund could be overstated or understated by the amount of the fourth quarter transfer. This would result in inconsistent financial presentation for analysis and policy purposes, and could also result in a misstatement in the financial statements for both funds.

GAAP requires each fund to recognize revenue in the appropriate accounting period and fund. Section 7.344 of the GASB Comprehensive Implementation Guide says the following when it addresses the issue of a government's use of one of its funds as a clearing account for property taxes:

Q—A county tax collector collects property taxes for all taxing bodies in the county, including the tax-levying funds of the county. The county uses an agency fund as a distribution mechanism for the taxes. At year-end, the collector is holding \$3,450,000 in the tax distribution account. Of that total, \$750,000 will be distributed to the county funds, and the remaining \$2,700,000 represents taxes collected for the other taxing bodies in the county. How does the county apply the “clearing account” provision in paragraph 111 of Statement 34 for agency funds? (225)

A—In the county's financial statements, the tax collector's agency fund would report only the \$2,700,000 in cash with an equal amount as a liability to other taxing bodies. The \$750,000 collected and on hand for the county's funds would be reported as cash (rather than taxes receivable or due from agency funds) in the appropriate funds. In essence, the collector has a “pooled” cash account, similar to an internal investment pool. The allocation of cash balances to the county funds is consistent with the requirement in paragraph 14 of Statement 31 that requires the “equity position” of each fund in an internal investment pool to be reported as assets in those funds.

The GASB Statement 31 requirement on reporting the equity position of each fund means that the local government property tax share should never be reported within the General Fund. The General Fund's purpose is to collect and expend unrestricted state receipts. However, the state has a fiduciary responsibility for the local property taxes it collects: these are not state

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-50: The Department of Revenue And Office Of State Budget Director Should Ensure Tax Receipts Belonging To County Governments Are Properly Accounted For In The Fiduciary Fund At Year End (Continued)**

receipts. By leaving them in the General Fund for several weeks or months after collection, General Fund receipts and fund balance are overstated until the transfer to the Special Deposit Trust Fund takes place. The transfer of these property tax amounts to the Special Deposit Trust Fund should take place before the fiscal year ends.

We recognize that the Finance & Administration Cabinet and the Office of the State Budget Director have specific statutory duties to properly manage the financial affairs of the Commonwealth, including compliance with budgetary requirements. Controlling expenditures, making realistic revenue estimates, and monitoring activity throughout the year are the proper ways to discharge that duty. Manipulating financial reporting is not a legitimate method of budgetary control. Even though the transfers were appropriately recorded during FY07, the policy permits and foresees inconsistent treatment because the timing will vary with changes in budgetary needs. Financial statements should be prepared in a manner that provides accurate, comparable data for users.

Recommendation

We recommend the Department of Revenue modify its MIXERS system to transfer the local government share of property taxes to the Special Deposit Trust Fund upon receipt. It should also incorporate this feature into the Comprehensive Tax System now under development.

Until Revenue's systems are able to do this, we recommend that DOR transfer the local share of property taxes to the Special Deposit Trust Fund no later than June 30 of each fiscal year, and implement a formal written policy requiring this transfer in order to reduce risks of a departure from GAAP in the future.

Management's Response and Corrective Action Plan

The Department of Revenue's procedure is to record the fiscal fourth quarter property tax transfers by the end of the fiscal year. This has been accomplished the past four years and it is our intent to continue this practice.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-51: The Department of Revenue Should Exercise Care To Assure Returns And Other Significant Documents Are Neither Lost Nor Destroyed

The Department of Revenue (DOR) lost or destroyed documents requested during its FY 2007 audit. The documents not available for inspection included:

- One corporate income tax return, which could not be located. Missing returns raise concerns regarding secure filing and storage, as well as questions as to whether taxpayer privacy has been maintained.
- Bank reconciliations prepared in FY07 for motor vehicle usage tax local bank accounts between July 2006 and December 2006. The hard copy of reconciliations were ordered shredded before the auditor had completed work in that section, and electronic copies were not available.

The corporate income tax record for the missing return indicates receipt of a tax-due return without payment, and a bill has been issued to the taxpayer. Records for the section working that type of return show receipt of the return, issuance of the bill, and shipment to storage (including date and box number). However, the return could not be found in the listed box or in several others searched. The missing return may be due to employee error, but the auditor is unable to test the validity of the taxpayer's bill without it. Failure to locate tax returns compromises DOR's ability to properly safeguard taxpayer information.

Each of Kentucky's 120 county clerks deposit motor vehicle usage (MVU) tax receipts (less 3% commission) in a local bank account, from which they transfer the daily deposit amount to Farmers Bank in Frankfort. The local banks mail monthly bank statements to DOR, where reconciliations are prepared to verify that the accounts retain no more than the allowed \$100. The reconciliations detect the presence and date of reconciling items, such as daily receipts that were deposited locally but not transferred to Frankfort, transfers for less than the deposit amount, or excessive bank fees, which are red flags signifying a need for further attention.

Since January 2007 bank reconciliations are prepared on electronic spreadsheets by MVU employees and stored on a DOR server. Before then, DOR operations employees at a separate processing facility prepared paper bank reconciliations. As DOR prepared to move to the State Office Building in fall 2007, the MVU Section Supervisor gave permission to operations staff to shred all paper bank reconciliations and notified all appropriate personnel, including the Road Fund Tax Branch Manager and Miscellaneous Tax Division Director. The rationale for this decision was that all reconciliations within the retention period also exist in electronic form. However, testing indicated that only eight of the twenty-five 2006 bank reconciliations could be produced, and that no comprehensive electronic record of pre-2007 bank reconciliations exists. Performing bank reconciliations is a significant internal control, but the auditor was unable to conclude that it operated reliably in FY07.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-51: The Department of Revenue Should Exercise Care To Assure Returns And Other Significant Documents Are Neither Lost Nor Destroyed (Continued)

KRS 131.081 (15) states in part that, “Taxpayers shall have the right to privacy with regard to the information provided on their Kentucky tax returns and reports, including any attached information or documents...no information pertaining to the returns, reports, or the affairs of a person’s business shall be divulged by the cabinet to any person....”

KRS 131.185 states, “Income tax returns shall be kept for five (5) years; primary accounting records of tax payments, seven (7) years; and records containing all data of motor vehicle registration, three (3) years....”

DOR must follow the records retention schedule published by the State Archives and Records Commission. The December 2003 (current) edition of the General Schedule for State Agencies - Fiscal Records identifies bank reconciliations as part of series F0072, Banking Record File. The schedule requires an agency to retain records for three years, and then transfer them to the State Records Center, which may destroy them after five years (provided that the records have been audited).

DOR should maintain tax returns and financial records in a manner that ensures compliance with confidentiality and record retention laws and ensures accountability to Kentucky taxpayers.

Recommendation

DOR should:

- Review record retention requirements with all levels of management.
- Stress the importance of taking care and following procedures that relate to filing and tracking documentation.
- Ensure confidential taxpayer information is protected and preserved as required by statute.

Management’s Response and Corrective Action Plan

Regarding Motor Fuels Reconciliations:

Department of Revenue employees have been made aware that there is a retention schedule document and that this document must be referenced before decisions are made regarding document destruction. They have been advised on how to obtain retention schedule information. The retention schedule will be followed in the future even though, in the case of Motor Vehicle Usage Tax, the information is now electronic.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-51: The Department of Revenue Should Exercise Care To Assure Returns And Other Significant Documents Are Neither Lost Nor Destroyed (Continued)****Management's Response and Corrective Action Plan (Continued)***Regarding Corporation Income Tax:*

The tracking procedures will remain in place for numbering boxes and return types. However, no corporate return will leave the batch folder for review after the batch verification process unless it is requested by the Commissioner or Ombudsman. The employees working at the Central Files location will be instructed to not remove returns unless instructed by the Director of Operations or their immediate branch manager. If an immediate bill needs to be created, a copy of the return will be made and the original placed back in the batch for future imaging. The goal for 2008 processing includes a quicker turnaround to get the corporate returns to the third-party vendor for imaging. This will allow for immediate retrieval thus allowing the creation of bills and refunds from images of the returns.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-52: The Department of Revenue Should Ensure Refunds And Distributions Are Properly Coded Within eMARS

Inconsistency in the Department of Revenue's (DOR) coding transactions has resulted in significant inaccuracy in the Commonwealth's accounting records. General Fund refunds for FY07 were understated by \$84,636,850 in Kentucky's Enhanced Management and Reporting System (eMARS). Refunds from the Special Deposit Trust Fund were overstated in eMARS by \$187,636,199 for Utility Gross Receipts License Tax (UGRL) and by \$86,018,986 for Telecommunications Tax (Telecom).

The automated Checkwriter process handles most refunds, and these were generally coded correctly. However, most manually processed refunds entered in eMARS on GAX2 documents were not coded as refunds but were instead coded as negative receipts. This occurred because the accounting templates used to create refund transactions did not include the appropriate source code, and the employees who entered document information did not add it. This caused receipts and refunds to be understated by the same amount on each of the affected transactions. Since the net receipt amount was correct, the reconciliation process did not detect this persistent error. It appears that no management comparison of refund amounts in eMARS and DOR's records occurred. Total General Fund refunds for FY07 recorded in eMARS were \$650,531,564 while DOR reported \$735,168,415. This includes understatements of \$37,007,052 for corporate income tax refunds and \$29,435,309 for individual income tax refunds.

The Special Deposit Trust Fund makes periodic distributions to local governments and the General Fund, but these distributions are coded in eMARS as refunds. Actual refunds to taxpayers from this fund are also coded as refunds. Consequently, the calculation of receipts minus refunds that represents net receipts for other taxes really represents undistributed receipts remaining in the Special Deposit Trust Fund. Coding distributions as refunds also yields an overstatement of refunds in eMARS; for UGRL and Telecom taxes alone, refunds were overstated by more than a quarter of a billion dollars in FY07.

Although refunds were reported incorrectly in the state's financial accounting system, ultimately refunds are properly accounted for in the Commonwealth's basic financial statements. However, the state's financial accounting system also is used to generate reports that enable fiscal managers to forecast cash flow needs in order to maximize investment income and minimize interest expense, budget analysts to project revenues and expenditures, and policy makers to draft legislation serving the Commonwealth's needs. Significant transaction miscoding distorts financial information and handicaps users.

Proper internal controls dictate that data recorded in the financial accounting system be accurate and consistently categorized in such a way to produce accurate, reliable financial report.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-52: The Department of Revenue Should Ensure Refunds And Distributions Are Properly Coded Within eMARS (Continued)

Recommendation

DOR should work with the Finance and Administration Cabinet and Commonwealth Office of Technology to implement the following changes to the eMARS:

- Create new templates or modify existing ones used to issue refunds manually. These should include the appropriate source code specification, which is Department Revenue Source = 04.
- Establish a distinct code to identify distributions from trust and agency funds. Modify the eMARS templates used to process distributions to incorporate this code, and train users to apply it.

Management's Response and Corrective Action Plan

In response to the following recommendation:

“Create new templates or modify existing ones used to issue refunds manually. These should include the appropriate source code specification, which is Department Revenue Source = 04.”

The problem with GAX2 documents prepared for eMARS refunds has been identified and an additional step has now been added to insure that the correct code is used for refunds.

In response to the following recommendation:

“Establish a distinct code to identify distributions from trust and agency funds. Modify the eMARS templates used to process distributions to incorporate this code, and train users to apply it.”

The Department of Revenue agrees with the Auditor's office that refunds and payments to the Local Taxing Authorities need to be made under different codes. The Department of Revenue has already communicated with the Finance and Administration Cabinet and they are researching to determine how to resolve this in E-Mars. The Telecommunications and Utilities Gross Receipts Tax checkwriter will remain coded as it currently is in E-MARS. These changes to the checkwriter file will need to be made by the Commonwealth Office of Technology and will be implemented as soon as possible.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-53: The Department of Revenue Should Improve Security Arrangements During Processing And Ensure Existing Procedures Are Followed**

While the Department of Revenue (DOR) has responded to prior year findings by implementing improvements to physical security arrangements at its processing facility, some weaknesses remain. Corporate and individual tax returns with checks attached were stored overnight in offices that, though locked, lack security camera coverage and fire protection. Security cameras cover the vault door and key storage, but not the vault interior. The auditor also observed a breach of vault procedures when people entered the vault to conduct or observe the taking of inventory of cigarette tax stamp but did not sign the vault entry log.

During peak times, DOR is unable to process and deposit all the checks received with pay returns on the day they are received. Carts holding these returns are stored overnight in offices at the processing facility. The offices are locked at night, but no security camera coverage or fire protection is in place for them. This leaves the checks vulnerable to fire and theft.

In its response to the FY06 finding, DOR stated that it would not act on the auditor's recommendation to install a security camera within the vault at the processing facility because the cost would be too high to justify in light of the department's move to new facilities by fall 2007. The new facility provides security camera both inside and outside the vault, but throughout FY07 no security camera covered the boxes of cigarette tax stamps. These are a liquid, portable asset. The tax value of the stamps as of the year-end inventory on June 29, 2007 was \$55,386,978.

When the year-end inventory of cigarette tax stamps was taken, four observers (two DOR employees, an internal auditor, and the independent auditor) accompanied the two DOR employees responsible for taking inventory. If proper procedures are not followed in the auditor's presence, this calls into question their operating effectiveness.

Good internal controls dictate that appropriate precautions be taken to safeguard assets from loss, damage, or misappropriation. Strong internal controls are essential to protect the department's assets.

Recommendation

The Department of Revenue should:

- Investigate creating fireproof storage convenient to return processing areas.
- Maintain the newly-added security camera coverage for the interior of the vault in its new location.
- Stress to its employees the importance of following procedures consistently and in all relevant circumstances.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-53: The Department of Revenue Should Improve Security Arrangements During Processing And Ensure Existing Procedures Are Followed (Continued)

Management's Response and Corrective Action Plan

Cash, checks, and other sensitive material are placed in a concrete secured vault. Security cameras have been installed (See Auditor's memorandum of December 19, 2007). Procedures are in place regarding vault security and all employees have been advised.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-REV-54: The Department of Revenue Should Strengthen Its Cash Handling Procedures And Ensure Employees In All Divisions Comply

In June 2007, the auditor asked for assistance locating checks mailed to Department of Revenue (DOR) in March 2007 that had not cleared the bank. Following this inquiry, DOR was able to locate the checks at the Office of Property Valuation. Nine checks from seven counties totaling \$295,643 were received, logged in, and placed in interoffice mail envelopes to be forwarded to the Division of Operations for deposit. However, they were misplaced and not found until after the auditor's inquiry.

DOR's procedures for processing the property tax receipts from Sheriffs were not sufficient to ensure the timely deposit of the tax receipts. The unwritten procedures called for an employee of the office to pick up the checks and accompanying reports at the post office box. Then the employee should log in, copy, and forward the checks and reports to Revenue Operations via messenger mail to be deposited. In this case the checks were placed in an envelope and sat aside unnoticed for three months.

DOR did not have adequate procedures in place to safeguard cash assets of the Commonwealth. As a result, there was a three-month delay in depositing \$295,643 of property tax receipts.

