

**LETTER FROM THE AUDITOR OF PUBLIC ACCOUNTS
KENTUCKY REVENUE CABINET**

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

For the Year Ended June 30, 2003



**CRIT LUALLEN
AUDITOR OF PUBLIC ACCOUNTS
www.kyauditor.net**

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

TABLE OF CONTENTS

MANAGEMENT LETTER.....	1
LIST OF ABBREVIATIONS/ACRONYMS.....	3
FINANCIAL STATEMENT FINDINGS	5
<i>Reportable Conditions Relating to Internal Controls and/or Reportable Instances of Noncompliance</i>	<i>5</i>
FINDING 03-REV-1: The Kentucky Revenue Cabinet Should Improve Communication Between Divisions To Ensure Taxpayer Information Is Protected	5
FINDING 03-REV-2: The Kentucky Revenue Cabinet Should Update Its Computer Systems To Remove System Limitations Affecting Accuracy And Reliability Of Reporting	7
FINDING 03-REV-3: The Revenue Cabinet Should Strengthen The Security Surrounding Administrator Accounts	9
FINDING 03-REV-4: The Revenue Cabinet Should Ensure All User Accounts On Its Agency Machines Are Necessary.....	11
FINDING 03-REV-5: The Kentucky Revenue Cabinet Should Develop A System For Reconciling Critical Information And Investigating Any Discrepancies	12
<i>Other Matters Relating to Internal Controls and/or Instances of Noncompliance</i>	<i>13</i>
FINDING 03-REV-6: The Kentucky Revenue Cabinet Should Develop Computer Applications To Streamline The Crosschecking Of Motor Fuels Dealer Reports	13
FINDING 03-REV-7: The Kentucky Revenue Cabinet Should Document The Motor Vehicle Usage Recap Reports Receipt Date And Impose Fines For Late Reports As Allowed By KRS 138.464.....	14
FINDING 03-REV-8: The Revenue Cabinet Should Ensure That Security Information Leakage Concerning Agency Devices Is Minimized	15
FINDING 03-REV-9: The Kentucky Revenue Cabinet Password Policy Should Be Consistently Applied To All Local Area Network Machines	17
FINDING 03-REV-10: The Revenue Cabinet Should Ensure That All Open Ports On Agency Machines Have A Business-Related Purpose	19
FINDING 03-REV-11: Motor Vehicle Usage Receipts Should Be Timely And Properly Deposited With The State Treasurer	21
FINDING 03-REV-12: The Kentucky Revenue Cabinet Should Ensure Mathematical Accuracy And Completeness Of Key Information	23
FINDING 03-REV-13: The Division Of Property Valuation Education And Research Branch Should Reconcile Receipts To MARS And Ensure Checks Are Timely Deposited.....	24
SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS.....	26



C R I T L U A L L E N
A U D I T O R O F P U B L I C A C C O U N T S

Robbie Rudolph, Secretary, Finance and Administration Cabinet
Kentucky Revenue Cabinet

MANAGEMENT LETTER

Pursuant to KRS 43.090 (1), which states, "Immediately upon completion of each audit and investigation, except those provided for in KRS 43.070, the Auditor shall prepare a report of his findings and recommendations." We are providing this letter to the Kentucky Revenue Cabinet to comply with KRS 43.090.

This letter presents the results of the work performed at the Kentucky Revenue Cabinet, as part of our annual audit of the Commonwealth of Kentucky's financial statements.

In planning and performing our audit of the basic financial statements of the Commonwealth for the year ended June 30, 2003, we considered the Kentucky Revenue Cabinet's internal control in order to determine our auditing procedures for the purpose of expressing an opinion on the financial statements and not to provide assurance on internal control. However, we noted certain matters involving the internal control and its operation that we considered to be reportable conditions under standards established by the American Institute of Certified Public Accountants. Reportable conditions involve matters coming to our attention relating to significant deficiencies in the design or operation of internal control that, in our judgment, could adversely affect the Kentucky Revenue Cabinet's ability to record, process, summarize, and report financial data consistent with the assertions of management in the financial statements.

Our consideration of internal control was for the limited purpose described in the preceding paragraph and would not necessarily disclose all matters that might be reportable conditions. In addition, because of inherent limitations in internal control, errors or fraud may occur and not be detected by such controls.

As part of our audit of the Commonwealth's basic financial statements, we also performed tests of the Kentucky Revenue Cabinet's compliance with certain provisions of laws, regulations, contracts, and grants, noncompliance with which could have a direct and material effect on the determination of financial statement amounts. The results of those tests disclosed no instances of noncompliance that are required to be reported under *Government Auditing Standards*.



Robbie Rudolph, Secretary, Finance and Administration Cabinet
Kentucky Revenue Cabinet

Some findings are Other Matters that we have included in this letter to communicate with management in accordance with auditing standards generally accepted in the United States of America and *Government Auditing Standards*.

Included in this letter are the following:

- ◆ Acronym List
- ◆ Findings and Recommendations (Reportable Conditions and Other Matters)
- ◆ Summary Schedule of Prior Year Audit Findings

We have issued our Statewide Single Audit of the Commonwealth of Kentucky that contains the Kentucky Revenue Cabinet's findings, as well as those of other agencies of the Commonwealth. This report can be viewed on our website at www.kyauditor.net.

