

**Audit Results From
CAFR and Single Audit Procedures**

Department of Health

**For the Year Ended
June 30, 2005**

**STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY**

**Department of Audit
Division of State Audit**

Arthur A. Hayes, Jr., CPA, JD, CFE
Director

Edward Burr, CPA
Assistant Director

Kandi B. Thomas, CPA, CFE
Audit Manager

Michael S. Edwards, CPA
In-Charge Auditor

Demaro R. Isom
Benjamin Rogers
Jonathan S. Ward, CFE
Staff Auditors

Amy Brack
Editor

Comptroller of the Treasury, Division of State Audit
1500 James K. Polk Building, Nashville, TN 37243-0246
(615) 401-7897

Financial/compliance audits of state departments and agencies are available on-line at
www.comptroller.state.tn.us/sa/reports/index.html.

For more information about the Comptroller of the Treasury, please visit our website at
www.comptroller.state.tn.us.

**Department of Health
For the Year Ended June 30, 2005**

TABLE OF CONTENTS

	<u>Page</u>
Executive Summary	1
Transmittal Letter	3
Results of Procedures	4
Findings and Recommendations	6
Status of Prior Audit Findings	15
Observations and Comments	16

**Department of Health
For the Year Ended June 30, 2005**

EXECUTIVE SUMMARY

Findings

- FINDING 1 As noted in the previous audit, the department did not perform an inventory audit of a high-risk food delivery vendor for the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) when information raising concerns about the vendor's contract came to management's attention. Because of the high risk of fraud by the vendor, the department should have performed more extensive monitoring of this vendor to ensure that resources allocated for the WIC program were properly expended (page 6).
- FINDING 2 As noted in the prior audit, the department did not have information systems policies and procedures governing the user authorization process over the Patient Tracking and Billing Management Information System and still has not fully addressed the risks of unauthorized access to PTBMIS (page 8).
- FINDING 3 As noted in the prior audit, the department's controls over access to the federal Vaccine Management System (VACMAN), which is the computer system that the department uses to place vaccine orders with the federal Centers for Disease Control (CDC), need improvement. The department has not assessed and mitigated the risks of misappropriation, misuse, or waste of vaccine associated with ineffective controls over the VACMAN computer system (page 9).
- FINDING 4 The department did not assess the risks of inadequate policies and procedures for proper follow-up and corrective action of monitoring deficiencies identified when the department performed monitoring activities of subrecipients for the Block Grants for Prevention and Treatment of Substance Abuse (SAPT) program (page 11).
- FINDING 5 Management has not assessed and mitigated the risks associated with unauthorized program changes to the department's Alcohol and Drug Abuse Management Information System, which contains confidential patient information; management has also failed to test and approve a disaster recovery plan (page 13).

This report addresses reportable conditions in internal control and noncompliance issues found at the Department of Health during our annual audit of the state's financial statements and major federal programs. For the complete results of our audit of the State of Tennessee, please see the State of Tennessee *Comprehensive Annual Financial Report* for the Year Ended June 30, 2005, and the State of Tennessee *Single Audit Report* for the Year Ended June 30, 2005. The scope of our audit procedures at the Department of Health was limited. During the audit for the year ended June 30, 2005, our work at the Department of Health focused on three major federal programs: Immunization Grants, Block Grants for Prevention and Treatment of Substance Abuse, and the Special Supplemental Nutrition Program for Women, Infants, and Children. We audited these federally funded programs to determine whether the department complied with certain federal requirements and whether the department had an adequate system of internal control over the program to ensure compliance. Management's response is included following each finding.



STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY
State Capitol
Nashville, Tennessee 37243-0260
(615) 741-2501

John G. Morgan
Comptroller

April 6, 2006

The Honorable Phil Bredesen, Governor
and
Members of the General Assembly
State Capitol
Nashville, Tennessee 37243
and
The Honorable Kenneth S. Robinson, Commissioner
Department of Health
Cordell Hull Building, 426 Fifth Avenue North
Nashville, Tennessee 37247

Ladies and Gentlemen:

Transmitted herewith are the results of certain limited procedures performed at the Department of Health as a part of our audit of the *Comprehensive Annual Financial Report* of the State of Tennessee for the year ended June 30, 2005, and our audit of compliance with the requirements described in the U.S. Office of Management and Budget Circular A-133 Compliance Supplement.

Our review of management's controls and compliance with laws, regulations, and the provisions of contracts and grants resulted in certain findings which are detailed in the Findings and Recommendations section.