Transporting cash through regular messenger mail increases the risk of mishandling of cash, theft or loss. Messengers could leave the cash unattended, store mail in areas that were accessible to several people, or not locked in a secure location.

Good internal controls dictate that physical controls to secure and safeguard cash, check and other negotiable instruments be established and in place. Strong internal controls are necessary to prevent mishandling of funds and to safeguard against loss. They also protect employees from inappropriate charges of mishandling of funds by defining responsibilities in the cash handling process.

KRS 41.070 states that receipts should be deposited in the "*most prompt and cost-efficient manner available.*" Complete and prompt deposits of the cash receipts are critical in meeting the state's cash flow needs, maximizing interest income, and avoiding potential interest expenses.

Recommendation

We recommend:

- DOR emphasize appropriate cash handling procedures in all divisions that receive cash. Management should ensure that all personnel are aware of their expectations. Periodically, management should conduct reviews to ensure personnel are adhering to written procedures.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-REV-54: The Department of Revenue Should Strengthen Its Cash Handling Procedures And Ensure Employees In All Divisions Comply (Continued)****Recommendation (Continued)**

- Finance Internal Audit examine the cash handling procedures and periodically perform procedures to ensure they are being followed.
- DOR consistently identify Perimeter Park as the address for taxpayer payments, and consider a method of notifying taxpayers who routinely send payments to Fair Oaks. This will reduce the need to transport cash receipts between offices and ensure a more timely deposit.

Management's Response and Corrective Action Plan

This was an isolated incident. Procedures have been drafted and distributed to ensure proper cash handling. Note that "Perimeter Park" is now located in the same location as all other Frankfort Department of Revenue offices. All offices are encouraged to utilize the Division of Operations for incoming returns/payments.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-55: The Kentucky Transportation Cabinet Should Adhere To Established Procedures Governing System Access Request For The Transportation Information Payroll System

The Kentucky Transportation Cabinet (KYTC) did not adhere to established procedures concerning logical security governing the Transportation Information Payroll System (TIPS). Specifically, these procedures reflect that a new user access request form must be completed by the Supervisors and submitted to the Payroll Branch and that the Payroll Branch then sends the request to the KYTC Office of Information Technology (OIT). Supervisors must complete a request for termination and submit that request to the Payroll Branch anytime an employee leaves KYTC due to retirement, resignation, dismissal, death, transfer, or when the employee is no longer entering time. This must be done to ensure their system access is deleted.

We tested a sample of 8 of the 84 new users provided TIPS access since last tested during our FY2005 audit. Our testing revealed that access request procedures were not followed for 4 of the 8 users. This represented 50% of our sample and approximately 4.8% of all new users. Specifically, 1 request could not be located and there were 3 instances of access being provided for two Commonwealth of Technology (COT) Support Group employees. Discussions revealed that KYTC did not require the established procedures to be followed for these two individuals since these individuals already have the ability to change their own access.

Further, of the 229 current TIPS users we noted 35 instances, or approximately 15%, where the accounts had not been used at all in 2007. Some of these accounts have not been used since 2003.

Allowing users the ability to access information without proper authorization, particularly when allowing them to alter his or her own access levels, may subject the processing of data to errors and/or omissions and may compromise the integrity of data processed through the Transportation Information Payroll System. Further, intruders often use inactive accounts to break into a network.

The foundation of logical security is access control, which refers to how the system is being accessed and by whom. 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, if an account has not been used for a reasonable period of time, the account should be disabled until it is needed or removed if it will not be used in the future. This minimizes the possibility that an unauthorized user will access the account. Finally, users should not be given the authority to alter their own access levels to critical systems, and security policies should be consistently applied.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-55: The Kentucky Transportation Cabinet Should Adhere To Established Procedures Governing System Access Request For The Transportation Information Payroll System (Continued)**

Recommendation

We recommend KYTC consistently apply the established logical security policies and procedures governing TIPS access. Access requests should be completed for all new users, should include all necessary information and appropriate authorizations, and should be retained for support. We recommend that the TIPS access levels provided the COT Support Group be reduced to prevent those users from altering their own access levels.

We further recommend that access levels for all user accounts be reviewed to determine whether the accounts are still valid accounts that are required for business-related purposes. If not, the accounts should be disabled or deleted depending on the necessity of reinstatement of the account. All procedures should be consistently applied and all appropriate personnel should be reminded of the policies in place.

Management's Response and Corrective Action Plan

KYTC agrees that policies and procedures which clearly identify the processes and documentation required for account and access establishment, change, and removal are essential in an effective information security implementation.

KYTC agrees that if an account has not been used for a reasonable period of time, it should be disabled until it is needed or removed if it will not be used in the future. KYTC now requests that COT disable any account that has not been used in 90 days.

KYTC believes that the implementation of existing policy is in line with the APA recommendations. It is, however, likely that the policy and procedure verbiage could be stated more concisely, resulting in policies and procedures which more accurately reflect the implementation.

KYTC agrees that allowing users the ability to access information without proper authorization particularly when allowing them to alter his or her own access levels may subject the processing of data to errors and/or omissions and may compromise the integrity of data processed through the Transportation Integrated Payroll System.

KYTC will work with COT to ensure that COT provides a formal request for the employee identified as having expanded access without the proper approvals.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-55: The Kentucky Transportation Cabinet Should Adhere To Established Procedures Governing System Access Request For The Transportation Information Payroll System (Continued)

Management's Response and Corrective Action Plan Continued)

KYTC will work with COT to see that users should not be given the authority to alter their own access levels to TIPS.

KYTC and COT will work together to ensure that proper procedures are adhered to when providing access to the TIPS system and make changes as necessary.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-56: The Kentucky Transportation Cabinet Should Ensure Security Information Leakage For Agency Computer Devices Is Minimized

During the security assessment performed for FY 2007 on machines for which the Kentucky Transportation Cabinet (KYTC) has oversight responsibility, we found instances where machines provided information to anonymous users that could potentially help an intruder with developing details for an attack. Specifically we noted the following:

- Security controls governing Network Neighborhood folders revealed one of four domains open with eighteen machines accessible to thousands of individuals having access to Network Neighborhood on the state's network. This information was available by accessing agency domains listed under the Microsoft Windows Network within Windows Explorer.

Review of KYTC domains revealed one domain that listed three hundred and sixty machines on-line at the time of review. Of which eighteen, or five percent reflected directories and/or contents residing on the machine.

All but one, or seventeen, of the machines revealed subfolders containing sample music play lists, sample pictures, and a listing of connected printers. The remaining machine reflected printers, faxes, and scheduled tasks for the machine. Six machines revealed several files with .tbl extensions. One machine revealed 92 objects within a folder titled "Election" including multiple Microsoft Word and Microsoft Excel documents. One machine allowed the security settings for the printer to be modified to allow the "everyone" profile to take ownership of the printer, the ability to manage the printer, manage documents, and change permissions. Another machine had security settings for one of the printer's "everyone" profile set to allow the user the ability to manage the printers and documents.

Two machines within the domain revealed documents containing social security numbers for a total of 15 individuals.

- One machine revealed the user's name.
- Six machines revealed the version of FTP software being used through port 21 though anonymous access was not allowed.
- One machine revealed the version of SMTP software being used through port 25.
- One machine revealed the version of VNC software being used through ports 5800 and 5900.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-56: The Kentucky Transportation Cabinet Should Ensure Security Information Leakage For Agency Computer Devices Is Minimized (Continued)

- Two machines revealed the server version through port 8080.
- One machine revealed the version of web service software being used through port 80.

For security purposes, detailed information concerning the specific machines 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.

If a machine is set up to provide excessive information associated with the machine or applicable network, then an intruder could use this provided information in attempts to gain unauthorized access to the machine or network. Further, the permissions granted to these machines could allow an individual to not only read the content of a folder that may have sensitive or confidential information contained within, but also to potentially create, delete, or modify printer settings.

An agency's domain and machine information that is accessible to the public through inquiry tools should be kept at a minimum. Agencies should ensure that information such as versions of software and the machine's name and/or role is not divulged or is stated in the most minimal of terms. To accomplish this, an agency can set devices to not respond to certain types of inquiries. Further, security measures should be in place to adequately secure local workstations.

Recommendation

We recommend KYTC restrict the level of information provided by their network machines to public or anonymous users. Remedial steps should include limiting or restricting the type of response machines provide based on certain inquiries. Further, KYTC should review all domains/workstations available through the Network Neighborhood to ensure all files are adequately secured.

Though some of the machines may be physically located within the Commonwealth's Office of Technology (COT) and/or managed by COT, KYTC management is ultimately responsible for the security of KYTC resources.

Management's Response and Corrective Action Plan

- *KYTC agrees that all KYTC domains/workstations available through the Network Neighborhood should be adequately secured.*

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-56: The Kentucky Transportation Cabinet Should Ensure Security Information Leakage For Agency Computer Devices Is Minimized (Continued)**

Management's Response and Corrective Action Plan (Continued)

- *KYTC is working with COT to develop a communication solution to better inform the users within the CC domain of the type security issues that have been addressed within this document. There are a wide array of entities tied to this domain that avoid strict oversight by any Executive branch.*
- *KYTC realizes that the ultimate responsibility for KYTC domain resources rests with KYTC. KYTC and COT must jointly resolve the issues described here. Logical groupings have already begun that should allow for better management capabilities of the CC domain, including grouping the domain under infrastructure that could drastically improve the ability to dictate security changes.*
- *KYTC agrees to work with COT to take steps toward addressing issues that should limit information provided by network machines to public or anonymous users.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-57: The Kentucky Transportation Cabinet Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose

During the FY2007 security vulnerability assessment for machines for which the Kentucky Transportation Cabinet (KYTC) has oversight responsibility, our examination revealed that there were twenty-three machines with ports open that may not have a specific business-related purpose. Though KYTC is a consolidated agency and the Commonwealth Office of Technology (COT) maintains these machines, it is ultimately the responsibility of KYTC to ensure the integrity of all machines associated with KYTC. Due to the large number of issues, we grouped the findings below by port number.

Port 21- FTP

Six machines were identified as having Port 21 open that did not properly display a security banner. Three of these machines were also commented on during our FY06 assessment. All but one of the six machines did not display an appropriate security banner. One machine allowed anonymous access. Anonymous access via FTP should be restricted. Further, each of the six machines should be reviewed to ensure there is a business related purpose for port 21.

Port 22 - SSH Remote Login Protocol

Two machines were identified as having port 22 open. This port should be verified for business-related use for port 22 and to ensure the software version is updated to compensate for known vulnerabilities. Each machine was also reported within the FY06 audit report.

Port 23 - Telnet

Six machines were identified as having Port 23 open. Four did not properly display a security banner. Any user of telnet services on the network should be prompted by a banner to confirm authorized use. This port would be attractive to an unauthorized hacker, this type of information and be properly bannered. Further the vulnerabilities associated with this port lends to the necessity of the agency to review these instances to ensure that the port has a business related purpose and where possible COT and KYTC should consider replacing Telnet with the safer alternative, SSH.

Port 25 - SMTP (Simple Mail Transfer Protocol)

Six machines were identified as having Port 25 open. It is unclear if there is a business-related purpose for this open port, and there are multiple vulnerabilities associated with it. For each machine port 25 should be verified for business-related use. Further, one of the machines appears to be running a very outdated version of the software.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-57: The Kentucky Transportation Cabinet Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose (Continued)**

Port 111 – SUN Remote Procedure Call (sunrpc)

Six machines were identified as having Port 111 open. Each of these machines were also reported during the FY06 assessment. Security concerns: Provides rpc port map without authentication and has no logging or filtering. This port is used by the Unix Sunrpc service, which is a gateway to a variety of other services. Each of these instances should be verified as a legitimate, properly sanctioned and licensed by the agency and as serving a business related purpose.

Port 514 – cmd

Two machines were identified as having port 514 open. Like exec, except automatic authentication is performed. Server accepts syslog entries from remote host. These instances should be reviewed to verify a business-related use for port 514. Each instance was also report during the FY06 assessment.

Port 1433 – MSSQL server

One machine was identified as having port 1433 open. This instance should be reviewed to verify a business-related purpose.

Port 2049 – shilp – nfs server

Two machines were found with port 2049 open. This port is used by the (NFS) Network File Sharing service and is common on Unix. It is typically secured only by address based authentication and should not be used offsite. If unrestricted anyone can read or write files remotely. These instances should be reviewed to verify a business-related purpose and proper restriction.

Port 3389 – Windows Remote Desktop Protocol (RDP)

Seven machines were identified as having Port 3389 open. This service is a multi-channel protocol that allows a user to connect to a computer running Microsoft Terminal Services. Each of these instances should be verified as authorized, as serving a business-related purpose, and to ensure adequate access controls are in place.

Port 5631 – pcANYWHERE

Nine machines were identified as having Port 5631 open. Five of which were responsive and available to the Internet. Five instances were also reported during the FY06 assessment. Each instances should be verified as authorized and serving a business-related purpose and properly secured against unauthorized access.

Port 5800 and 5900 – VNC

One machine was identified as having port 5800 and 5900 open and running VNC. VNC is graphical remote access software and can be a useful tool but lend to security risks. The use of this software should be verified as having a business related purpose.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-57: The Kentucky Transportation Cabinet Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose (Continued)**

Port 6129 – DameWare

Eight machines were identified as having Port 6129 open. While remote control programs can be beneficial, the agency should verify that this port is in fact a legitimate copy of Dameware, are authorized, adequate authorization to the application, and that they serve a business-related purpose.

Port 8080 – HTTP Alternate

Six machines were identified as having Port 8080 open. Each of these instances should be verified as serving a business-related purpose.

Port 8081 – black-icecap user console

Ten machines were identified as having Port 8081 open. This port indicates the Network admin port for Black Ice's host-based firewall/intrusion detection program. The agency should review the product to ensure that it wasn't shipped with the default logon. Further, each of these instances should be verified as authorized and serving the intended business-related purpose.

Port 49400 – Compaq

Six machines were identified as having port 49400 open. Two of which were reported during the FY06 assessment. This port may be a web service providing Compaq diagnostics (Compaq Insight Manager) or could be a proxy service. These instances should be verified as serving a business-related purpose.

Miscellaneous ports to be reviewed for business purpose:

Port 1521 – nCube License Manager (5 machines)

Port 1808 – Oracle – VP2 (5 machines)

Port 1809 – Oracle – VP1 (5 machines)

Port 2000 – Remotely AnyWhere (3 machines)

Port 2001 – dc – or nfr20 web queries (2 machines)

Port 9090 – Remote Mgt. Sun Java Web Service Admin module. Each of these were reported during the FY06 assessment. (2 machines)

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-57: The Kentucky Transportation Cabinet Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose (Continued)

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

For security purposes, detailed information concerning 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.

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

The existence of open ports is an invitation for intruders to enter your system. To minimize the risk of unauthorized access to a machine, only necessary, business-related ports should be open. Further, the application residing at these ports should be secured to the extent possible and accessible services should be properly bannered to provide adequate warning that access to the system is limited to authorized users and that unauthorized access is illegal.

Recommendation

We recommend KYTC review all noted open ports to ensure there is a specific authorized, business-related purpose requiring the port to be open. If not required, then that port should be closed. If the port is necessary then KYTC should ensure the most recent patches are implemented for the service in use, applications are kept updated, and that adequate logical security controls are implemented to prevent unauthorized access as necessary.