This letter is intended solely for the information and use of management 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,



Crit Luallen
Auditor of Public Accounts

LIST OF ABBREVIATIONS/ACRONYMS

ACH	Automated Clearinghouse
APA	Auditor of Public Accounts
BDC	Backup Domain Controllers
Commonwealth	Commonwealth of Kentucky
CR	Cash Receipt
EFT	Electronic Fund Transfers
ERB	Education and Research Branch
FTP	File Transfer Protocol
FY	Fiscal Year
FYE	Fiscal Year End
GOT	Governor's Office for Technology
ID	Identification
IT	Information Technology
KRC	Kentucky Revenue Cabinet
KRS	Kentucky Revised Statutes
LAN	Local Area Network
LSA	Local Security Authority
MARS	Management Administrative Reporting System
MFD	Multi Function Device
MFE	Modernized Front End
MVU	Motor Vehicle Usage
N/A	Not Applicable
NT	Network
OS	Operating System
PDC	Primary Domain Controller
PVA	Property Valuation Administrator
REV	Kentucky Revenue Cabinet
Revenue	Kentucky Revenue Cabinet
SMTP	Simple Mail Transfer Protocol
SQL	Structured Query Language
VPN	Virtual Private Network

THIS PAGE LEFT BLANK INTENTIONALLY

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 03-REV-1: The Kentucky Revenue Cabinet Should Improve
Communication Between Divisions To Ensure Taxpayer Information Is Protected**

During the Revenue Cabinet (Revenue) audit, we noted problems in the refunds, accounts receivable, and receipts audit sections related to missing or difficult to locate tax returns. While searching for returns, we noted problems with the communication between the tax divisions and central files regarding tracking of tax returns transferred to central files.

REFUNDS AUDIT SECTION

We tested controls over refunds and noted weaknesses in Revenue's ability to retain and locate corporate tax returns to comply with confidentiality and record retention laws.

We tested 42 corporate tax refunds, and Revenue failed to provide a tax return for one (1) corporate taxpayer of \$381,004. Initially, 12 tax returns were missing, but Revenue located 11 of the returns over a one-month period. We were able to view the last return on Revenue's corporate coding system; however, we were not able to determine if the return was reviewed.

ACCOUNTS RECEIVABLE AUDIT SECTION

We were unable to locate one (1) corporate license tax return. The return amount due per the Compliance and Receivable System was \$440,909.

RECEIPTS AUDIT SECTION

We were unable to locate three (3) Motor Fuels Dealer Reports. The return amount paid per MIXERS was \$32,156.

When tax returns are missing, we cannot determine if the returns were lost, stolen, destroyed, or ever received. Thus, missing documentation causes us to question the legitimacy of a transaction, particularly when a refund is issued. Tax returns are the most persuasive evidence available to support that refunds are legitimate, properly recorded, and classified within the financial statements.

A disorganized filing system compromises Revenue's ability to properly safeguard taxpayer information, as required by KRS 131.081 and 131.185. The benefits of retaining tax records are lost, if the documentation cannot be easily located and retrieved at the central filing repository.

KRS 131.081 (15) states, "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 . . ."

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 03-REV-1: The Kentucky Revenue Cabinet Should Improve
Communication Between Divisions To Ensure Taxpayer Information Is Protected
(Continued)**

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 . . ."

Good internal controls dictate tax returns be maintained in a manner that ensures compliance with confidentiality and record retention laws and ensures accountability to Kentucky taxpayers.

Recommendation

Revenue should ensure confidential taxpayer information is protected and preserved as required by statute. Revenue should consider improving communication between the tax divisions and the central files division. For example, one person from each division could keep track of the batches of tax returns being shipped to central files. Also, when searching for a return, the appropriate division should be notified that the return is not at central files, and a division employee should follow up with central files employees to make sure the return is located.

Management's Response and Corrective Action Plan

Revenue agrees with the auditor's findings that additional controls should be implemented to ensure that confidential taxpayer information is protected and preserved, as required by statute.

As a result, Revenue has designated the Central Files Section as a restricted area, which requires an employee to have special permission in order to gain access.

The Division of Revenue Operations has already implemented tracking logs to document where a return was sent after processing. Similar tracking logs will also be implemented for each division to improve communication between the divisions and the Central Files Section.

Additionally, Revenue has allocated four (4) interim resources to the Central Files Section to assist in eliminating backlogs, and to help with the purging of records that have met the required retention period.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 03-REV-2: The Kentucky Revenue Cabinet Should Update Its Computer Systems To Remove System Limitations Affecting Accuracy And Reliability Of Reporting**

We identified and tested 13 accelerated sales tax receipts totaling \$211,488,106. We noted the Revenue sales tax database does not process payments that equal or exceed \$1,000,000; thus, a single transaction exceeding \$1,000,000 will show up on the Revenue mainframe report as 999,999 in a succession of lines with the bottom line total as the balancing amount. Data that is processed in this manner is difficult for end users to understand.

In FY 01, this system limitation resulted in two (2) accelerated payments, which overstated receipts in Revenue's mainframe system by \$7.5 million. While no errors were found in testing this FY, the recording process that caused the errors in FY 01 has not been corrected and has the potential to cause revenues to be incorrectly recorded in the future.

While FY 03 financial statement information was not affected as a result of these weaknesses, the system limitations could affect the accuracy and reliability of the Revenue reporting system. Tax information that is not captured exactly as reported on the tax return makes it difficult to determine that receipts were recorded at the proper amounts and increases the likelihood that errors will go undetected by Revenue.

Good internal controls dictate that receipts should be properly posted to computer records from supporting documentation, and all data processed by significant systems should be reviewed to determine accuracy and completeness.