Sincerely,

John G. Morgan
Comptroller of the Treasury

JGM/kbt
05/110



STATE OF TENNESSEE
COMPTROLLER OF THE TREASURY
DEPARTMENT OF AUDIT
DIVISION OF STATE AUDIT

JAMES K. POLK STATE OFFICE BUILDING, SUITE 1500
NASHVILLE, TENNESSEE 37243-0264
PHONE (615) 401-7897 ♦ FAX (615) 532-2765

December 20, 2005

The Honorable John G. Morgan
Comptroller of the Treasury
State Capitol
Nashville, Tennessee 37243

Dear Mr. Morgan:

We have performed certain audit procedures at the Department of Health as part of our audit of the financial statements of the State of Tennessee as of and for the year ended June 30, 2005. Our objective was to obtain reasonable assurance about whether the State of Tennessee's financial statements were free of material misstatement. We emphasize that this has not been a comprehensive audit of the Department of Health.

We also have audited certain federal financial assistance programs as part of our audit of the state's compliance with the requirements described in the U.S. Office of Management and Budget (OMB) Circular A-133 Compliance Supplement. The following table identifies the State of Tennessee's major federal programs administered by the Department of Health. We performed certain audit procedures on these programs as part of our objective to obtain reasonable assurance about whether the State of Tennessee complied with the types of requirements that are applicable to each of its major federal programs.

**Major Federal Programs Administered by the
Department of Health
For the Year Ended June 30, 2005
(in thousands)**

<u>CFDA Number</u>	<u>Program Name</u>	<u>Federal Disbursements</u>
10.557	Special Supplemental Nutrition Program for Women, Infants, and Children	\$101,452
93.268	Immunization Grants	\$30,806
93.959	Block Grants for Prevention and Treatment of Substance Abuse	\$30,015

Source: State of Tennessee's Schedule of Expenditures of Federal Awards for the year ended June 30, 2005.

The Honorable John G. Morgan
December 20, 2005
Page Two

We conducted our audit in accordance with auditing standards generally accepted in the United States of America and the standards contained in *Government Auditing Standards*, issued by the Comptroller General of the United States.

We have issued an unqualified opinion, dated December 20, 2005, on the State of Tennessee's financial statements for the year ended June 30, 2005. We will issue, at a later date, the State of Tennessee *Single Audit Report* for the same period. In accordance with *Government Auditing Standards*, we will report on our consideration of the State of Tennessee's internal control over financial reporting and our tests of its compliance with certain laws, regulations, and provisions of contracts and grants in the *Single Audit Report*. That report will also contain our report on the State of Tennessee's compliance with requirements applicable to each major federal program and internal control over compliance in accordance with OMB Circular A-133.

As a result of our procedures, we identified certain internal control and compliance issues related to the major federal programs at the Department of Health. Those issues, along with management's response, are described immediately following this letter. We have reported other less significant matters involving the department's internal control and instances of noncompliance to the Department of Health's management in a separate letter.

This report is intended solely for the information and use of the General Assembly of the State of Tennessee and management, and is not intended to be and should not be used by anyone other than these specified parties. However, this report is a matter of public record.

Sincerely,

A handwritten signature in black ink that reads "Arthur A. Hayes, Jr." The signature is written in a cursive style with a large, prominent initial "A".

Arthur A. Hayes, Jr., CPA
Director

FINDINGS AND RECOMMENDATIONS

1. The department still did not perform an inventory audit of a high-risk WIC vendor even though auditors identified the risk of vendor fraud in the prior audit

Finding

As noted in the previous audit, the Department of Health did not perform an inventory audit of a high-risk food delivery vendor for the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC) when information raising concerns about the vendor's contract came to management's attention. The Department of Health reimbursed this vendor \$1,667,033 for food vouchers redeemed for the year ended June 30, 2005.

As noted in the prior audit report, the following information came to management's attention:

- The WIC Director for Davidson County/Metropolitan government awarded a food delivery agreement to a vendor which was owned by her secretary's husband, creating a potential conflict of interest. The vendor was the parent company of three WIC food delivery vendors within Davidson County.
- The vendor was allowed to maintain food stores which provided only WIC food items which could be redeemed with WIC vouchers, rather than traditional WIC retail food stores that provide WIC and non-WIC food items. These were the only non-retail food delivery stores in the state. WIC products at these stores were sold for amounts which were higher than for similar products at the traditional retail WIC vendors.

In addition, we noted that these three food stores had among the highest WIC voucher redemptions during the period ended June 30, 2004, when compared to voucher redemptions of other vendors in Davidson County and in other regions of the state.

In the prior audit report, we recommended that the department perform more extensive monitoring procedures including performing audits of the vendor's records to compare the claims for reimbursement against records of inventory purchases from wholesalers. Management did not concur with the finding and stated that the department was precluded from performing other compliance activities because such activities are virtually impossible in a WIC-only store.