Though some of the machines may be physically located within the Commonwealth's Office of Technology (COT) and/or managed by COT, KYTC management is ultimately responsible for the security of KYTC resources.

Management's Response and Corrective Action Plan

- *KYTC met with COT regarding the port and protocol issues described within this document. KYTC acknowledges ultimate ownership of issues stemming from open ports on KYTC networked servers.*

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-57: The Kentucky Transportation Cabinet Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose (Continued)****Management's Response and Corrective Action Plan (Continued)**

KYTC and COT assume that where not referenced, port information refers to TCP, and not UDP port reference. Much of the work involved with verifying port legitimacy falls within server teams responsible for the administration of the devices, as operating system requirements dictate, along with applications, the need for specific ports and protocols to be open on devices.

- KYTC agrees to work with COT to ensure that the most recent patches are implemented for the service in use if the port is necessary, ensure that applications are kept updated, and that adequate logical security controls are implemented to prevent unauthorized access as necessary.*
- Joint decisions from KYTC and COT will close many of the issues described within this document. We have also concluded that many of the open ports found are legitimate and KYTC is working with COT server teams regarding several specific servers. Subsequent meetings with COT will resolve any remaining issues noted.*
- KYTC will work with COT to ensure proper security is applied in all instances requiring security related issues with both ports described within this document, along with any other commonly known vulnerabilities.*

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-58: The Kentucky Transportation Cabinet Should Ensure Management Is Aware Of Hiring Policies And Identify Penalties For Noncompliance**

The Auditor of Public Accounts (APA) received a report from the Kentucky Transportation Cabinet (KYTC) Office of Inspector General (OIG) related to an investigation of a KYTC Project Director who hired two (2) employees without authorization pursuant to KRS 18A.005 (1) to work for the Business Opportunity and Workforce Development (BOWD) Center, a project which was supported by a federal grant from the Federal Highway Administration (FHWA). As part of our audit, we reviewed the OIG's report, the supporting documentation, and further discussed the matter with KYTC management.

The circumstances indicate that the Project Director believed an agreement between KYTC and the University of Louisville (UofL) permitted her to hire employees to work on the BOWD Center project, and that UofL would be administratively responsible for their wages. However, the Project Director did not have appointing authority, and did not obtain advance approval from either UofL or KYTC for the hiring decision. Because proper policies and procedures were not followed, these two employees were not on the KYTC or UofL payroll, and therefore were not getting compensated for their work from March 12 to April 6, 2007. The KYTC Project Director made an independent decision to pay each employee \$1,000 for compensation out of her personal funds.

Once the Project Director brought the payment to the attention of KYTC management, they requested supporting documentation for the payments. The Project Director produced copies of cancelled checks paid to each employee and timesheets for the period labeled "Kentucky Transportation Cabinet Standard Time Roster." Upon reviewing the documentation, KYTC management decided that the two employees had performed a service to KYTC and reimbursed the Project Director for the \$2,000 from the Road Fund in a non-1099 reportable category.

No additional compensation was paid to the two employees for any remaining amounts earned, and no withholdings were deducted from the payments they received from the Project Director. Since the reimbursement from KYTC was made directly to the Project Director, and was recorded in a non-1099 reportable category, neither the individual employees' earnings nor the reimbursement are accounted for in a way to reflect accurate wages for year-end individual tax reporting.

KYTC was awarded a new grant by the FHWA to establish the BOWD Center, and KYTC further contracted the project administration to UofL to "provide programs and support services." Even though the KYTC Program Director believed UofL to be the responsible party in the employee hiring process, there was no authorization given by either UofL or KYTC to hire employees. The KYTC management apparently disagreed

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-58: The Kentucky Transportation Cabinet Should Ensure Management Is Aware Of Hiring Policies And Identify Penalties For Noncompliance (Continued)

internally about whether these two individuals could be hired and whether they could be paid back wages for work already performed.

Also, KYTC management reimbursed the Project Director for expenses it believed was made in good faith for a service provided to the Commonwealth. However, by identifying those services as being reimbursable based on the benefit provided to the Commonwealth, KYTC is indicating that the work performed by the two employees was of value and merits full compensation. We saw no evidence that only part of the work performed by the employees benefited the program.

The unauthorized hiring of employees by the Project Director does not meet the criteria set forth in KRS 18A.005 (1) regarding “appointing authority” designations. These circumstances also create a noncompliance with KRS 18A.125(3). No intentions to defraud or to purposely circumvent the statute were noted, but the effect of the action is a noncompliance. This statute applies for “any person appointed or employed in contravention of any provision of KRS 18A.005 to 18A.200 or of any rule, regulation, or order thereunder...,” which we believe to meet the criteria for this circumstance.

Also, it appears that the employees have not received the full amount earned during the period. We are not aware of an agreed upon hourly rate between the Program Director and the employees, but since these employees were hired by KYTC as interim employees as of May 1, 2007, we applied that rate of pay to estimate the employees’ earnings. Timesheets indicate each employee worked 156 hours each, and in applying a \$11.95 per hour rate, each employee’s gross pay for the period should be \$1,864 for the period between March 12 and April 6. We did not determine whether the employees worked any hours between April 6, 2007 and the effective date of their interim positions of May 1, 2007. Also, we noted that the employees documented travel expense on their timesheets. If these expenses are eligible under 200 KAR 2:006, the employees should be reimbursed. Using the state rate in place during the timeframe (\$.40/mile for March and \$.41/mile for April), the combined reimbursement for the two employees would be an additional \$790 due.

Because the employees were paid by personal check, and the Project Director’s reimbursement was made from a non-1099 reporting category, federal, state and FICA withholdings on those earnings have been bypassed.

This situation also exposes the KYTC to potential liabilities regarding the Fair Labor Standards Act, workers’ compensation, unemployment insurance, and any applicable state or federal confidentiality provisions in place since the employees may have had access to personal information of program participants.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-58: The Kentucky Transportation Cabinet Should Ensure Management Is Aware Of Hiring Policies And Identify Penalties For Noncompliance (Continued)**

The KYTC reimbursement to the Project Director was not made from the BOWD Center project's federal funds, and therefore no federal questioned costs were identified.

KRS 18A.005 (1): "Appointing authority means the agency head or any person whom he has authorized by law to designate to act on behalf of the agency with respect to employee appointments, position establishments, payroll documents, register requests, waiver requests, requests for certification, or other position actions. Such designation shall be in writing and signed by both the agency head and his designee. Prior to the exercise of appointing authority, such designation shall be filed with the secretary."

KRS 18A.125 (3) states, "Any person appointed or employed in contravention of any provision of KRS 18A.005 to 18A.200 or of any rule, regulation, or order thereunder, who performs services for which he is not paid, may maintain an action against the officer or officers, employee or employees, who purported so to appoint or employ him, to recover the agreed pay for such services, or the reasonable value thereof if no pay was agreed upon. No such officer or employee shall be reimbursed by the Commonwealth at any time for any sum paid to such persons on account of such services."

IRS Publication 15-A "Employer's Supplemental Tax Guide" provides guidance on determining employer-employee relationships. It states, "An employer must generally withhold federal income taxes, withhold and pay social security and Medicare taxes, and pay unemployment tax on wages paid to an employee." The publication also identifies when employer-employee relationships exist, which would indicate that an employer-employee relationship did exist in this case.

Recommendation

KYTC determine the full amount of compensation due to the two employees, pay those employees for the full amount of wages due in a method that will correct all taxable wage reports and withholdings. KYTC should withhold from these wages the net amount paid by the Project Director in order to refund the Road Fund for the KYTC's reimbursement. KYTC should consult with the Department of Revenue to assess accurate tax reporting requirements.

KYTC train managers, directors and other management level employees regarding the agency's hiring policies, identifying penalties for noncompliance.

KYTC should consult with the Finance and Administration Cabinet and the Personnel Cabinet to determine how to resolve any personnel matters that do not strictly adhere to the provisions in KRS Chapter 18A.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-58: The Kentucky Transportation Cabinet Should Ensure Management Is Aware Of Hiring Policies And Identify Penalties For Noncompliance (Continued)**

Management's Response and Corrective Action Plan

In regards to the first recommendation that full compensation be paid to these employees, the Cabinet agrees. An earlier determination made by Transportation Cabinet's Office of Personnel Management that the personnel appointments could not be backdated to reflect actual employment date was reversed by the Personnel Cabinet. With this decision we were able to compensate these two employees for all hours worked, deduct all applicable taxes and reimburse the state Road Fund \$2,000 from the net amount. The payment to these employees covers the time period of March 12, 2007 through April 30, 2007. With this action all financial transactions are in order.

On the second recommendation we agree that the Cabinet is responsible for properly training all managers on the agencies hiring practices and we believe we have fulfilled this responsibility. This action, by one manager, was a complete outlier and in response to extraordinary circumstances which resulted in a bad decision, but one we believe was made in good faith. We do not expect these circumstances to be repeated.

On the third recommendation, KYTC will consult with the Finance and Administration Cabinet and the Personnel Cabinet when necessary to resolve personnel matters that are out of the ordinary. According to General Counsel within the Kentucky Transportation Cabinet, there was no violation of KRS 18A with this transaction.

Auditor's Reply

Although we are pleased that KYTC did eventually fully reimburse these employees for the full amount that they earned, we also must emphasize that KRS 18A.125 (3) appears to have been violated. These two employees were hired by a KYTC employee without appointing authority, they followed the time reporting policies of KYTC, and initially were not paid by KYTC for the services they provided. We feel the requirements of this statute are important for the KYTC to note in order to fully recognize the importance of training related to personnel matters.

Also, we believe one other point is important to make related to this finding. Based on the circumstances of this case, it appears that an organizational independence impairment may exist between KYTC Internal Audit and management in its chain of command. We will provide KYTC with additional details of this impairment and recommendations, which will be followed up again during our FY 2008 audit.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-59: The Kentucky Transportation Cabinet Should Implement Formal Policies And Procedures Regarding Inventory Purchased With A Procurement Card

Kentucky Transportation Cabinet (KYTC) has maintenance barns in 12 districts throughout Kentucky. During the 2007 year-end Maintenance Materials Inventory observation the Auditor of Public Accounts (APA) became aware of material inventory that was not recorded in the Operations Management System (OMS). The auditor observed multiple items of materials on shelves that were listed on the OMS Inventory Report as having zero (0) units on hand. During the inventory count, the KYTC inventory counter neither counted nor documented for the items to be corrected on the OMS Inventory Report. After the inventory was complete, the auditor inquired why the items were not included as part of the inventory. KYTC personnel claimed that the items were purchased with a Procurement Card (ProCard); as a result, adding those items to the OMS inventory was not required. KYTC personnel explained that most items that are purchased with a ProCard are for items needed immediately. However, in this case, it's evident that more items were purchased than immediately needed and were stocked as inventory. Therefore, those items should have been entered into the OMS inventory system.

The KYTC OMS Material Inventory Guide does not specifically address inventory purchased with a ProCard. A lack of formalized procedures on ProCard purchases can lead to inconsistent understanding among the district staff on how and when to record inventory in its entirety. Without recording the entire inventory in OMS, the agency does not maintain accurate inventory records. This may result in misappropriated assets. Due to the lack of documented procedures on ProCard purchases, and without accurate inventory records, the agency is more susceptible to unauthorized purchases and theft.

Proper internal controls dictate that all purchases, including those made with ProCard, be evaluated to determine whether they should be included in supplies or capital assets inventory.

Although the Finance and Administrative Cabinet (FAC) ProCard Manual has not been updated with language consistent with the current accounting system, the FAC policy identified in the most current ProCard Manual states, "It is the responsibility of the Agency Program Administrator to communicate all purchases of Fixed Assets and/or tangible/trackable items to the agency property officer or fiscal officer. Since the Procurement Card document will not generate a Fixed Asset Shell document in Advantage Financial, it is essential the Agency Program Administrator communicate such purchases to ensure the items are properly inventoried in Advantage." KYTC uses OMS to organize their inventory, and the FAC policy clearly indicates that the intent is for applicable ProCard purchases to be inventoried. Therefore, it is the responsibility of the Program Administrator to communicate the purchases to the OMS timekeeper.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-59: The Kentucky Transportation Cabinet Should Implement Formal Policies And Procedures Regarding Inventory Purchased With A Procurement Card (Continued)**

Recommendation

We recommend the OMS Materials User Guide include a formalized procedure regarding the inventory purchased with a ProCard. The OMS Materials User Guide should also include a policy or definition of what constitutes “immediate need” to assist OMS Coordinators in determining the length of time materials can be on hand before they are considered inventory items.

We also recommend that all OMS Coordinators be notified that all inventory should be recorded in OMS regardless of how it was purchased.

Management’s Response and Corrective Action Plan

The OMS team will make an addition to the Material Users Guide to document the appropriate procedure for procard purchases. All material purchases should be entered into OMS if they are to be stored on the lot for any amount of time. The users will not have to enter procard purchases if they will be using the item immediately after the purchase on a project. In these instances the user will just create a direct cost on the appropriate work order for the amount of the material. We will inform the coordinators and make an addition to the manual to document that all material purchases need to be brought into OMS if they are going to be stored on the lot for any amount of time, regardless of how the item was acquired. These changes to the Users Guide will be completed by December 30, 2007.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-60: The Kentucky Transportation Cabinet Should Strengthen Inventory Controls To Ensure Proper Precautions Are Taken To Safeguard Assets**

Safeguarding of assets at the Kentucky Transportation Cabinet (KYTC) maintenance barns is inadequate. The areas where KYTC stores materials and supplies are not protected against access by unauthorized personnel. Private contractors have access and/or keys to the maintenance barns so they can enter the KYTC lot at any time. Private contractors also store their supplies and materials in the same area that KYTC stores its materials.

The Auditor of Public Accounts (APA) became aware that private contractors stored materials at the KYTC maintenance barns during the FY2007 maintenance materials inventory observation. The contractors' supplies and materials were stored together with the KYTC materials. The inventory team could not determine which materials were KYTC and which materials belonged to the contractors. The inventory team also informed the auditor that the contractors had a key so they could access the lot after hours, and KYTC staff could not be certain that contractors were only taking their own materials and supplies.

Although it is convenient for the private contractors to have their supplies and materials stored nearby at a KYTC maintenance barn, there is a greater risk of theft and asset misappropriation due to unauthorized access by non-employees and because materials are not distinctly separated from KYTC materials.

Good internal controls dictate that proper precautions be taken to safeguard assets from loss, damage, or misappropriation. Strong internal controls are essential to protect the department's assets.

Recommendation

We recommend private contractors only be given access to the KYTC maintenance barns with KYTC personnel present.