Recommendation

We recommend Revenue take the following actions to correct these weaknesses:

- Update the Revenue mainframe system to process tax payments that equal or exceed \$1,000,000; and,
- Complete update of Modernized Front End (MFE) to process all accelerated sales tax returns; this would reduce manual processing and should increase mathematical accuracy, which would increase the reliability of the mainframe data. If this is not feasible, due to the magnitude of the tax payments involved, all accelerated sales tax returns should have a secondary level of review that includes verifying, editing, and approving all adjustments.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 03-REV-2: The Kentucky Revenue Cabinet Should Update Its Computer Systems To Remove System Limitations Affecting Accuracy And Reliability Of Reporting (Continued)**

Management's Response and Corrective Action Plan

Revenue agrees that updating the mainframe system to accommodate payment transactions greater than \$1,000,000 would provide more concise, accurate, and efficient information for end users to interpret and understand. While the current system may be more difficult to interpret and understand, payments transactions are represented in their entirety. In addition, as noted in this audit comment, no errors were identified while testing the system for FY 2003. Given the current budget constraints and plans to build a new system for compliance to the national Streamline Sales Tax initiative, updating the current mainframe system at this time may not be a priority or the best use of resources.

Revenue also agrees that putting Accelerated Sales Tax returns on the MFE would be a more efficient and effective processing tool than the current environment. However, given the current budget constraints, plans for a new national Streamline Sales Tax initiative, a system rewrite, and possible legislative changes, this change will not likely occur during FY '04.

It is recognized that whenever a dollar amount exceeding a single payment of over \$1,000,000 is received, the Sales and Use Tax system does not display that record as one transaction. The Sales and Use Tax system does, however, contain the correct amount and this information is reflected in receipts. It is also recognized that the Sales and Use Tax system does not always effectively handle accelerated payments. These payments are worked manually by Revenue employees. It has been determined that the most effective approach is to build controls within the new Sales and Use Tax system, which is being designed to accommodate the needs of the national Streamline Sales Tax Agreement. This new system will most likely be complete within FYE [Fiscal Year End] 06.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 03-REV-3: The Revenue Cabinet Should Strengthen The Security Surrounding Administrator Accounts**

During the security vulnerability testing of Revenue machines, the auditor found several instances of lax security over administrator accounts, resulting in potential intrusion vulnerabilities. These instances vary in severity; combined, they demonstrate that the Revenue local area network (LAN) was vulnerable during the year under review.

We examined 43 Revenue machines and found three (3) machines where the administrator accounts had not been renamed or disabled. Since these accounts cannot be locked out if the account is not renamed, these machines could be vulnerable to a brute force attack. Two (2) of these machines were included in our prior year report comment for the same issue. Further, six (6) machines were noted with administrator level accounts that had been adequately renamed; however, the passwords had not been changed frequently to comply with agency password policy. The passwords on these machines had not been changed for periods ranging from 161 to 433 days. One (1) of these machines had been noted for the same issue in our prior year report comment.

The auditor also examined all Revenue controlled machines for specific applications running on port 1433 and found that two (2) of these machines allowed the auditor to gain "Master" access through Structured Query Language (SQL) using a default administrator logon. This type of access will provide an unauthorized user with complete access to the application. Further, the user would be granted local system account rights to the machine on which the application resides. The auditor initiated an SQL Tool on both of these machines to view the available drives on each system and view the respective directories and files. The auditor noted an electronic file of income tax transactions on one (1) of these machines, including taxpayer attributes of names, addresses, and social security numbers. Access to this confidential data was available to unauthorized users during the audit period. This issue had been resolved at the time of our follow-up assessment in October 2003. However, the vulnerability existed during portions of FY 03.

Administrator accounts are very powerful and can allow full access to the system or application. Therefore, these accounts should be scrutinized to ensure they are adequately secured. At a minimum, the passwords for these accounts should be changed from the system defaults. Further, some administrator accounts can be renamed to help obscure them from an unauthorized user's view. Finally, all administrator passwords should be changed in compliance with established password policies.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 03-REV-3: The Revenue Cabinet Should Strengthen The Security Surrounding Administrator Accounts (Continued)**

Recommendation

We recommend that Revenue review all machines to ensure the administrator accounts have been changed from the default naming conventions and have a password established that is not a default password. This should include a review of all SQL application administrator passwords. Finally, Revenue should ensure all administrator accounts adhere to the established password policies by ensuring all administrator level passwords are changed at the established expiration interval.

Management's Response and Corrective Action Plan

KRC would like to document that the vulnerabilities discovered by APA were only uncovered after gaining internal access to the KRC network. KRC has protected its network resources from external attacks through firewall technology.

All servers were checked to make sure that all default administrator and guest IDs have been renamed and that default passwords have been changed. All corrections were completed by December 17. The local administrator account that was found on a workstation was appropriately removed from this machine on 12/8/03.

KRC policy is to change the local administrator account passwords on both workstations and servers every 30 days. Our review shows that this policy has not been followed. We have readdressed this issue with our Network Administrators and the Network Support Manager will monitor to ensure this policy is being followed in the future. We are also looking into tools or scripts that would allow us to quickly change local administrative passwords throughout the domain.

FINANCIAL STATEMENT FINDINGS

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

FINDING 03-REV-4: The Revenue Cabinet Should Ensure All User Accounts On Its Agency Machines Are Necessary

During the security vulnerability testing of Revenue machines, the auditor discovered several instances where services were established without adequate user account control.

The auditor attempted a remote logon to machines with known applications accessible through a File Transfer Protocol (FTP) session. The auditor was able to create an FTP session through port 21 on five (5) machines with the anonymous logins. These machines allowed connections without having to provide any type of user ID or password. One (1) of these machines was a web server, and the FTP service allowed anonymous access to all directories and files on the web server. However, no sensitive tax information was viewable on this web server through this FTP service.

Intruders often use inactive accounts to break into a network. If a user account has not been utilized for some time, the account should be disabled until it is needed. This minimizes the possibility that an unauthorized user will use the account. If an account is not going to be reinstated, then it should be deleted. Further, default administrator, guest, and anonymous accounts in operating systems and applications are some of the first accounts that an intruder will attempt to use. They should be assigned strong passwords or, where possible, renamed or removed immediately after installation.

Recommendation

We recommend Revenue ensure all machines with FTP services running on them restrict access to default, anonymous, or guest logons as necessary.

Management's Response and Corrective Action Plan

KRC would like to document that the vulnerabilities discovered by APA were only uncovered after gaining internal access to the KRC network. KRC has protected its network resources from external attacks through firewall technology.

Revenue staff reviewed all instances of FTP services and has ensured that only those that require it for a business need have it enabled. We have also ensured that all of these servers have anonymous access disabled. One server mentioned is a server not in the Revenue domain. This server is within the GOT domain and Revenue forms are stored there for citizens to FTP from the web. It is our understanding that anonymous has been enabled on that server which is administered by GOT.

Revenue also reviewed machines that were running SMTP and determined that two of the four instances could be disabled. That was completed in early December.

Revenue has reviewed all servers currently installed and renamed administrator and guest accounts. We have restricted anonymous wherever possible.

FINANCIAL STATEMENT FINDINGS***Reportable Conditions Relating to Internal Controls and/or
Reportable Instances of Noncompliance*****FINDING 03-REV-5: The Kentucky Revenue Cabinet Should Develop A System For Reconciling Critical Information And Investigating Any Discrepancies**

Revenue does not have a system in place to input or reconcile critical information to the mainframe system; this has been reported during prior audits and continues to be a problem. Due to the lack of reconciliation, Revenue cannot ensure that amounts reported remitted are correct. While Revenue has had a reconciliation project underway for several years, the system was not operational during the FY 03 audit. It is expected that the project will be fully operational by the end of FY 04.

Failure to reconcile increases the chance that fraudulent reporting would go undetected by Revenue. By not reconciling this information, the Commonwealth may not be receiving the correct amount of income tax due.

Revenue should have adequate systems in place to reasonably ensure that all taxes due the Commonwealth are collected, and taxpayers are reporting key information in compliance with Commonwealth laws. Reconciling is a key component to determining taxpayer compliance and should be part of Revenue's taxpayer compliance programs.

Recommendation

Revenue should develop a system for reconciling critical information and investigate any discrepancies. The proposed reconciliation system will allow Revenue to perform several different types of reconciliations.

Management's Response and Corrective Action Plan

The reconciliation system is now in place and one of the critical reconciliations recommended is currently being performed. In addition, the second phase of the reconciliation system, which will allow Revenue to perform other types of reconciliations, is scheduled to be completed in Fiscal Year 05.

FINANCIAL STATEMENT FINDINGS

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

FINDING 03-REV-6: The Kentucky Revenue Cabinet Should Develop Computer Applications To Streamline The Crosschecking Of Motor Fuels Dealer Reports

Revenue's motor fuels tax section has a significant backlog in crosschecking motor fuels dealer reports. Reports are filed with the motor fuels tax section by fuel dealers and transporters (also known as common carriers). The transporter's report of motor fuel delivered is filed each month by transporters, which includes details that list every consignee to whom motor fuel was delivered, type of fuel, number of gallons, etc. The transporter must provide one duplicate of this report so that Revenue can associate it with the appropriate monthly dealer's reports. The transporter reports are tracked to ensure each licensee is filing a monthly report and that the report is timely.

During the FY 03 audit, we tested 53 reports and noted 44 instances where Motor Fuels Dealer Reports were not crosschecked.

In the prior year, Revenue agreed with our finding and stated in their corrective action plan that additional staff had been hired/assigned to reduce the backlog. These efforts have not significantly reduced the backlog.

When dealer reports are not crosschecked, there may be errors or omissions that are not detected in a timely manner. Good internal controls dictate that all available resources are used for ensuring the accuracy of motor fuels reports.

Recommendation

Revenue should consider developing new computer applications that will streamline the crosschecking of dealer reports, such as creating a database that would allow the dealer reports to be crosschecked electronically. Until such a system can be implemented, Revenue should redesign procedures to better use existing resources. One change to consider is using audit-sampling methods to select dealer reports to be crosschecked.

Management's Response and Corrective Action Plan

Revenue concurs with the auditor's findings on the crosschecking of motor fuels dealer reports. Revenue's Motor Fuels Tax Compliance Section has examined the possibility of electronic crosschecking and will expand investigation into this option. The section has also attempted statistical sampling and found its application difficult based on the numerous transaction types and the different points of taxation created by our border states. However, new crosschecking methods will continue to be investigated. Material inventory reduction is anticipated in the upcoming fiscal year. This reduction will depend on the retention of the current compliment of trained employees. Inventory levels are now below 29,000 as compared to 33,000 at the time of the audit.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Instances of Noncompliance*****FINDING 03-REV-7: The Kentucky Revenue Cabinet Should Document The Motor Vehicle Usage Recap Reports Receipt Date And Impose Fines For Late Reports As Allowed By KRS 138.464**

Revenue oversees the collection of motor vehicle usage tax. County clerks are required to submit weekly motor vehicle usage tax recapitulation reports within 15 days per KRS 138.464, which subjects the clerk to penalties for reports not filed timely. Revenue date stamps motor vehicle usage tax recapitulation reports received to document the receipt date of these time-sensitive reports.