We also recommend any supplies and materials stored at the KYTC maintenance barns belonging to private contractors be kept in a separate location from the KYTC materials and supplies.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-60: The Kentucky Transportation Cabinet Should Strengthen Inventory Controls To Ensure Proper Precautions Are Taken To Safeguard Assets (Continued)

Management's Response and Corrective Action Plan

We accept the recommendation of the APA and it is our plan to safeguard the department's assets by:

- *Requiring all keys to the KYTC maintenance barns be confiscated from private contractors and require district personnel to limit private contractor access to KYTC maintenance barns to regular business hours unless prior arrangement has been made ensuring a member of KYTC personnel is present if after-hour access is necessary.*
- *Designate an area for private contractors to store their materials separate from KYTC materials.*

This action will be documented in the Maintenance materials manual no later than December 2007.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-61: The Kentucky Transportation Cabinet Should Improve Procedures For Maintenance Materials

The Kentucky Transportation Cabinet (KYTC) has maintenance barns in 12 districts throughout Kentucky. These maintenance barns contain not only heavy equipment used for highway safety, but also necessary supplies and material to keep state roads passable. The amount of inventory in these maintenance barns totaled \$36,705,232 million for FY07. We observed district personnel conducting their inventory to determine if maintenance materials were counted correctly and to determine if inventory management procedures were adequate. KYTC Internal Auditors also observed several inventory counts as well and communicated their results to KYTC management.

We issued comments the previous three years regarding various inconsistencies in the inventory process. These included inconsistent treatment of guardrail systems; unclear responsibilities for items such as antifreeze, oil, grease, etc; and no policies and procedures in place. Some districts have shown some improvements; however, there are still some problems in some districts:

- A comparison of the actual count to quantities listed on perpetual inventory sheets from Operations Management System (OMS) revealed numerous discrepancies in quantities recorded, such as inconsistent amounts for windshield wiper fluid, pipe bands, aggregates and other inventory items. We have seen improvements in FY07, but OMS is still not being used effectively to track materials used or on hand.
- Proper inventory procedures were not followed:
 - The person performing the inventory was the same person responsible for ordering and issuing inventory.
 - Two people did not always perform the inventory counts.
 - Bulk materials were not formed in the standard stockpile shapes, cone or tent. Instead of measuring items 1) they were estimated based on how many loads would fit in a dump truck; 2) they were measured by taking steps around the unformed pile; or 3) the heights/widths of the aggregate piles were “eyeballed” instead of measured. Some maintenance lots maintain their aggregates behind concrete barriers. They claim it would be too time consuming to pull the aggregated out of the barriers to form into a cone or tent shape. This would also result in a loss of aggregates because of the shifting. Therefore, they were not able to measure the way the OMS Materials Inventory User’s Guide instructs.
 - Bulk Materials were not calculated as outlined in the Stockpile Quantity Calculation Procedures. When auditor inquired why the calculation sheets were not used, the inventory taker claimed the calculations in the OMS Materials Inventory User’s Guide didn’t provide an accurate calculation,

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-61: The Kentucky Transportation Cabinet Should Improve Procedures For Maintenance Materials (Continued)

because they always came out with a different answer than when they performed their own calculation.

- The OMS Material Inventory User's Guide inventory count procedures were not provided to all inventory takers. Prior to the inventory, the inventory taker explained his planned procedures and appeared to have a sufficient understanding of the inventory process. He also claimed he had performed the inventory for years. However, during the inventory several errors in the process were made. At the conclusion of the inventory the auditor discussed the performance and showed the inventory taker the procedures as outlined in the OMS Material Inventory User's Guide. The inventory taker claimed it was the first time he had seen those procedures.
- Not all inventories were recorded in OMS. During the inventory one county had a pallet of Gabion Baskets and the OMS Timekeeper had no idea where they came from or whom they belonged to. They were not on the OMS inventory report and were not added to the inventory report.
- Scrap and salvage material was mixed in with the regular inventory. During the inventory process the inventory taker was having trouble determining which material was to be counted. The scrap and salvage material was in the same pile as the regular usable materials. Scrap and salvage items were also still on the OMS report. OMS timekeeper was not sure how to remove the items from the report.
- When confirming corrections to OMS, discrepancies were noted. After the inventory is complete the districts are required to reconcile the inventory sheets to match the actual physical inventory count. The discrepancies found were immaterial; however, a proper reconciliation was not complete.

Inaccurate quantities in OMS are due to the fact that some crewmembers delivering and picking up or using materials don't always inform the timekeeper. When crewmembers do not inform the timekeeper of inventory inflow and outflows, OMS is not updated properly. This leads to shortages or overages in amounts of inventory in each district.

The KYTC "OMS Material Inventory User's Guide" provides details for district personnel regarding the physical inventory count of maintenance material. When these procedures are not provided to the timekeepers and followed, inconsistent or inaccurate counts could occur.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-61: The Kentucky Transportation Cabinet Should Improve Procedures For Maintenance Materials (Continued)

The KYTC “OMS Material Inventory User’s Guide” is not inclusive all areas of concern in the inventory count. Several districts had the same questions on how some of the inventory should be recorded, stored, disposed and removed from OMS. Inconsistencies or inaccurate counts could occur when procedures are not entirely documented.

The KYTC “OMS Material Inventory User’s Guide” was revised in 2007. This manual provides details for district personnel regarding inventory maintenance including material management, reconciliations, and inventory procedures.

The KYTC “OMS Material Inventory User’s Guide” provides the following guidelines:

- The person responsible for ordering and issuing inventory should not be counting the inventory. This means that timekeepers should only help with locating materials, but should not be in charge of counting or recording of inventory items.
- Counts shall be performed in teams of at least two people. One person is responsible for the count, and the other is responsible for recording.
- Prior to inventory, items should be organized. Like items should be grouped together in one area and stockpiles should be shaped to make measurements easier. Standard stockpile shapes for bulk materials are cone or tent.
- Bulk material stockpile quantities should be calculated as outlined in the Stockpile Quantity Calculation Procedures.

Good internal controls dictate:

- The inventory data of the inflow and outflow of materials be up to date. The OMS system should reflect accurate quantities of all available inventory items.
- Proper training be provided to all inventory takers. The KYTC “OMS Material Inventory User’s Guide” should be presented to all inventory takers.
- Proper procedures be performed in the reconciliation process between the actual inventory count to the quantities of inventory in OMS. KYTC “OMS Material Inventory User’s Guide” explains proper procedures for performing the reconciliation process and should be completed in its entirety.
- Materials be properly organized. Materials that are scrap and salvaged should not be placed with usable materials.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-61: The Kentucky Transportation Cabinet Should Improve Procedures For Maintenance Materials (Continued)

Recommendation

We recommend:

- KYTC provide additional training to the OMS timekeepers, district personnel, and the inventory teams that conduct the annual inventory to make sure they understand the inventory procedures.
- KYTC require the inventory teams to sign a statement saying they have read and understand the inventory procedures as set forth in the KYTC “OMS Materials Inventory User’s Guide” prior to the year-end inventory being conducted.
- All inventory activity be recorded in OMS as it occurs. Crewmembers should be reminded to always inform the timekeepers of inventory increases and decreases.
- Additional procedures be added to the “OMS Materials Inventory User’s Guide” to clarify how the following items should be recorded, store, disposed and removed in OMS:
 - Inventory that is returned upon completion of project, both usable and non-usable (guard rail, pipe, etc).
 - Obsolete items (including a definition of what makes an item obsolete).
 - Scrapped items.
- District personnel double-check their reconciliation in order to make sure all corrections were made. The OMS Administrator should remove the ability to delete OMS transactions. If a correction is needed, a separate reversing transaction referencing the original incorrect transaction should be entered.

Management’s Response and Corrective Action Plan

The OMS Team accepts the recommendations of the APA and plan to:

- *Update the “OMS Materials Inventory User’s Guide” with procedures that address the following:*
 - *Inventory that is returned upon completion of project*
 - *Obsolete items*
 - *Scrapped items*
 - *Process of how items are to be stored, disposed, and removed in OM*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-61: The Kentucky Transportation Cabinet Should Improve Procedures For Maintenance Materials (Continued)

Management's Response and Corrective Action Plan (Continued)

- *Provide additional training to OMS district personnel to ensure uniformity in inventory count practices.*
- *Require all inventory teams to sign an acknowledgement statement indicating they have read and understand the inventory procedures.*

Our tentative timeframe to have all necessary changes made to the OMS Materials Inventory User's Guide will be the end of December 2007 and the training of district personnel by the end of February 2008.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-62: The Kentucky Transportation Cabinet Should Ensure Management Is Aware Of Equipment Purchase Procedures And Implement Procedures For Noncompliance**

During the Kentucky Transportation Cabinet (KYTC) audit of capital assets, we reviewed the agency's disposals of buildings and equipment for fiscal year 2007 (FY07). Our testing identified equipment that was sold improperly and without the authority of the Finance and Administration Cabinet (FAC). In these transactions, KYTC extended credit to a county government for the purchase of equipment, and the final reimbursement to the Commonwealth was netted against other state funds due to the county in the following fiscal year.

Equipment sold to a County Fiscal Court did not follow appropriate policies and procedures. On January 22, 2007 four pieces of equipment were sold to one county for \$19,000 via an arrangement in which the county agreed to pay by August 10, 2007. The Director of the Division of Equipment made the recommendation for surplus, but the Delegated Agency Head did not approve the surplus property form until November 8, 2007, which was 9 ½ months after the equipment transfer. The Director of Division of Surplus Property (in the FAC) also approved the document on November 8, 2007, but the form contained a written note stating, "Equipment sold improperly and without authority of Finance by the Transportation Cabinet, Office of the Secretary. SP." On May 24, 2007, another piece of equipment was sold to the same county for \$7,500, again via a similar arrangement.

The two arrangements created by KYTC to transfer the equipment were documented on forms titled "Memorandum of Agreement." However, the "Memorandum of Agreement" was signed by only the County Judge Executive, and did not contain a signature by an authorized agent of the KYTC. According to KYTC personnel, the agreement was created because the County Judge Executive stated that the county needed equipment and did not have the money to purchase it. KYTC made a decision to create the "Memorandum of Agreement" as a way to transfer the property to the county, and obtain an agreement for payment using future county road aid funds as a guarantee. The "Memorandum of Agreement" required the county to pay a total of \$26,500 by August 10, 2007, or the KYTC could withhold or offset the amount from future funding. On August 27, 2007, KYTC created an interaccount transaction to reimburse the Division of Equipment \$26,500 for the equipment purchased by this county by offsetting the Road Aid Fund that is portioned to the counties on an annual basis.

Since the "Memorandum of Agreement" was issued in FY 07 selling the county the equipment, but the \$26,500 was not withheld until FY 08, it should have been reported as an accounts receivable by KYTC. Discussions with the KYTC staff verified that it was not recorded in accounts receivable, which understates the FY07 receivables by \$26,500.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-62: The Kentucky Transportation Cabinet Should Ensure Management Is Aware Of Equipment Purchase Procedures And Implement Procedures For Noncompliance (Continued)**

Based on discussions with KYTC personnel, the KYTC Secretary's Office gave the Division of Equipment the authority to transfer the property without following the documented policies and procedures set forth by the FAC for the appropriate disposal of surplus property.

The failure of KYTC to obtain two signatures on the "Memorandum of Agreement" raises questions about the validity of the agreement. A valid "Memorandum of Agreement" should be signed by all the parties involved in order to document a mutual understanding of the transaction.

Also, the "Memorandum of Agreement" created by KYTC says "The County agrees to be responsible and/or liable for all costs associated with this purchase and if for some reason, payment is not received, the Cabinet shall have the right to withhold and/or offset the amount from future funding pursuant to state and/or federal law and/or pursue and remedy in law or equity". Based on this language and also due to the absence of signatures from both parties, the "Memorandum of Agreement" form appears to act more as a promissory note than a Memorandum of Agreement. This indicates KYTC extended credit to the county for the purchase of the equipment.

Per the FAC User Guide: Surplus Property Disposal, "...Payments for surplus property transferred to a local government or non-profit organization can be paid with official organization check, i.e., no personal checks." There are no provisions for transferring surplus property on a credit basis.

Also, proper internal controls dictate that KYTC should not enter into financial lending arrangements with any local government based on future anticipated County Road Aid funds. KYTC should instead direct the government to obtain financing from legitimate lending institutions, which can assess the government's financial stability.

Proper internal control also dictates that all MOAs be signed by both parties in order for the agency to properly document that a legal binding agreement existed.

FAC requires each agency to report accounts receivable as of June 30 in the annual Closing Package to satisfy financial reporting requirements, as well as KRS 45.241. KRS 45.241 (10) (b) states,

Each cabinet shall report annually by October 1 to the Interim Joint Committee on Appropriations and Revenue on:

The amount of previous fiscal year unliquidated debt by agency, including debts due to improper payments, fund type, category, and age, the latter to

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-62: The Kentucky Transportation Cabinet Should Ensure Management Is Aware Of Equipment Purchase Procedures And Implement Procedures For Noncompliance (Continued)

be categorized as less than one (1) year, less than five (5) years, less than ten (10) years, and over ten (10) years; and the amount, by agency, of liquidated debt, including debts due to improper payments, not referred to the Department of Revenue; a summary, by criteria listed in subsection (6)(a) of this section, of reasons the Department of Revenue provided for not requesting referral of those liquidated debts; and a summary of the actions each agency is taking to collect those liquidated debts.

Recommendation

We recommend:

- KYTC Division of Equipment reviews the FAC User Guide: Surplus Property Disposal, and implement procedures to ensure compliance.
- KYTC should refrain from granting advancements or loans to local governments based on future anticipated Road Aid allocations.
- KYTC should implement procedures to ensure that all accounts receivable are properly recorded at year-end.
- KYTC should obtain necessary approvals from both parties when entering into Memorandums of Agreement.

Management's Response and Corrective Action Plan

The Division of Equipment acknowledges that proper procedures were not followed concerning two isolated incidents of the sale of surplus equipment. However, this was beyond the control of Division of Equipment employees. The Director – Division of Equipment entered into this arrangement even after being informed by Division of Equipment personnel that proper procedures for the sale of surplus property were not being followed. The Director, after contacting the Secretary's Office, chose to proceed with the process and instructed employees to prepare the paperwork. The Director – Division of Equipment chose to not send the documents through the proper channels. Personnel responsible for reporting of fiscal year closing did not have access to any documentation concerning this incident. The transfer of money was not made during fiscal year 06-07 nor was the proper documentation of sale, so there were no indicators of this sale transpiring for employees responsible for the closing to consider. Employees will include this in fiscal year 08 closing as the transfer of money was in August 2007.

The Division of Equipment would like to note to the auditors that they completely understand the laws, rules, and regulations governing the sale of surplus equipment. These employees have always held themselves to the highest ethical level concerning the disposal of surplus equipment.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-62: The Kentucky Transportation Cabinet Should Ensure Management Is Aware Of Equipment Purchase Procedures And Implement Procedures For Noncompliance (Continued)**

Management's Response and Corrective Action Plan (Continued)

Those procedures have always been followed and will continue to be followed by personnel involved. The Division of Equipment has never before granted advancements, credit, or Memorandums of Agreement.

Auditor's Reply

The APA does concur that the money transfer and proper signature authority did not occur until FY08. However, the transfer of the equipment including the title transfer and the memorandum of agreement occurred in FY07. At this time KYTC categorized the equipment as a disposal in FY07. Due to the equipment showing up on the Fixed Asset listing as a disposal in FY07, and the transfer of money not taking place until FY08, it should have been an accounts receivable in FY07.