We tested 25 motor vehicle usage tax recapitulation reports and noted 14 recap reports were not date stamped when received and envelopes were not maintained to assist in determining the receipt date. Documenting receipt date is necessary to enforce KRS 138.464, which provides penalties for late-filed reports.

Without a date stamp, there is no verifiable documentation of the receipt date to support the imposition of fines for late-filed reports; as such, there is no support for penalizing county clerks that have not filed their recapitulation reports in a timely manner.

Good internal control dictate that documents with specified deadlines are date stamped to provide verifiable documentation of the receipt date.

Recommendation

We recommend Revenue ensure recap reports are date stamped or envelopes are maintained to provided documentation of the receipt date so that KRS 138.464 can be enforced.

Management's Response and Corrective Action Plan

Revenue agrees with the auditor's recommendation and has procedures in place to keep the envelope with the "recap" report, or stamp the report itself if the date on the envelope is illegible. Revenue has re-enforced the need for following this procedure to staff involved in the daily performance of this duty.

FINANCIAL STATEMENT FINDINGS

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

FINDING 03-REV-8: The Revenue Cabinet Should Ensure That Security Information Leakage Concerning Agency Devices Is Minimized

As noted in the previous audit, the Revenue Cabinet did not restrict critical information divulged by their network machines. During the review of the Revenue LAN security for FY 03, we discovered several instances where machines within the LAN provided information to anonymous users that could potentially help an intruder with developing details for an attack.

Using standard scanning tools, we examined all computer device names and other remarks located within the Revenue domains. The naming convention of servers was not sufficiently ambiguous to disguise the function of 15 machines. Further, remarks available from two (2) machines provided excessive user information.

We also ran other vulnerability assessment tools twice during the fiscal year on 43 machines within the Revenue domains to determine if they would return information on Local Security Authority (LSA), Password Policies, Valid User, Group, or Share Lists.

The following table depicts the number of machines that would provide this information.

Type of Information	Number of machines	Percentage of 43 machines providing information
LSA	36	83.7%
Password Policies	8	16.3%
Valid User List	8	16.3%
Valid Group List	1	2.3%
Valid Share List	1	2.3%

Two of these machines had been noted with the same issues in our prior year audit report.

The amount of information provided to an anonymous user has decreased from the prior audit period. However, this type of information should be restricted because it would be considered useful to a hacker.

An agency's domain information that is accessible to the world at large through inquiry tools should be kept at a minimum. Agencies should ensure that information such as location, accounts associated with the machine, data residing on the machine, and the machine's 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, can use naming conventions that obscure the purpose of machines, and can provide no comments on machine activity.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Instances of Noncompliance*****FINDING 03-REV-8: The Revenue Cabinet Should Ensure That Security Information Leakage Concerning Agency Devices Is Minimized (Continued)**

Recommendation

We recommend that Revenue restrict the information that is being provided by its LAN machines to anonymous users. First, the naming convention for the noted machines should be altered to make their purpose more ambiguous and less identifiable to an unauthorized user and any unnecessary comments associated with the servers should be removed. Second, boundaries should be placed on what types of responses machines make available based on certain inquiries.

Management's Response and Corrective Action Plan

KRC would like to document that the vulnerabilities discovered by APA were only uncovered after gaining internal access to the KRC network. KRC has protected its network resources from external attacks through firewall technology.

As we replace or rebuild servers, KRC has been renaming them with non-descriptive names and restricting comments so as to limit information available to unauthorized users. Approximately 75% of KRC servers have been named with ambiguous names to disguise their function. KRC reviewed all servers and corrected any that had inadvertently been built with anonymous access enabled. As with other agencies using GOT mail services, our domain controller can not have anonymous access restricted because that would interfere with synchronization with the Enterprise Messaging System domain at GOT. We hope that our planned move to Active Directory and GOT's upgrade to Exchange 2003 will eliminate this issue. In the past, KRC has not restricted anonymous access on desktops but has now added the relative patch to the current desktop image so that inquiries will not provide information on password policies, user, group or share lists. KRC is in the process of building a script to patch all installed desktops on the KRC network.

FINANCIAL STATEMENT FINDINGS

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

FINDING 03-REV-9: The Kentucky Revenue Cabinet Password Policy Should Be Consistently Applied To All Local Area Network Machines

As was noted in the prior audit, password policies established on certain critical Revenue machines did not adhere to the agency password policies. During the FY 2003 audit, we reviewed the password policies of all Primary Domain Controllers (PDC), Backup Domain Controllers (BDC), SQL, and a sample of Network (NT) machines within the Revenue domains, for a total of 43 machines. We were able to obtain the password policies for 8 of these machines.

We found that the password policies established on five (5) machines did not agree to the Governor's Office for Technology (GOT) standard password policy adopted by the agency. One of these machines had also been noted with the same issue in our prior audit report. See the table below for a summary of our findings.

Security Measure	Standard	Number of machines not in compliance with policy	Percentage of 8 machines not in compliance with policy
Minimum Length	8 characters – GOT	4 – None	50.0%
Minimum Age	1 day – GOT	5 – None	62.5%
Maximum Age	31 days – GOT	4 – 42 days	50.0%
Lockout Threshold	3 attempts – GOT	4 – None	50.0%

Some improvements were made after the FY 02 audit concerning the implementation of password policies. Revenue had changed the password policy attributes for all but one of the eleven machines noted in the prior year report comment.

To help ensure the security of a network, it is necessary for a strong password policy to be developed and implemented on all machines within the network. If machines within a network are not sufficiently secured, the network could be compromised through one of these more vulnerable paths.

Recommendation

We recommend that Revenue review all machines within their agency-owned domains to ensure that the password policy established on the machines complies with the GOT standard password policy. Further, procedures should be established to periodically review these settings for all Revenue machines to prevent reoccurrence of this issue.

FINANCIAL STATEMENT FINDINGS*Other Matters Relating to Internal Controls and/or Instances of Noncompliance***FINDING 03-REV-9: The Kentucky Revenue Cabinet Password Policy Should Be Consistently Applied To All Local Area Network Machines (Continued)**

Management's Response and Corrective Action Plan

KRC would like to document that the vulnerabilities discovered by APA were only uncovered after gaining internal access to the KRC network. KRC has protected its network resources from external attacks through firewall technology

KRC has reviewed the password policy on all agency servers and made corrections so that they all adhere to the standard password policy. We have ensured that the password policy has been included as part of our new "Server Build Checklist" for the network administrator staff so that new servers will be built correctly. Two of the eight machines reported by the APA are agency workstations and KRC had not previously applied password policies to workstations. We now have added the standard password policy to the desktop image for our workstations and, as workstations are replaced or rebuilt, the standard password policy will be proliferated across all workstations until all are protected by the password policy.

FINANCIAL STATEMENT FINDINGS

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

FINDING 03-REV-10: The Revenue Cabinet Should Ensure That All Open Ports On Agency Machines Have A Business-Related Purpose

During the security vulnerability testing of Revenue machines, the auditor determined that there were several machines with ports open that may not have a specific business-related purpose. Additionally, we noted several web service vulnerabilities that indicate updated patches are needed. Due to the large number of issues, the auditor has grouped the findings below by port number and application.

Port 80 – Hypertext Transfer Protocol

First, there were ten machines with port 80 open that would not display the website. Five of these machines had also been noted in a prior audit report comment with this same issue. When no default page or restricted logon is required, normally this shows that there is no application/web service running at the port. Second, eleven websites provided configuration information of printers or print servers. This situation allows too much access to an unauthorized or anonymous user.

Third, seven machines provided information from a Nortel Networks Interface for an Extranet Switch, allowing administrative access to these machines through any internet browser. Finally, six machines provided a Hewlett Packard web interface, but the full images for these web pages are not viewable.

Port 443 – Hypertext Transfer Protocol over Secure Socket Layer

Four servers were found with port 443 open but would not display a website. One of these machines had been noted with this issue in the prior audit report comment. None of the ports appear to have an application/web service running on them.

Port 8080 – World Wide Web – Proxy

One machine was found with port 8080 open, but the website was not accessible.

Other Ports

There were six machines in which the trojan port 1033 (Netspy) was listed as open. Another trojan port 1042 (Bla1.1) was open on two machines and one machine has port 6776 (subseven) open.

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. Finally, proper maintenance requires that software patches be installed promptly on all servers to strengthen security.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Instances of Noncompliance*****FINDING 03-REV-10: The Revenue Cabinet Should Ensure That All Open Ports On Agency Machines Have A Business-Related Purpose (Continued)**

Recommendation

We recommend that Revenue perform a review of all open ports on the machines discussed in this comment. If there is not a specific business-related purpose requiring a port to be open, then that port should be closed. Further, we recommend that Revenue begin a periodic review of open ports on all machines owned by the agency to ensure necessity. Revenue should also ensure updated patches are installed on all machines under their control.

Management's Response and Corrective Action Plan

KRC would like to document that the vulnerabilities discovered by APA were only uncovered after gaining internal access to the KRC network. KRC has protected its network resources from external attacks through firewall technology.

Revenue reviewed all open ports and has determined that only a few of the cited instances could be closed. Port 80 must be enabled on some printers and multi-function devices for printer management and MFD scanning capability. When possible, the web sites are disabled and most require a specific userid and password in order to update the device. KRC requests that when these same instances are found in future audits, that a note be made in the report that these ports have been previously justified by KRC as necessary for a specific business function.

KRC continues to consolidate server applications in order to limit the number of web servers on the network. Revenue has ensured that all patches have been made to their web servers and staff are testing new patches relative to the Revenue environment and applying them to network devices as they become available.

All Revenue locations are protected by Nortel Contivity VPN switches that are administered by GOT. The web interface is open so that they may manage them remotely but is userid and password protected. All further questions about these devices should be directed to GOT.

KRC has worked with Microsoft and cannot find a way to close port 443 on NT 4.0 servers. We have been more successful when upgrading application servers to Win 2000 OS. Revenue has researched the possible use of mid-range ports from 1024-5000 and has determined that the Windows OS does some dynamic allocations within this range.

FINANCIAL STATEMENT FINDINGS

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

FINDING 03-REV-11: Motor Vehicle Usage Receipts Should Be Timely And Properly Deposited With The State Treasurer

Revenue receives Motor Vehicle Usage receipts from the various county clerks via pass-through accounts. The county clerks deposit the state's portion of receipts in the account and then either calls in the deposit amount to trigger the transfer to the State Treasurer or Revenue writes a check to the State Treasurer from the account on a weekly basis.

During tests of Motor Vehicle Usage receipts, we found numerous instances where receipts had not been timely or properly deposited with the State Treasurer. Examples of the problems we found were:

- ACH counties failing to make required daily call-ins of deposits totaling \$158,341;
- errors in call-in amounts totaling \$30,332 that were not corrected even months later;
- a call-in for \$6,016 made without corresponding deposit;
- one pass-through account was overdrawn, due to a call-in error, resulting in a Non-Sufficient Funds charge to that account.

Revenue employees had documented these errors in their monthly reconciliations and carried them forward to subsequent reconciliations. Yet, at the time of testing, employees had not taken any action to correct these problems with the pass through accounts.