We would also like to note that during our interview with the former KYTC Director of the Division of Equipment, he indicated the decision to sell the equipment to the county came from the Secretary's Office. He stated that once the Secretary's Office was aware of the situation, it was their decision to create a Memorandum of Agreement and disregard the policies and procedures.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-63: The Kentucky Transportation Cabinet Should Ensure Proper Approvals Are Constantly Applied

During the fiscal year 2007 Kentucky Transportation Cabinet (KYTC) testing of expenditures, we noted several instances where the same person applied the first and second level approvals in the eMARS system. The documents in question were for contractor pay estimates. Normally, these transactions require the Division of Construction to apply the first level approval, and the Division of Accounts applies the second/final level of approval. We noted instances where the Division of Construction approval was bypassed, and the Division of Accounts applied both approvals.

The bypass in the approval process was caused by pressures to get the payments out in a timely manner.

Although, the risk of fraud is minimized because contractor pay estimates are approved at the District Level before being entered into the eMARS system, an individual should not have the ability to apply first and second level approvals in eMARS. There is an increased risk that an individual could commit fraud and/or illegal acts and it remain undetected.

Good internal controls dictate all transactions should be properly authorized to ensure data integrity. No single user should have the ability to bypass the established approval process for transactions entered into the accounting system.

Recommendation

We recommend the Division of Accounts refrain from bypassing approvals for contractor pay estimates and other transactions in eMARS. If possible, KYTC should review approval authority of its personnel to ensure it allows only proper authorizations and reduces the risk of bypassed controls. In addition, we recommend that the individuals in the Division of Accounts and the Division of Construction be reminded of the importance of the correct approval process.

Management's Response and Corrective Action Plan

The KYTC Division of Accounts adheres to established internal controls, procedures, and policies. However, the challenges facing KYTC in relationship to paying construction vendors during the eMARS conversion was enormous. As evidenced by these payments, some conversion issues did not present themselves for several months. There were instances where it was necessary to deviate from normal procedures to ensure that contractors were paid in accordance with contractual stipulations. The tracking data clearly indicates that the approvals applied by Accounts were made at the end of workdays in an attempt to ensure that payments would hit the nightly cycle.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-63: The Kentucky Transportation Cabinet Should Ensure Proper Approvals Are Constantly Applied (Continued)**

Management's Response and Corrective Action Plan (Continued)

At no time were payments in jeopardy of being erroneous or diversion due to very stringent compensating controls such as:

- Two of the cited payments were mailed directly to the vendor and not handled by KYTC staff.*
- One payment (because of the lateness of remittance) was turned over to the vendor who signed for the payment.*
- The payment transactions were generated through an automated interface which is not controlled by any one individual.*
- All payment estimates originate in remote locations and are logged into the interface system by program managers.*
- No one in Accounts has the capacity to create interface transactions.*
- All interface transactions were pre-audited by a Pre-Audit Branch employee.*
- The approvals were applied by the Assistant Director who is not a Pre-Audit Branch employee.*
- There was significant transparency in producing these payments through the involvement of dozens of KYTC and Finance Cabinet personnel who were involved in moving these transactions as evidenced by numerous emails and electronic actions.*
- The interface was designed to have all levels of approvals applied by the system. However, this feature has been turned off so the Accounts Pre-Audit Branch can review and manage all approvals.*
- Only the Director and Assistant Director of Accounts have access to both worklists. No other employees can apply both approvals.*

Please note that we agree this was not the preferred manner in which to process these transactions. However, it was necessary under the circumstances. State and Federal funds were not at risk throughout this process. The Division of Accounts believes in strong internal controls and will continue to adhere to established policies and procedures.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-64: The Kentucky Transportation Cabinet Should Implement a Policy Or Written Procedures Regarding Capitalized Cost

The Kentucky Transportation Cabinet (KYTC) is not properly classifying infrastructure expenses. The structure of the eMARS accounting model allows the Cabinet to track expenditures around the three major areas (Capitalized, Maintenance, and Preservation) identified for the modified approach. During testing of capitalized expenditures for FY 07, we reviewed the supporting documentation on forty (40) infrastructure expenses and noted:

- Three (3) expenditures totaling \$719 were improperly classified as capitalization expenses. These expenditures included the purchase of air fresheners, paper and office supplies.

The KYTC Division of Accounts performs a pre-audit on all expenses greater than \$1,000. These expenditures did not meet the \$1,000 threshold; therefore, they were not reviewed by accounting staff. Proper internal control over capitalization expenditures processing requires appropriate review and authorization. In cases in which Division of Accounts staff do not pre-audit expenditures, district staff should be trained on proper classification of expenditures.

Expenditures that are improperly classified as capitalization expenses inflate the amount shown on the financial statement for costs associated with maintaining the Commonwealth's infrastructure at specified condition levels.

GASB Statement No 34 Basic Financial Statements - and Managements Discussion and Analysis - for State and Local Governments introduces an alternative approach to infrastructure assets that it terms the modified approach. The modified approach supports asset preservation and is an alternative to depreciation.

This alternative allows the Commonwealth to capitalize those expenditures that increase the original capacity or efficiency of the infrastructure assets that are being capitalized.

Good internal controls dictate that expenditure be properly classified to ensure accurate financial reporting.

Recommendation

We recommend the Kentucky Transportation Cabinet provide a policy or establish written procedures documenting what costs can be capitalized, and train all district staff entering invoices regarding this policy.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-64: The Kentucky Transportation Cabinet Should Implement a Policy Or Written Procedures Regarding Capitalized Cost (Continued)

Management's Response and Corrective Action Plan

KYTC understands the importance of proper internal controls over the classification of expenditures within the eMARS accounting and budget structure and agrees that documented policies and procedures must be in place so that staff entering invoices can understand the proper classification of costs. KYTC has established controls to avoid the possibility of material misstatements within the financial statements; however, with all internal control structures absolute assurance is impossible. KYTC will take corrective action to ensure that policies and procedures related to the classification and identification of highway infrastructure costs are documented and are communicated to all affected personnel.

In regards to the specific condition of this finding, KYTC employees annually process over \$1.5 billion in accounts payable. We feel the finding contained herein demonstrates that these controls are working as designed since the error detected by APA is only .02% of the value of the transactions sampled. It is important to note that the costs deemed improperly classified by APA were in fact costs directly attributed to specific road projects. The items in question were office supplies used specifically by KYTC engineers overseeing three massive projects. Although these expenditures appear at first to be indirect costs they were in fact charged to the benefiting cost objective.

Auditor's Reply

The APA does appreciate that KYTC understands the importance of the documented policies and procedures in regards to the proper classification of capitalized cost.

KYTC's response indicates that the errors identified account for only .02% of the total expenses in the sample; however, out of the 40 documents tested three of them were coded in error. When the error rate is considered along with the agency's lack of a formalized policy, it increases the risk that potentially more significant errors exist due to an improper methodology for capitalizing costs. Items coded to capitalized expenses should only be for long-lived items having a useful life greater than one year. The items should not be disposable or consumable. Even if the office and janitorial supplies were used by the agency during the course of project-related work, they should not be coded as a capitalized expense. The APA will examine KYTC's methodology more closely during the FY 08 audit to determine the extent of this methodology for capitalizing costs.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-65: The Kentucky Transportation Cabinet Should Ensure That Bridge Inspections Be Performed In A Timely Manner

The Kentucky Transportation Cabinet's (KYTC) Division of Maintenance is responsible for inspecting bridges in the state of Kentucky once every two (2) years for structural damage and/or any issues that may effect its operation. Inspectors throughout the state inspect each bridge using the Structure Inventory and Appraisal Sheet (Bridge Inspection Report) to document their findings to the Cabinet. We reviewed 40 Bridge Inspection Reports and found the following weaknesses:

- Bridges in the Commonwealth of Kentucky were not inspected timely. 35 of the 40 bridges were inspected more than two (2) years from the previous inspection date. The Bridge Inspection Report includes an inspection date that is completed by the inspector at the time the inspection takes place. When reviewing the Bridge Inspection Reports we found 35 inspection dates that exceeded the two (2) year threshold for inspections.
- The Bridge Inspection Reports were not properly reviewed. After the bridge is inspected, the Bridge Inspection Reports are reviewed by the District and the Central Office. Of the 40 bridges inspected 34 were not properly or completely reviewed. 23 of the 40 bridges inspected had no inspection review. There was also no indicator on the Bridge Inspection Report to show a review had taken place, however KYTC was able to provide review information upon request. There were eleven (11) bridge inspections that only had District level review.

Lack of timely inspections violates Title 23 Highways, Chapter I, Federal Highway Administration, Department of Transportation regulations. Without regularly scheduled inspections there is a risk that the changes in the physical and functional conditions of the bridges will not be identified.

Inspections that are not reviewed timely do not provide the quality control and quality assurance that is required by the Federal Highway Administration. If reviews of inspections are not performed in a timely manner the validity of the inspection may come into question. The inspections may include time sensitive information that would be critical to the continued quality and use of the bridges. The requirement that bridges' be inspected every two (2) years loses its effectiveness if the review process is delayed.

Title 23 Highways, Chapter I, Federal Highway Administration, Department of Transportation regulations, Subpart C-National Bridge Inspection Standards, Sec. 650.305 - Frequency of inspections states "(a) Each Bridge is to be inspected at regular intervals not to exceed 2 years in accordance with section 2.3 of the AASHTO Manual (3) of Code of Federal Regulations."

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-TC-65: The Kentucky Transportation Cabinet Should Ensure That Bridge Inspections Be Performed In A Timely Manner (Continued)

Sec 650.303 Inspection Procedures states “(a) Each highway department shall include a bridge inspection organization capable of performing inspections, preparing reports, and determining ratings in accordance with the provisions of the AASHTO Manual \1\ and the Standards contained herein.

Title 23 Highways, Chapter I, Federal Highway Administration, Department of Transportation regulations, Subpart C—National Bridge Inspection Standards, Sec 605.313 Inspection Procedures states “(g) *Quality control and quality assurance.* Assure systematic quality control (QC) and quality assurance (QA) procedures are used to maintain a high degree of accuracy and consistency in the inspection program. Include periodic field review of inspection teams, periodic bridge inspection refresher training for program managers and team leaders, and independent review of inspection reports and computations.”

Recommendation

We recommend KYTC adhere to the requirements of Title 23 Highways, Chapter I, Federal Highway Administration, Department of Transportation regulations related to Inspection Procedures and Inspection Frequency.

Management’s Response and Corrective Action Plan

To ensure compliance with the National Bridge Inspection Standards as promulgated in 23 CFR 650, Subpart C, we found through further investigation:

17 of the 35 bridges exceeding the 24 month inspection cycle are acceptable within KYTC policy and NBIS (23 CFR 650 C) policy guidelines.

Explanation: KYTC policy for assignment of inspection work is on a monthly schedule (i.e. Bridges in a particular county or region, within a district, are assigned for inspection in a calendar month. If county XX is assigned for inspection in February, each February the substandard bridges in county will be inspected at the prescribed 12 month interval and the remaining structures on the 24 month cycle will be inspected every other February). KYTC internal policy provides for 30 days following an assigned month leeway for inclement weather, high water, mechanical access scheduling, resource procurement or other unavoidable hindrances beyond control. The same 30 day leeway is allowed by the FHWA and NBIS.

Corrective action: None

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-65: The Kentucky Transportation Cabinet Should Ensure That Bridge Inspections Be Performed In A Timely Manner (Continued)****Management's Response and Corrective Action Plan (Continued)**

Quality Control Measures: The KYTC, in response to revisions to the National Bridge Inspection Standards as published in the Federal Register, December 14, 2004, has implemented a Quality Control/ Quality Assurance policy for the Bridge Inspection program. A copy of KYTC QC/QA policy will be made available upon your request.

18 of the 35 bridges fell outside the normal inspection cycle and are considered delinquent for frequency of inspection in accordance with 23 CFR 650 C.

Explanation: KYTC began the process of implementing Pontis Bridge Management System (BMS), new software for bridge inspection data collection and bridge management, in February 2007. A key component of Pontis BMS is a highly sophisticated means for tracking inspection cycles and due dates for inspections. To accommodate the data transfer from KBIS (old operating platform) to Pontis (new platform), all electronic input of ongoing inspection data being collected was delayed for 8 months causing significant backlog of paper copies of inspection reports needing to be input to database; in addition to the problems associated with the system switch is the additional time required to gather element level data in addition to NBI data necessary for inspections in Pontis BMS. The additional time necessary for inspection was both anticipated and deemed acceptable with every effort to adhere as closely to inspection frequency as possible. The bridges that fall under this explanation with delinquent inspection cycles in the following list will be marked with "Pontis":

District One

053-B00021N: Pontis

004-B00028N: Pontis

District Two

117-C00051N: Pontis

054-B00137R: Pontis

District Five

056-B00330N: Data showing on server database (info supplied to LRC) and actual inspection data inconsistent- Last inspection was 03/2007; inadequate staffing.

056-B00310L: Data showing on server database (info supplied to LRC) and actual inspection data inconsistent- Last inspection was 07/2007; inadequate staffing.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-65: The Kentucky Transportation Cabinet Should Ensure That Bridge Inspections Be Performed In A Timely Manner (Continued)****Management's Response and Corrective Action Plan (Continued)****District Seven**

105-B0067N: Pontis; inadequate staffing

105-B00138N: Pontis; inadequate staffing

034-B00043N: Pontis; inadequate staffing

034-B00119N: Pontis; inadequate staffing

District Ten

013-B00053N: Pontis; paper copy will be downloaded into Pontis. (Inspection performed on 7/18/2007)

013-B00060N: Pontis; paper copy will be downloaded into Pontis. (Inspection performed on 7/18/2007)

013-C00029N: Pontis; paper copy will be downloaded into Pontis. (Inspection performed on 7/18/2007)

District Eleven

063-C00007N: The District Bridge Engineer changed the inspection cycle from February completion date to a July completion date (accounts for 5 months of delinquency) the remainder of delinquency is attributed to Pontis.

026-B00085N: Pontis

District Twelve

036-B00130N: Pontis

067-B00111N: Pontis

067-B00095N Pontis

Corrective Action: Inspectors in every district are working at 100% capacity and being reminded of the need to catch up to normal inspection cycles. A contract for outside inspection labor has been set up through Division of Purchases for hourly labor hires. These contracts are being utilized to the fullest extent to advance the cycles back into compliance. Additional full time inspection staff is needed in most districts to ensure KYTC's continued ability to perform inspections timely.

A formal report for delinquencies due to unacceptable schedule change will be sent to District Eleven Inspection staff and Management Personnel.

Quality control Measures: Internal Quality Assurance reviews, as well as FHWA Bridge Inspection Program Audits, are ongoing to track performance during the impeded schedule.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-65: The Kentucky Transportation Cabinet Should Ensure That Bridge Inspections Be Performed In A Timely Manner (Continued)****Management's Response and Corrective Action Plan (Continued)**

Of the 40 bridges inspected 34 were not properly or completely reviewed; 23 of the 40 bridges inspected had no inspection review; eleven (11) bridge inspections only had District level review.

Explanation: Many operational modifications have been systematically added/repared as part of KYTC's implementation of Pontis BMS. The process allowing electronic review of inspection data has just recently become operational. All paper copies of inspections received proper Q/A review at the district level throughout the migration period. Primary electronic reviews and Secondary (Central Office) reviews have commenced since the "Review Applet" in Pontis has become operational.