While KRS 138.464 allows Revenue to impose penalties for failure to make required deposits or transfers, Revenue had not imposed penalties for any of the instances where the proper amounts were not deposited or transferred timely. The Commonwealth loses potential interest when monies are not deposited in the State Treasury timely.

By not imposing penalties, Revenue has not provided the counties with an incentive to make timely and accurate deposits and transfer of state funds to the State Treasurer. Valuable employee time is spent tracking the errors in deposits over extended periods, rather than correcting the problems and imposing penalties.

KRS 138.464 states,

The clerk shall deposit motor vehicle usage tax collections not later than the next business day following receipt in a Commonwealth of Kentucky, Revenue Cabinet account in a bank designated as a depository for state funds. The clerk may be required to then cause the funds to be transferred from the local depository bank to the State Treasury in whatever manner and at times prescribed by the secretary of the Revenue Cabinet or his designee . . . Failure to deposit or, if required, transfer collections as required above shall subject the clerk to a penalty of two and one-half percent (2.5%) of the amount not deposited or, if required, not transferred as required above.”

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Instances of Noncompliance*****FINDING 03-REV-11: Motor Vehicle Usage Receipts Should Be Timely And Properly Deposited With The State Treasurer (Continued)**

KRS 41.070 states receipts should be deposited in the "most prompt and cost-efficient manner available."

Recommendation

Revenue should immediately correct known errors and implement procedures to ensure future errors are dealt with timely. Revenue should also consider assessing penalties as allowed by KRS 138.464.

In addition, Revenue should consider changing procedures to reduce the man hours required to track 120 separate checking accounts. For instance, switching from temporary deposit accounts to daily Electronic Fund Transfers (EFTs) from clerk accounts.

Management's Response and Corrective Action Plan

Revenue agrees with the auditor's recommendation and the known errors have been corrected. Revenue staff routinely works with Clerks to correct errors as soon as possible. Procedures and guidelines will be reinforced with appropriate employees. Managers will implement a quality assurance program to ensure errors are corrected timely.

Revenue is currently reviewing the entire process associated with the remitting of MVU tax by County Clerks. This review is being done in an effort to make the entire process more efficient and effective. This review includes potentially mandating Electronic Funds Transfer (EFT) from all counties, suggesting more efficient methods of processing current EFT payments, and efficient methods of applying penalties when warranted. Revenue estimates that the changes as a result of this review will be implemented by the end of FY'05.

Eliminating the temporary deposit accounts is also an issue being reviewed. These accounts are currently required by statute, and any change in this method of deposit will require statutory changes.

FINANCIAL STATEMENT FINDINGS

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

FINDING 03-REV-12: The Kentucky Revenue Cabinet Should Ensure Mathematical Accuracy And Completeness Of Key Information

Revenue does not have adequate procedures to ensure critical taxpayer information is accurate and complete. There are limited procedures in place to verify the accuracy and completeness of critical taxpayer information.

Without adequate procedures, taxpayers could pay the wrong amount of tax. It is Revenue's responsibility to ensure, to a reasonable degree, that all revenue owed to the Commonwealth is collected.

Recommendation

We recommend Revenue implement procedures to verify the accuracy and completeness of critical taxpayer information.

Management's Response and Corrective Action Plan

Revenue agrees with the auditor's recommendation that additional procedures should be implemented to improve the processing of taxpayer information.

FINANCIAL STATEMENT FINDINGS***Other Matters Relating to Internal Controls and/or Instances of Noncompliance*****FINDING 03-REV-13: The Division Of Property Valuation Education And Research Branch Should Reconcile Receipts To Management Administrative Reporting System And Ensure Checks Are Timely Deposited**

During the Receipts audit, we documented the procedures related to the depositing of checks by the Office of Financial and Administrative Services, PVA Administrative Support Branch (the Office). The Office deposits money given directly to them from county Property Valuation Administrators (PVAs) for deputy hire and money given to them by the Division of Property Valuation Education and Research Branch (ERB) for educational courses. We noted the following weaknesses:

- The ERB does not review the CR (cash receipt) documents or other supporting documentation to ensure the Office deposited all checks and recorded all deposits in Management Administrative Reporting System (MARS).
- The ERB holds checks until the information is entered into its computer system and then gives them to the Office for deposit. During our testing, we noticed one check dated May 1, 2001 that was deposited August 2, 2002. We were unable to determine why the check was not deposited for so long.

An incorrect amount could be entered on the CR document in MARS, and ERB would not be aware of the problem. Checks could be lost or misplaced while being held for an extended period of time. Also, the state could be earning interest if the checks were deposited quickly.

Proper internal controls dictate agencies reconcile supporting documentation to the CRs in MARS. KRS 41.070 states receipts should be deposited in the "most prompt and cost-efficient manner available."

Recommendation

We recommend the following:

- The Office will provide copies of the approved CR documents and copies of checks to the ERB employee responsible for handling the Education Registration. The Office will add the check number to the CR document description line because ERB tracks checks by check number. The ERB employee will add a column to the access database and check off all checks deposited.
- ERB should consider implementing procedures for submitting checks to be deposited every 2-3 business days.

FINANCIAL STATEMENT FINDINGS

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

FINDING 03-REV-13: The Division Of Property Valuation Education And Research Branch Should Reconcile Receipts To Management Administrative Reporting System And Ensure Checks Are Timely Deposited (Continued)

Management's Response and Corrective Action Plan

Revenue concurs with the recommendation of the Auditor of Public Account (APA). The PVA Administrative Support Branch started including the check number on the CR documents and providing copies of the approved CR documents and checks to the PVA Education and Research Branch (ERB) in December 2003. In addition, the ERB has implemented procedures to ensure that checks are submitted to the PVA Administrative Support Branch for deposit every 2-3 business days.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
<u>Reportable Conditions</u>					
<i>(1) Audit findings that have been fully corrected:</i>					
FY 02	02-REV-4	The Kentucky Revenue Cabinet Should Ensure All Open Ports On Agency Machines Have A Business-Related Purpose	N/A	0	Due to improvements, this finding is downgraded to another matter for FY 03. See 03-REV-10.
<i>(2) Audit findings not corrected or partially corrected:</i>					
FY 02	02-REV-1	The Kentucky Revenue Cabinet Should Ensure Confidential Taxpayer Information Is Protected And Preserved As Required By Statute	N/A	0	See 03-REV-1.
FY 02	02-REV-2	The Kentucky Revenue Cabinet Should Update The Sales Tax Database And Automate Processing Of Accelerated Tax Returns	N/A	0	See 03-REV-2.
FY 02	02-REV-3	The Kentucky Revenue Cabinet Should Strengthen The Security Surrounding Administrator Accounts	N/A	0	See 03-REV-3.
FY 02	02-REV-5	The Kentucky Revenue Cabinet Should Ensure All User Accounts On The Agency Servers Are Necessary	N/A	0	See 03-REV-4.
FY 01	01-REV-1	The Revenue Cabinet Should Update The Sales Tax Database And Automate Processing Of Accelerated Tax Returns	N/A	0	See 03-REV-2.
FY 01	01-REV-3	The Revenue Cabinet Should Have A System In Place To Reconcile Critical Information	N/A	0	See 03-REV-5.

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

There were no findings for this section.

(4) Audit finding is no longer valid:

There were no findings for this section.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
<u>Material Weaknesses/Noncompliances</u>					
<i>(1) Audit findings that have been fully corrected:</i>					
There were no findings for this section.					
<i>(2) Audit findings not corrected or partially corrected:</i>					
FY 02	02-REV-6	The Kentucky Revenue Cabinet Should Have A System In Place To Reconcile Critical Information	N/A	0	The reconciliation is expected to be operational in FY 04. Due to improvements, this finding is downgraded to a reportable condition for FY 03. See 03-REV-5.
<i>(3) Corrective action taken is significantly different from corrective action previously reported:</i>					
There were no findings for this section.					
<i>(4) Audit finding is no longer valid:</i>					
There were no findings for this section.					
<u>Other Matters</u>					
<i>(1) Audit findings that have been fully corrected:</i>					
FY 02	02-REV-9	The Kentucky Revenue Cabinet Should Distribute Receipts Prior To Year End	N/A	0	Resolved during FY 03.
FY 02	02-REV-10	The Kentucky Revenue Cabinet Should Ensure That Individual Income Tax Refunds Are Properly Approved	N/A	0	Resolved during FY 03.
FY 02	02-REV-11	The Kentucky Revenue Cabinet Should Remove The Simple Network Management Protocol Service Or Change The Default Community String	N/A	0	Resolved during FY 03.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
<u>Other Matters</u>					
<i>(2) Audit findings not corrected or partially corrected:</i>					
FY 02	02-REV-7	The Kentucky Revenue Cabinet Should Implement A System For Crosschecking Motor Fuels Dealer Reports	N/A	0	See 03-REV-6.
FY 02	02-REV-8	The Kentucky Revenue Cabinet Should Date Stamp Motor Fuels And Motor Vehicle Usage Tax Reports	N/A	0	See 03-REV-7.
FY 02	02-REV-12	The Kentucky Revenue Cabinet Should Ensure That Security Information Leakage Concerning Agency Devices Is Minimized	N/A	0	See 03-REV-8.
FY 02	02-REV-13	The Kentucky Revenue Cabinet Password Policy Should Be Consistently Applied To All Local Area Network Servers	N/A	0	See 03-REV-9.
FY 01	01-REV-4	The Revenue Cabinet Should Implement A System For Crosschecking Motor Fuels Dealer Reports	N/A	0	See 02-REV-7.
FY 01	01-REV-5	The Revenue Cabinet Should Ensure That All Tax Files Are Safeguarded	N/A	0	See 03-REV-1.
FY 01	01-REV-9	Revenue Password Policy Should Be Consistently Applied To All Local Area Network Servers	N/A	0	See 03-REV-9.
FY 01	01-REV-10	Revenue Cabinet Should Ensure That Information Leakage Concerning Agency Devices Is Minimized	N/A	0	See 03-REV-8.

SUMMARY SCHEDULE OF PRIOR AUDIT FINDINGS
FOR THE YEAR ENDED JUNE 30, 2003

Fiscal Year	Finding Number	Finding	CFDA Number	Questioned Costs	Comments
<u>Other Matters</u>					
<i>(2) Audit findings not corrected or partially corrected (Continued):</i>					
FY 98	98-KRC-1	The Revenue Cabinet Should Properly Safeguard Corporation Tax Returns	N/A	0	The Accounts Receivable comment is resolved since no problems were noted. However, during refunds and receipts testing, some tax return could not be located. See 03-REV-1.
FY 98	98-KRC-3	The Revenue Cabinet Should Ensure That Motor Fuel Reports Are Cross-Checked as Required	N/A	0	See 03-REV-6.
FY 97	97-KRC-7	The Revenue Cabinet Should Properly Safeguard Corporation Tax Returns	N/A	0	See 03-REV-1.

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

There were no findings for this section.

(4) Audit finding is no longer valid:

There were no findings for this section.

THIS PAGE LEFT BLANK INTENTIONALLY