Corrective action: Continued work on Primary and Secondary reviews of all inspection reports.

Quality Control Measures: The KYTC, in response to revisions to the National Bridge Inspection Standards as published in the Federal Register, December 14, 2004, has implemented a Quality Control/ Quality Assurance policy for the Bridge Inspection program. A copy will be made available upon your request.

KYTC Division of Maintenance, under FHWA oversight, is (1) aggressively working toward full implementation of Pontis BMS with 100% operational capacity, (2) encouraging KYTC executive staff and district management staff to hire more inspectors, (3) continuing efforts to rectify backlogs of inspections due and necessary reviews and (4) continuing to monitor the Bridge inspection program by means of QC/QA reviews. Program compliance with the National Bridge Inspection Standards and State guidelines will remain a priority for the Kentucky Transportation Cabinet.

Auditor's Reply

KYTC's response indicates that it is an acceptable practice to exceed the 24 month requirement by 30 days. NBIS does provide for the 30 day "leeway" or grace period for certain circumstances that are unavoidable or beyond control. According to NBIS "The adjusted date should not extend more than 30 days beyond the scheduled inspection date, and subsequent inspections should adhere to the previously established interval".

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-TC-65: The Kentucky Transportation Cabinet Should Ensure That Bridge Inspections Be Performed In A Timely Manner (Continued)**

Auditor's Reply (Continued)

The 30-day extension was not brought to the attention of the Auditor, it was not documented as a formal policy of KYTC, nor was any written justification for the 30-day extension presented to the Auditor. Without an approved documented procedure there is a risk of abuse to grant a longer inspection cycle.

In addition to the corrective action plan noted by KYTC, there should be some documentation implemented to indicate that a review of the Bridge Inspection Report has taken place at either district or central office level.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-DOC-66: The Department Of Corrections Should Ensure All DOC Gateway Routers Managed By The Commonwealth Office Of Technology Are Properly Configured And Maintained**

While performing security vulnerability assessments for machines owned by the Kentucky Department of Corrections (DOC), concerns relating to the configuration of a DOC gateway were identified. Testing revealed that the gateway was extremely susceptible to denial of service (DOS) attacks. Further, discussions with DOC management revealed that the agency had experienced critical network service connectivity issues during the last several years that according to DOC were not resolved by the Commonwealth Office of Technology (COT). COT maintains the DOC network infrastructure.

Our initial scanning efforts within the DOC central-level network noted no service connectivity issues. However, our security assessment tools resulted in a temporary disruption of service when we attempted to access the network of one of the larger correctional facilities from within the central-level DOC network. Our assessment traffic encountered a DOC gateway router that physically resides at and is managed by COT. The parameters of our security-testing tool had to be scaled back to the lowest level of activity to prevent significantly degrading the network due to this gateway router not appropriately handling multiple network traffic sessions. Problems with the gateway router resulting in network degradation were also identified later when the office was not performing security assessment testing.

As a result of our findings, COT increased the session table limits of this gateway router as a temporary resolution to the problem encountered by DOC. However, the concern remains that this machine is not properly handling network traffic sessions as intended.

Discussions with DOC management revealed that DOC often experienced system access difficulties since it implemented video streaming technologies several years ago. This concern is strengthened due to the planned implementation of additional new systems that could significantly increase network traffic. It is our understanding that during the last several months COT had been performing feasibility studies to address DOC infrastructure improvements, but the feasibility studies had not been presented to DOC for consideration at the time of our fieldwork.

An improperly configured gateway could lead to future disruptions of service if the session limit is exhausted. Session table limits could be exhausted due to a spike in normal network activity, a malicious DOS attempt, or other reasons. Current DOC system traffic is within a narrow margin of the sessions allowed on the DOC gateway router and could continue to cause future disruptions of service as new automated systems are implemented through this network.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DOC-66: The Department Of Corrections Should Ensure All DOC Gateway Routers Managed By The Commonwealth Office Of Technology Are Properly Configured And Maintained (Continued)

To lessen the risk of future service disruptions, the DOC gateway router should be configured to provide an adequate session limit to accommodate the level of traffic generated by DOC after the implementation of KOMS. The session table should be able to accommodate any spikes in regular DOC traffic in addition to the requirements of other new systems to be implemented in the upcoming year. Gateway routers should handle traffic sessions in a manner consistent with industry expectations. Network infrastructures should be established and maintained in a manner to ensure acceptable availability of all critical systems.

Recommendation

We recommend DOC work closely with COT to ensure that the configuration changes to the gateway router are adequate to sufficiently prevent any future service disruption issues. Any anomalies noted with the actions being performed by the gateway router should be investigated and resolved with the understanding that an increase in traffic load is expected during the coming year. We further recommend that DOC request COT to complete and present to DOC management any feasibility studies initiated regarding improvements to the DOC infrastructure. Further, these two agencies should work together to ensure an acceptable level of system availability exists for all current and planned critical DOC systems.

Management's Response and Corrective Action Plan

DOC sent an e-mail to COT to review the Cause/Effect, Criteria, and Recommendations above. COT has responded they will review the above issue and get back with us. We will resolve the issue above with COT based on COT/DOC recommendations.

COT reviewed the findings and concluded that they believe the current configuration of the DOC firewall to be sufficient for current DOC business/security objectives. However they state that DOC should consider an additional firewall to improve business continuity.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-DOC-67: The Department Of Corrections Should Ensure Anonymous FTP Access To Agency Machines Is Disabled**

During the security vulnerability assessments for FY 2007 for machines owned by the Kentucky Department of Corrections (DOC), our examination revealed two machines with an open file transfer protocol (FTP) connection that allowed anonymous access.

Specific to one of these machines, we noted fourteen files that could be downloaded via anonymous FTP connection from outside the agency network. Included among these files was sensitive information from a personnel application, which included social security numbers, names, and leave balances of some facility employees. Further, the server allowed files to be uploaded through this anonymous connection. DOC subsequently disabled the anonymous access to this server after the vulnerability was identified by our audit. However, this vulnerability was present during FY 2007.

Specific to the second machine, similar weaknesses existed as noted above with the exception that this connection could only be accessed from within the agency's network. Further, though we noted six files on this machine that could be accessed and downloaded via FTP, they did not contain sensitive information. In particular, the files contained demographic information, which are extracts from the Offender Records Information Operations Network (ORION) application that are loaded to this server by the Commonwealth Office of Technology (COT). Discussions revealed that COT did not require the anonymous FTP access but DOC is currently assessing the changes necessary to some interfacing programs before closing this anonymous FTP access. At the end of our fieldwork this vulnerability still existed. It should be noted that this FTP service allowed uploads to the server with anonymous access as well.

For security purposes, detailed information concerning the specific servers that contributed to these findings is being intentionally omitted from this comment. However, these issues are thoroughly documented and will be sent hardcopy to the appropriate agency personnel.

The existence of anonymous FTP access to agency servers is an invitation for intruders to enter the system and potentially gain access to sensitive information. The ability to upload files to agency servers could result in files being altered or malicious code being executed. It appears that this vulnerability occurred due to the system reverting to default settings after a patch was applied and/or based on miscommunications between DOC and COT.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-DOC-67: The Department Of Corrections Should Ensure Anonymous FTP Access To Agency Machines Is Disabled (Continued)**

To minimize the risk of unauthorized access to a machine, all internal and external users accessing agency servers via FTP should do so using a valid userid and password. Anonymous access should not be utilized since any unauthorized users can gain access to agency resources.

Recommendation

We recommend that DOC review all agency machines to ensure that all FTP services have anonymous access disabled. In any cases where anonymous FTP access was utilized for business purposes, individual user accounts and passwords should be established to ensure that users are properly authorized to access the server. We also recommend that any necessary changes be made to embedded passwords within programs interfacing with these FTP servers so that anonymous access can be eliminated. If this is not feasible then compensating security measures should be taken to secure these FTP services.

Management's Response and Corrective Action Plan

DOC will continue to review all agency machines to ensure that FTP services have anonymous access disabled. If there are instances where this service is required we will remedy as soon as we are able. To further alleviate any problems noted with the second machine referenced above the machine will need to be moved to the Central Office and appropriate firewall rules will be put in place. Encryption software will be implemented for the system that resides on this machine to secure the data that is transmitted. DOC is currently assessing the changes necessary to some interfacing programs.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-DOC-68: The Department Of Corrections Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose**

During the security vulnerability assessments for FY 2007 for machines owned by the Kentucky Department of Corrections (DOC), our examination of 234 machines revealed that there were fifty-two machines (or 22%) with ports open that may not have a specific business-related purpose, one of which was noted during the FY 2006 vulnerability assessment. Due to the large number of issues, we grouped the findings below by port number and application.

Port 7 – Echo

One machine was identified as having Port 7 open, which is used for the Echo protocol. Unless there is a strong business reason for this service running, it should be disabled since it can waste resource space and CPU cycles and can be abused in several manners.

Port 9 – Discard

One machine was identified as having Port 9 open, which is used for the Discard protocol. Unless there is a strong business reason for this service running, it should be disabled since it can waste resource space and CPU cycles and can be abused in several manners.

Port 13 – Daytime

One machine was identified as having Port 13 open, which is used for the Daytime protocol. Unless there is a strong business reason for this service running, it should be disabled since it can waste resource space and CPU cycles and can be abused in several manners.

Port 17 – Quote of the Day

One machine was identified as having Port 17 open, which is used for the Quote of the Day protocol. Unless there is a strong business reason for this service running, it should be disabled since it can waste resource space and CPU cycles and can be abused in several manners.

Port 19 – Character Generator

One machine was identified as having Port 19 open, which is used for the Character Generator protocol. Unless there is a strong business reason for this service running, it should be disabled since it can waste resource space and CPU cycles and can be abused in several manners.

Port 21 – FTP

Fourteen machines were identified as having Port 21 open allowing anonymous FTP access, two of which will be included in a separate comment regarding file transfer protocol (FTP) anonymous access due to the severity of the information that was accessible on those machines. We were able to access five of the fourteen machines from within the agency; we were able to access the remaining nine machines from our office outside the agency network. All fourteen machines should have anonymous access via FTP restricted.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-DOC-68: The Department Of Corrections Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose (Continued)**

Port 23 – Telnet

One machine was identified as having Port 23 open that did not have a password set. The telnet session allowed for printer configuration settings to be viewed and changed. Any user of telnet services on the network should be required to provide an authorized username and password.

Port 25 – SMTP

Six machines were identified as having Port 25 open, which is used for the Simple Mail Transfer Protocol (SMTP). It is unclear if there is a business-related purpose for this open port, and there are multiple vulnerabilities associated with it.

Port 53 – DNS

One machine was identified as having Port 53 open, which is used for the Domain Name Server (DNS) service. There are many security vulnerabilities associated with this service. A remote attacker could execute arbitrary code with the privileges of the application that made the request or cause a denial of service. In follow-up to the FY 2006 formal comment, the agency indicated that this open port was necessary for domain controllers; however, this is not a domain controller.

Port 80 – HTTP

Thirty-six machines were identified as having Port 80 open. Specifically, there were nineteen machines that indicated the website was under construction. Of the remaining seventeen machines, there were three machines that displayed no web page. In addition, two machines provided an outdated DOC webpage that appears to no longer be in use. When no default website page or login request is present, normally this means that no application/web service is running and the port is not needed. This exposure would be enticing to a hacker, so the necessity of this port should be determined. The remaining twelve machines had print management websites running, which permitted an anonymous user to change printer and network configuration settings and possibly passwords. These machines are susceptible to attack and should be password protected.

Port 81 – HOSTS2 Name Server

One machine was identified as having Port 81 open, which is typically used for the HOSTS2 Name Server protocol. There are multiple worms and Trojans associated with this port, and its necessity should be reviewed.

Port 110 – POP3

One machine was identified as having Port 110 open, which is typically used for the Post Office Protocol – Version 3 (POP3). There are multiple Trojans associated with this port, and its necessity should be reviewed.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-DOC-68: The Department Of Corrections Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose (Continued)**

Port 111 – sunrpc

Three machines were identified as having Port 111 open, one of which was also noted during the FY 2006 vulnerability assessment. This port is used by the Unix Sun Remote Procedure Call (RPC) service, which is a gateway to a variety of other services. We could not determine the validity of the service, and it is a potential Trojan port.

Port 161 – SNMP

Two machines were identified as having Port 161 open. This port is running Simple Network Management Protocol using writeable community strings. One of the machines noted allows the default private and proxy community strings, and the remaining machine allows the default public and snmp-read community strings. There are also several Denial of Service attacks associated with this port.

Port 443 – HTTPS

Two machines were identified as having Port 443 open and provided a page cannot be displayed message. When no default website page or login request is present, normally this means that no application/web service is running and the port is not needed. This exposure would be enticing to a hacker, so the necessity of this port should be determined.

Port 1433 – Microsoft SQL Server

Sixteen machines were identified as having Port 1433 open, which is typically used for Microsoft SQL server. The auditor connected to the servers utilizing default administrator credentials and a null password. Once connected, the auditor could view the machines' C:\ drives and other local drives. Housed on these machines was sensitive information from multiple DOC systems, including both inmate and personnel/payroll information. We were also able to access numerous configuration, SQL, and registry files. Each of the sixteen machines has a web service running, and the auditor was able to navigate to the directory housing the HyperText Markup Language (HTML) code. We were also able to open the directory containing the machines' Security Accounts Manager (SAM) files. The "sa" account should have a strong password so as to avoid being compromised. Basically, we gained full access to these machines. These ports should be closed or secured with strong passwords.

Port 2103 – zephyr-clt

One machine was identified as having Port 2103 open, which is typically used for the Zephyr serv-hm connection protocol. The necessity of this open port should be determined.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-DOC-68: The Department Of Corrections Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose (Continued)****Port 2301 & 49400 – compaqdiag**

Two machines were identified as having Ports 2301 and 49400 open, which are used for the Compaq Information Manager (CIM). No default page could be opened when connecting to either port on these two machines, which seems to indicate that the CIM service is not running.

Port 2702 – SMS

One machine was identified as having Port 2702 open, which is typically used for the Microsoft Systems Management Server (SMS) service. The powerful tools within this service make it a desirable platform to take control of a network. After gaining access to the SMS site database, an attacker gets virtually unlimited control of the SMS server, which allows the attacker to distribute malicious code to SMS clients and get remote control for those clients.

Port 5631 & 5632 – pcan anywhere

Twenty machines were identified as having port 5631 open, one of which also had Port 5632 open. Port 5631 listens on other ports to find other PCAnywhere servers on the local segment. Vulnerabilities may exist for both ports in the form of denial of service attacks.

Port 5800 & 5900 – VNC

One machine was identified as having Ports 5800 and 5900 open, which are used for the Virtual Network Computing (VNC) service. This machine did not display a VNC login page, which indicates that the service may not be running.

Port 8000 – irdmi

One machine was identified as having Port 8000 open, which is used for the iRDMI protocol and is a common alternative HTTP port. There are multiple vulnerabilities associated with this port, and its necessity to be reviewed.

Port 8009 – ajp13

Three machines were identified as having Port 8009 open, which is used for the Apache Jserv Protocol. DOC should ensure that the version of Apache running in connection with the Jserv Protocol is the most current. The necessity of this open port should also be reviewed.

Port 8889 – ddi-tcp-2

Three machines were identified as having Port 8889 open, which is used for the Desktop Data TCP 1 Protocol. A password-stealing worm is known to reside on this port. The necessity of this open port should be reviewed.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DOC-68: The Department Of Corrections Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose (Continued)

Other Ports (6250)

Three machines had a port open (Port 6250) that does not appear to specifically relate to known business applications. DOC should review all open ports on machines to ensure that all have a valid business-related purpose.

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

For security purposes, detailed information concerning the specific servers or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues are thoroughly documented and will be sent hardcopy to the appropriate agency personnel.

The existence of unused open ports, default profiles, and outdated system software increase potential security vulnerabilities and is an invitation for intruders to enter the system. Further, system configuration information would be useful to a hacker and should be restricted. In addition, once an intruder has access to one computer on the network through the default administrator account, the hijacked machine can then be used to attack other machines with more desirable resources.

To minimize the risk of unauthorized access to a machine, only necessary business-related ports should be open, default profiles should be avoided and system software should be kept up to date. Further, information concerning system configuration should not be made publicly available, and anonymous users should never have the ability to change these settings. The default administrator and user accounts should be secured with strong passwords to avoid being compromised.

Recommendation

We recommend DOC review all open ports to ensure there is a specific business-related purpose requiring the port to be open. If not required, then that port should be closed. If the port is necessary then DOC should ensure the most recent patches are implemented for the service in use, applications are kept updated, and that adequate logical security controls are implemented to prevent unauthorized access as necessary. DOC should disable any default profiles, disable all anonymous access to critical services, and ensure services left open are secured with a strong password.

FINANCIAL STATEMENT FINDINGS*Significant Deficiencies Relating to Internal Controls***FINDING 07-DOC-68: The Department Of Corrections Should Ensure All Open Ports On Networked Servers Have A Business - Related Purpose (Continued)****Management's Response and Corrective Action Plan**

Migration to Active Directory on January 19, 2007 resulted in one machine in question being disconnected, alleviating the instances of Port 7, Port 9, Port 13, Port 17, and Port 19 on that machine.

DOC will review the list of other open ports to ensure that there is a specific business reason requiring the port to be open. Many of these ports are located at our various institutions. All institutions affected have been notified and will review open ports on their LANS and supply the Office of Support Services' Deputy Commissioner with a response relative to their respective institutions.

DOC will ensure that patches are implemented for the service in use, applications are kept updated, and that logical security controls are in place to prevent unauthorized access. DOC will review all default profiles, anonymous access, and ensure services left open are secured with a password, which meets security requirements established.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DOC-69: The Department Of Corrections Should Develop And Implement A System Development Life Cycle Policy To Govern System Development, Testing, Modifications And Implementation

The Department of Corrections (DOC) did not develop and implement formal System Development Life Cycle (SDLC) procedures governing controls for system development, testing, modifications, and implementation. During fiscal year (FY) 2007 a new personnel timekeeping system, KRONOS, was implemented at five DOC locations to replace the manual process of managing staff time and entering it into Customer Information Control System (CICS) for processing by the Uniform Personnel and Payroll System (UPPS). Further, subsequent to the date of our fieldwork, testing and implementation of Phase I for the Kentucky Offender Management System (KOMS) Project has been deployed to replace the Probation and Parole Case Management System (PPCMS).

Review of the SDLC methodology followed for KRONOS and KOMS revealed both methodologies are vendor driven. User acceptance system testing for the KRONOS system remained the responsibility of the agency. Within documentation of DOC correspondence with the KRONOS vendor and within a formal Test Environments Recommendations Report, the vendor had recommended the agency use an environment separate from production for their testing efforts. Further, the KRONOS Project Management Handbook provided to DOC by the vendor recommends that testing include the entire process from inputs to outputs for the system. DOC staff ran two tests, considered parallel, in the production environment prior to implementing the system July 1, 2006. Neither test was a complete test run of the entire process.

The scope of the initial test run was not formally developed to cover all various processing scenarios that could be encountered. Instead, the administrators developed the scope during a brainstorming session. Additionally, this first test run only covered a sample of 50 staff members out of a population of approximately 1,300 employees, less than 4%. Documentation of the sample, results, any errors and applicable resolutions was not retained.

The data within KRONOS was manually entered into CICS for each of the staff members during the first test run as a result of issues with the interface process that uploads the data from the KRONOS server to a dataset on the mainframe. The second test run was a full payroll run but again the staff manually entered the data from KRONOS into the CICS system as a result of an issue with the interface process. Results from the second run were only spot checked by the staff results, and resolutions were not formally documented and retained.

Additionally, interface issues between the UPPS and KRONOS forced DOC staff to manually reconcile accrual balances and adjust KRONOS hours to appropriately reflect balances per UPPS.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DOC-69: The Department Of Corrections Should Develop And Implement A System Development Life Cycle Policy To Govern System Development, Testing, Modifications And Implementation (Continued)

KRONOS pre-populates Holiday Leave for each active employee within the database for each location. Further, KRONOS does not de-activate employees within the system if they transfer to another location within DOC. If a staff member transfers between locations within DOC multiple records are sent to UPPS for processing. This resulted in an employee's leave and comp earned balances not being updated for leave taken or comp earned during three FY2007 pay periods that included a holiday. Our testing revealed DOC had not identified the instances of duplication. Our testing revealed that not only was this problem present during the testing phase but was also occurring during post implementation and the reconciliation between KRONOS and UPPS was not being completely and consistently performed. Subsequent to our testing DOC manually performed adjustments and took corrective action to manually terminate employees that transferred work locations within the applicable KRONOS database.

The SDLC methodology being employed by DOC for KOMS is also vendor driven. However, again there are portions of the process that remain the DOC's responsibility. 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 will be turned over to DOC who will then be responsible for functional testing and any modifications to the system. Again, DOC has no formal SDLC policy or methodology established to control this process.

Because the testing methodology performed by DOC did not adequately consider all possible processing scenarios and a full reconciliation was not performed between KRONOS and UPPS, errors with the system processing were not identified until after the system went into live production processes. Because of this, inefficiencies and anomalies with the operations of the KRONOS system were not resolved prior to implementation. DOC and KRONOS staff members continue to spend time reviewing the program and processes to find resolutions as issues emerge. The errors noted include overpayment for some staff that should have been on leave without pay with some of that overpayment yet to be recouped at the time of our audit fieldwork.

Without formalized SDLC procedures, management increases the risk of implementing ineffective and inefficient systems and the risk that inaccurate or incomplete data will be entered within the production environment and adversely affect system-processing results. 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

FINDING 07-DOC-69: The Department Of Corrections Should Develop And Implement A System Development Life Cycle Policy To Govern System Development, Testing, Modifications And Implementation (Continued)

Recommendation

We recommend that DOC develop, implement and consistently apply adequate formal SDLC control policy and procedures. These policies and procedures 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 will develop, implement, and apply a Department wide SDLC policy. DOC's SDLC policy will include provisions to ensure that the vendor's procedures are adequate and that areas not covered by the vendor's policy are covered through DOCs internal policy. All projects will be monitored by DOC and any portion of the contract that does not involve SDLC will be supported by an internal DOC policy.

The SDLC policy will include testing strategies and methodologies, as well as control and maintenance of test and production environments, testing documentation, and procedures for migration of system changes into the production environment.

Phase One of KOMS did include testing strategies and methodologies as well as control and maintenance of test and production environments. DOC is currently in the process of completing documentation of Phase I. Phase II has not yet been implemented. Documentation for Phase II will be finalized after implementation is complete.

Concerning KRONOS the following is applicable:

KRONOS, our time keeping application, is being implemented in phases. KRONOS, the vendor, did/and is assisting with both Phase I testing and final implementation and Phase II testing and implementation of this process. DOC staff worked with KRONOS to test a multitude of applicable/pertinent scenarios.

Problems encountered in testing were brainstormed by DOC and KRONOS staff and guidance or a solution was provided by the vendor (KRONOS). An applicable and workable solution was then implemented.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-DOC-69: The Department Of Corrections Should Develop And Implement A System Development Life Cycle Policy To Govern System Development, Testing, Modifications And Implementation (Continued)**

Management's Response and Corrective Action Plan (Continued)

In Phase I all testing and implementation was done on the Production Server.

In Phase II all testing has been done on a test server. Implementation of Phase II has not yet been done - DOC is still in the testing phase.

Documentation for Phase I is still in development. Phase II documentation will be completed when Phase II has been implemented. Current documentation for Phase II is, understandably, incomplete at this time.

Currently Phase II is in the testing phase - with the vendor, KRONOS, assisting with the testing and eventual final implementation of Phase II. Once the testing is complete and all issues resolved, final implementation will take place.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DOC-70: The Department Of Corrections Should Develop And Implement A Policy Governing The Security Of Microsoft Outlook Public Folders

During FY 2007, the Auditor of Public Accounts discovered a significant security vulnerability that potentially allowed confidential and other information to be available to thousands of individuals having email access on the state's network. This information was available by accessing agency email folders listed under the heading, "public folders." We identified twelve "public folders" associated with the Department of Corrections (DOC) that had security issues.

Our review of the Corrections public folders (under the Justice public folder) identified twelve subfolders in which active calendars were viewable or confidential information was present. The following specific items of concern were noted:

- Within one of the subfolders we found one email that had a file attachment that had the social security number and date of birth of an Offender.
- Within one of the subfolders we found six emails that contained attachments revealing the social security numbers, dates of birth, and home placement locations for parolees.
- Within ten subfolders appear to be active calendars that were accessible that could potentially contain sensitive information.

As soon as these items were found, toward the end of the current Fiscal Year, we notified the Department of Corrections. Subsequently the Corrections folder was removed from visibility to the public.

The permissions granted to these folders could allow an individual to not only read the content of a folder, but also to potentially create, delete, copy, or modify the content of a folder depending on the permissions that are set for each.

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."

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DOC-70: The Department Of Corrections Should Develop And Implement A Policy Governing The Security Of Microsoft Outlook Public Folders (Continued)

Recommendation

We recommend that the agency continue to monitor the use of and access rights to agency public folders. We also recommend that the following actions be implemented immediately to ensure that any violations resulting from the inappropriate disclosure of information be reported:

- DOC should review the CIO Enterprise Policies, such as the CIO-060 Internet and Electronic Mail Acceptable Use Policy, and ensure compliance with requirements.
- DOC should develop a policy statement and specific procedures related to agency personnel responsibilities concerning the security of public folders and security measures to be taken concerning the E-mail transmission of sensitive data.
- DOC should designate specific agency personnel to administer the security access control permissions applied to public folders.
- Specified agency personnel should consistently review, on a regular basis, the security control permissions applied to public folders. Further the content within all public folders should be reviewed to ensure that all items are appropriate.
- DOC should report to all appropriate agencies or individuals that confidential information was potentially disclosed. Those requiring notification could include, but not be limited to:
 - Individuals whose social security numbers, health, or other personal information was accessible.
 - State or federal agencies that may require notification of the potential disclosure of confidential information.

Management's Response and Corrective Action Plan

- *DOC IT has reviewed the CIO Enterprise Policies such as CIO-060 Internet and Electronic Mail Acceptable Use Policy. DOC IT has also reminded staff of the acceptable use policy (via e-mail sent on 7/6/07).*
- *DOC will develop a policy concerning the security of public folders and security measures to be taken concerning the E-mail transmission of sensitive data.*
- *DOC IT has designated two individuals as administrators of security access and permissions applied to public folders.*
- *DOC IT personnel will review, on a regular basis, the security control permissions applied to public folders. During that review, the content within DOCs public folders will be reviewed to ensure that any/all items are appropriate.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-DOC-70: The Department Of Corrections Should Develop And Implement A Policy Governing The Security Of Microsoft Outlook Public Folders (Continued)

Management's Response and Corrective Action Plan (Continued)

- *DOC has removed these folders/e-mails/etc. from the public folders area as well as reviewing and removing any e-mails/etc that contain sensitive information.*
- *DOC has notified supervisors that sensitive information was potentially disclosed. Supervisors will notify, as they deem appropriate, affected individuals and/or agencies of the potential disclosure.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-PERS-71: The Personnel Cabinet Should Strengthen The Security Of System Accounts

For security purposes, detailed information concerning the specific servers or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues are thoroughly documented and have been reported in detail to the appropriate agency personnel.

During the security vulnerability assessments for FY 2007 for machines controlled by the Personnel Cabinet (Personnel), our examination revealed various system user accounts with password ages that exceeded the established password policy. Additionally, we noted several accounts that had been disabled that should be reviewed for necessity.

We obtained NetBIOS account information from one Personnel machine, which was a Primary Domain Controller (PDC). To determine if user accounts on these machines were in compliance with established Personnel policies, the auditor used the criterion that account passwords with ages over 31 days were non-compliant, which is the established agency policy. There were 54 accounts that met this criterion. These accounts had password ages between 39 and 1642 days. Also, there were 35 user accounts that were disabled, many of which had never been accessed or had not been accessed for over a year.

In addition, there were four accounts that were deemed to be unusual in nature and require further review. Three of these accounts are disabled and the other account is enabled but has not been accessed since 2004.

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 has not been used for a reasonable period of time, the account should be investigated and disabled, if appropriate. This minimizes the possibility that an unauthorized user will access the account. An account should be deleted if it is not going to be reinstated. Established password policies should be consistently applied and enforced.

Recommendation

We recommend that Personnel review all user accounts on all machines to determine which accounts are not in compliance with the established security policies. These accounts should be evaluated to determine if they are still valid accounts and are required for a business related purpose. If not, 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*****FINDING 07-PERS-71: The Personnel Cabinet Should Strengthen The Security Of System Accounts (Continued)**

Management's Response and Corrective Action Plan

The Systems Management Branch is in the process of reviewing the strength/age of the passwords on the accounts identified and have already deleted many of the disabled accounts. We have been in contact with the Commonwealth Office of Technology to inform them of our intent to request a review of the accounts in our domain which are managed by COT to ensure all unnecessary accounts are deleted. If our review indicates we have accounts which must have a static password, we will request a security exemption through COT. We estimate our review will be complete by January 15th, 2008.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-PERS-72: The Personnel Cabinet Should Disable The Simple Network Management Protocol Service On All Machines

For security purposes, detailed information concerning the specific servers or user accounts that contributed to these findings is being intentionally omitted from this comment. However, these issues are thoroughly documented and have been reported in detail to the appropriate agency personnel.

During the FY 2007 security vulnerability assessments of machines controlled by the Personnel Cabinet (Personnel), the auditor identified five machines that had the Simple Network Management Protocol (SNMP) service available and would allow an anonymous user to logon with the community string of “public” or “private.” These community strings are the default accounts for this service.

Information provided by the SNMP service concerning a machine’s functions could be useful to an intruder in developing an attack.

SNMP services should be properly implemented to ensure excessive information is not provided to unauthorized users. The default community name should be changed to increase security of the service.

Recommendation

We recommend that Personnel either disconnect the SNMP service on the noted machine or change the “public” and “private” community names to a more sophisticated name on all servers. Further, any new machines should be checked for the SNMP service to ensure the “public” and “private” community names have been changed.

Management’s Response and Corrective Action Plan

The Systems Management Branch has reviewed and verified Simple Network Management Protocol is only configured where necessary. On the servers identified as running this protocol, the community names have been changed. We will continue to investigate additional and new devices required to run SNMP and will change the community names as they are identified.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-PERS-73: The Personnel Cabinet Should Adhere To Established Procedures Governing System Access Requests For The Uniform Payroll And Personnel System

As noted in the prior year audit, the Personnel Cabinet did not adhere to established procedures concerning logical security governing the Uniform Payroll and Personnel System (UPPS). Specifically, these procedures require each employee to complete an access request form to ensure that UPPS users are provided properly authorized access to this mission critical system. Based on job responsibilities, state employees must complete a user access request form and obtain approval by the requestor's supervisor. Our audit revealed that some user access forms were not completed or maintained on file, and some of those on file were not properly completed in a consistent manner. Based on our test results, control issues were noted with seven out of the 30 users tested, or 23 percent of the sample population.

We selected a sample of access request forms for 30 new UPPS users, or 10 percent of the population. Of the users selected, the auditor could not locate the access request forms for three users, or 10 percent of the sample population. In addition, two of the users were granted access from forms that did not indicate the type of change being made, such as add, delete, or update. Further, one form contained the access request for two users. Within the request form the two user IDs were listed to be associated with the other user name and Organization Codes. The access requested for each user was inquiry to the same application.

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 UPPS.

The foundation of logical security is access control that refers to the level of access a user is granted within the system. Formal policies provide a security framework to educate management and users of their security responsibilities. The implementation and consistent application of formalized security policies and procedures ensures compliance and demonstrates 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 that the Personnel Cabinet consistently apply the established logical security policies and procedures applicable to the granting of UPPS system access to new users. Access request forms should be completed and maintained for all new users and should include all necessary information and appropriate authorizations to provide only the essential access required by the user to perform assigned job duties.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-PERS-73: The Personnel Cabinet Should Adhere To Established Procedures Governing System Access Requests For The Uniform Payroll And Personnel System (Continued)

Management's Response and Corrective Action Plan

We agree existing Personnel Cabinet policies and procedures were not consistently followed. Appropriate action has been taken to ensure these procedures will be followed in the future. In addition, supporting documentation has been requested for the users identified in this audit for which we were unable to produce accurate documentation.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-PERS-74: The Personnel Cabinet Should Ensure That Formal Program Modification Control Procedures Are Consistently Followed To Properly Control Changes To The Uniform Personnel And Payroll System**

Our FY 2007 audit of the Uniform Payroll and Personnel System (UPPS) related program modification controls identified weaknesses that should be addressed by the Department for Personnel Administration.

A sample of 17 change request forms from a population of 167 requests logged during the year was selected for testing. The formal Program Change Procedures documented by the Personnel Cabinet authorize the Director for the Division of Employment Management to approve program change requests. In the absence of the Division Director, the Commissioner of the Department of Personnel Administration is authorized to make these approvals. Of the 17 change requests reviewed, 10 requests were not appropriately approved. The Program Change Procedures did not include specific instructions for each field found on the change request form or how those fields are utilized, but discussions with the Commonwealth Office of Technology indicate the 'agency contact' field should represent the individual or the supervisor that is initiating the request. Of the 10 change requests that were not appropriately approved, four were signed as approved by the same individual initiating the change.

Further, we performed procedures to identify changes made during the fiscal year to 17 programs considered critical to UPPS processing. All program changes appeared reasonable and additional change request forms, where applicable, were requested and reviewed for completeness and proper authorization. This testing identified five additional instances of change request forms being approved by someone other than the two authorized individuals noted above. Further, one of these requests also appears to have been approved by the same individual that initiated the change request.

Failure to establish and to consistently apply proper program modification control procedures increases the risk that incorrect or unauthorized changes to critical applications could be placed into the live production environment and adversely affect system processing results for UPPS.

Program modification control procedures should be established and consistently applied in order to ensure that only appropriately authorized changes to critical applications are made and implemented within the production environment. These procedures should provide explicit instructions on the completion of program change request forms including a description of each field the agency is responsible for completing.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-PERS-74: The Personnel Cabinet Should Ensure That Formal Program Modification Control Procedures Are Consistently Followed To Properly Control Changes To The Uniform Personnel And Payroll System (Continued)****Recommendation**

We recommend that the Department of Personnel Administration expand the established program change procedures to include instructions detailing the process to complete each field of the program change request form. Adequate descriptions of each field on the change request form should be developed and properly distributed, and responsible employees should be notified as to the individuals authorized to approve the change requests. Authorization procedures established should ensure that an appropriate segregation of duties is maintained between the initiator of the change request and final agency approval. Further, modified programs should not be placed into the live production environment without the appropriate authorization.

Management's Response and Corrective Action Plan

The following issues were noted above regarding control procedures for programs changes and/or updates to UPPS for the Department for Personnel Administration:

- 1. Ten of seventeen requests were not appropriately approved,*
- 2. The Program Change Procedures did not include specific instructions for each fields found on the change request form (F001),*
- 3. Four of the ten inappropriately approved requests were signed as approved by the same individual initiating the change. This was also found in an additionally tested item, and*
- 4. Five instances found where change request forms were approved by someone other than the two authorized individuals noted in the Program Change Procedures.*

The Personnel Cabinet agrees with the issues noted and after review of the documents that were provided for audit purposes, our response is as follows:

- 1. Requests were found to lack a name in the Agency Contact Authorization field which should have been the Director of the Division of Employee Management (DEM) or in absence of that person, should have been the Commissioner of the Department for Personnel Administration.*

This oversight was due to the administrative assistant overlooking the field when processing the requests. Upon receiving completed requests for professional services, they are then forwarded to COT. Those generated and prepared from the Division of Employee Management should be

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-PERS-74: The Personnel Cabinet Should Ensure That Formal Program Modification Control Procedures Are Consistently Followed To Properly Control Changes To The Uniform Personnel And Payroll System (Continued)****Management's Response and Corrective Action Plan (Continued)**

trusted as approved by one of the two individuals listed above although we realize the need to be thorough in our documentation process.

This shall be corrected with a more detailed and thorough review of the F001 forms prior to submission to COT.

- 2. The Program Change Procedures currently outlining the routing process for submitting an F001 needs to include specific instructions for each field.*

*This shall be corrected with more thorough instructions which will be supplied to individuals requesting an F001 form and/or instructions on how to process a request. *Revised documents will be provided to Auditor of Public Accounts following this response.*

- 3. Requests were signed as accepted and approved by the same individual initiating the change.*

*Process guidelines and the F001 form will be revised to ensure proper segregation of duties are in place. They will reflect the appropriate roles and responsibilities of all individuals listed throughout the F001 form and involved in the request process. Specifically, the initiator of any F001 form will not approve the request and/or provide final sign-off that agency request has been completed accurately. *Revised documents detailing user responsibilities of the form will be provided subsequently to the Auditors Office.*

- 4. Request forms were approved by someone other than the two authorized individuals noted in the instructions and guidelines.*

This was a matter of limited space provided on the current F001 form. This shall be corrected with a revised F001 form that will allow more space to reflect the proper roles of those individuals involved in the F001 process.

** As noted above, due to the issues/concerns arising from this comment, we agree that the control procedures currently in place for changes being made to UPPS should be better defined and properly followed. These issues shall be corrected/clarified with more thorough instructions/procedures and a revised F001 form. Revised documents will outline the noted corrective measures and be distributed for use by agencies in completing F001 forms to effect program modifications to UPPS. This revised documentation will be provided to the Auditor's Office following this response.*

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-75: The Finance And Administration Cabinet Should Establish Controls Over Specific Purchase Order Documents To Ensure Contract Amounts Are Not Exceeded

Our FY 2007 audit of the Finance and Administration Cabinet (Finance) revealed the Enhanced Management Administrative and Reporting System (eMARS) Advantage Financial application did not have a functioning edit in place that would prohibit an end-user from creating payments against a contract requiring a Proof of Necessity (PON2) document that would exceed the contract amount on the PON2 document, in total or at the commodity line. Therefore, contract commodity lines or contract totals could be exceeded if controlled by a PON2 document.

Discussions revealed that the Finance was aware that the PON2 documents were not being properly controlled during FY 2007. In December 2006, an attempt was made by Finance to resolve this control weakness by creating records on the Document Control (DTOL) table within eMARS Advantage Financial that would establish tolerance levels on all payment request – commodity based documents (PRC) referencing a PON2 document. However, it was discovered that Finance did not configure this record correctly. Instead of adding an edit that would prohibit referenced line items from being overexpended, the system bypassed the edit. Further, the auditor found that payments could be made against a PON2 document on two types of payment documents: a payment request – commodity based (PRC) and an internal payment request – commodity (PRCI). Therefore, even if the controls within the DTOL table had been established correctly, those internal payments made on PRCI documents would not have been properly controlled.

Through a review of all PON2 documents issued or modified during FY 2007, the auditor found a total of 128 PON2 documents in exception:

- One hundred nineteen (119) PON2 documents were overexpended at the commodity level. The total of excess expenditures at the commodity level for all 119 PON2 documents was \$2,021,671.54. Forty-nine (49) of these PON2 documents had also been overexpended at the contract level.
- An additional nine (9) PON2 documents were overexpended at the commodity level at some point during FY 2007, but were subsequently corrected through modifications to the affected PON2 document. The collective overexpenditure for these documents was \$107,307.14. Six (6) of these PON2 documents were also overexpended at the contract level at some point during FY 2007.

Finally, the auditor discovered one PON2 document that had more PRC documents being referenced to it than were being reflected on the PON2 document. The eMARS vendor, CGI-AMS, determined that on the extra documents, the Accounting Line had a reference to the PON2 document, but showed that the Reference Type (RefType) was a “Memo.” According to CGI-AMS, if the “Memo” RefType is used on the Accounting Line of a payment document, then the payment will be attributed to the PON2 document for documentation purposes, however, there will be no liquidations postings or updates made to the referenced PON2 document.

FINANCIAL STATEMENT FINDINGS***Significant Deficiencies Relating to Internal Controls*****FINDING 07-FAC-75: The Finance And Administration Cabinet Should Establish Controls Over Specific Purchase Order Documents To Ensure Contract Amounts Are Not Exceeded (Continued)**

The lack of proper edits within eMARS has allowed payment documents to be processed through the system that overexpended PON2 documents at the commodity level by \$2,129,165.07. Further, when payments are not appropriately attributed to a contract, in the case of a “Memo” RefType, an increased potential exists for the intentional or unintentional overexpenditure of a contract.

Any department can create a PON2 document for personal service contracts, grants, and memorandums of agreement, which require review by the Government Contract Review Committee. These types of documents require a “Proof of Necessity” (PON) form to be completed and submitted to the Legislative Research Committee. This type of award is a contractual agreement between the State and a vendor to provide goods or services at pre-arranged prices and delivery dates. If changes in the contractual agreement are proposed that affect the pricing or delivery dates, a modification to the award should be created to allow the proper approvals to be applied.

Further, according to the Finance and Administration Cabinet Policy statement FAP 111-45-00 entitled Payment Documents, “An agency shall select the appropriate payment method for all goods and services...All payments referencing contracts and awards established in the State’s procurement system shall be made in the State’s procurement system and reference the appropriate award.”

Recommendation

We recommend that Finance work with CGI-AMS to establish an edit to prohibit all payment document types that could reference a PON2 document from processing expenditures that would exceed a PON2 contract amount in total or at the commodity or accounting line. In addition, Finance should look at the feasibility of adding an edit to processing that would prohibit a payment document from referencing a contract using the “Memo” Reference Type. Finally, Finance should reeducate all State departments concerning the proper use of the PON2 documents and the individual department’s responsibility for the overseeing of the contracts and associated expenditures.

FINANCIAL STATEMENT FINDINGS

Significant Deficiencies Relating to Internal Controls

FINDING 07-FAC-75: The Finance And Administration Cabinet Should Establish Controls Over Specific Purchase Order Documents To Ensure Contract Amounts Are Not Exceeded (Continued)

Management's Response and Corrective Action Plan

Tolerance edits have been configured in eMARS to prevent all types of "referencing" Payment Request documents (this would include PRC's, PRC2's, PRCI's, PRM's, PRMI's and PRN's) from over-expending all types of "referenced" Purchase Order documents (this would include PO's, PO2's, PON2's, DO's, DO2's, CT's, CT2's, CTT1's and CTT2's). These tolerance edits are enforced at the most granular level (the Accounting Line level) and prevent the "referenced" accounting line from being exceeded by either an individual "referencing" accounting line or the sum of all "referencing" accounting lines.

To accomplish this, the Commonwealth created an entry on the System Tolerance (STOL) table in eMARS to establish a "Reject Overage Tolerance" amount = \$.01 between "referencing" documents with a Doc Type = PR and "referenced" documents with a Doc Type = PO. When the "Reject Overage Tolerance" amount has been reached or exceeded on a PO Type document accounting line by a "referencing" accounting line on a PR Type document, eMARS will issue a 'hard' error message preventing an over-payment.

Please note, these tolerance edits are not performed when the "referencing" accounting line has a Reference Type = Memo. The "Memo" reference in eMARS is not an accounting based reference and thus does not perform any liquidation of the "referenced" accounting line. Therefore, a PR Type document with a "Memo" reference is essentially the same as a standalone payment. We will consider our options such as an event type for a cloned payment document or a workflow rule to intercept documents without a real reference, although this doesn't preclude the possible use of a standalone PRC or GAX payment to the vendor outside the contract.

We have reviewed the PON2 documents showing an overspent in FY 2007. After speaking with departmental contract administrators, we found that most of the conditions were known and have been rectified. In many cases there were overpayments and the vendors returned the payments. Several payments referenced the wrong contract creating an over and under spent condition across two contracts or contract years. We are following up on any conditions that haven't been settled. Further, we will publish a newsletter article on this subject and make sure it is covered in the class material for personal service contracts.

APPENDIX

COMMONWEALTH OF KENTUCKY
APPENDIX
FOR THE YEAR ENDED JUNE 30, 2007

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) 573-0050 or gregory.giesler@auditor.ky.gov. If copies of the CAFR for FY 07 are required, please contact Jonathan Miller, Finance and Administration Cabinet Secretary, at (502) 564-4240.

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
501 High Street
Room 808
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

**COMMONWEALTH OF KENTUCKY
APPENDIX
FOR THE YEAR ENDED JUNE 30, 2007
(Continued)**

Kentucky Teachers' Retirement System
479 Versailles Road
Frankfort, Kentucky 40601

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

**COMMONWEALTH OF KENTUCKY
APPENDIX
FOR THE YEAR ENDED JUNE 30, 2007
(Continued)**

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

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

Office of Public Employees Health Insurance
State Office Building, 2nd Floor
501 High Street
Frankfort, KY 40601

**COMMONWEALTH OF KENTUCKY
APPENDIX
FOR THE YEAR ENDED JUNE 30, 2007
(Continued)**

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

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

World Games 2010 Foundation, Inc.
2010 World Games Way
Lexington, Kentucky 40511