In our rebuttal to management's comment, we stated that the *Code of Federal Regulations*, Title 7, Part 246, Section 12(j)(4)(i), requires that for high-risk vendors,

The State agency must conduct compliance investigations of a minimum of five percent of the number of vendors authorized by the State agency as of October 1 of each fiscal year. The State agency must conduct compliance investigations on

all high-risk vendors up to the five percent minimum. . . . A compliance investigation of a high-risk vendor may be considered complete when the State agency determines that a sufficient number of compliance buys have been conducted to provide evidence of program noncompliance, when two compliance buys have been conducted in which no program violations are found, or when an inventory audit has been completed.

Our review during the current audit revealed that the department, as it had done in the previous year, classified this food delivery vendor as high-risk and performed monitoring visits for all three food stores during the year ended June 30, 2005; however, the recommended inventory audit was not performed. The monitoring visits did include ensuring product prices were within guidelines, that the vendor keeps required items in stock, observing transactions that take place, ensuring vouchers on hand are in compliance with rules and regulations, and discussing any findings that were taken.

We attempted, in the current audit, to obtain the vendor's inventory records (beginning inventory, purchases, goods sold, and ending inventory) to perform an inventory audit at each of the three vendor locations. The planned procedures included a comparison of the vendor's inventory purchases and distributions to the department's WIC food voucher redemption records for this vendor. However, the vendor's management could not provide the requested inventory records for the audit to be performed.

Because of the high risk of fraud by the vendor, the department should have performed an inventory audit of this vendor to ensure that resources allocated for the WIC program were properly expended.

Recommendation

The Commissioner should immediately demand that the vendor provide documentation of sufficient quantities of WIC inventory to match the quantities of WIC items charged to the WIC program. If adequate records are not provided, the Commissioner should then subject the vendor to sanctions that would include fines or disqualification as required by the rules of the program.

Management's Comment

We concur. Although the Department did not conduct an inventory audit, this vendor received additional monitoring beyond the regular vendor monitoring at the three locations. Location 1 – 10/1/04, 2/24/05, 7/7/05, 9/27/05; Location 2 – 10/21/04, 5/16/05; and Location 3— 10/1/04, 2/24/05, 7/7/05. Results continue to verify that the vendor was meeting current minimum stock and competitive price requirements. Monitoring results and observations verify that price reports indicate that each location is within the guidelines for their peer group. Regular price reports show that prices remain within the appropriate range for the peer group.

Based on recommendations by the State auditors, an inventory audit using the procedures in Chapter 7 of the WIC Vendor Management Manual began on February 22, 2006. Upon completion of the inventory audit, an assessment of the findings will provide the needed documentation for any action of disqualification, termination, or fines.

The current WIC Vendor Agreement states that the vendor agrees “to produce, upon request of an authorized WIC Program representative, bills of lading or invoices for a period not to exceed the previous ninety (90) days and/or pertinent inventory records used for federal tax reporting purposes, as proof of purchase of merchandise represented as being provided to program participants by redeemed voucher.” If adequate records are not provided, the vendor will be subject to sanctions that would include disqualification, termination, or fines as required by the rules of the program.

2. Management still has not fully addressed the risks of unauthorized access to PTBMIS

Finding

As noted in the prior audit, the Department of Health still did not have information systems policies and procedures governing the user authorization process for the Patient Tracking and Billing Management Information System (PTBMIS). Also as noted in the prior audit, department personnel still had not implemented user-level system security reporting for PTBMIS. Such security reports should be used to identify the level of access each user has to system screens, data, and processes.

Management concurred with the prior finding and prepared draft policies that will standardize the forms and rules used to assure that only approved users have access to PTBMIS functions. The draft policies will also specify users’ security levels within PTBMIS and procedures for termination of users’ access when necessary. However, these draft policies had not been approved and placed into operation. Management plans to have the policies formalized in January 2006.

Without formal policies and procedures over the PTBMIS authorization process, the department cannot mitigate the risk of unauthorized access to PTBMIS. Unauthorized access increases the risk that unauthorized changes can be made to the system without detection. Routinely monitoring access activities of system users can help identify significant problems, such as violations to segregation of duties or unauthorized access to sensitive information, and can help deter users from attempting inappropriate or unauthorized activities.

Recommendation

The Commissioner should ensure that the department’s Office for Information Technology (OIT) formally adopts policies and procedures for the user authorization process as soon as possible. OIT should also monitor PTBMIS user authorities and activities. All reviews

and actions should be fully documented and reviewed by top management for adequacy, completeness, and corrective actions.

The Commissioner should ensure that all risks related to PTBMIS system security controls are adequately identified and assessed in the department's documented risk assessment activities. The Commissioner should identify specific staff to be responsible for the design and implementation of internal controls to prevent and detect exceptions timely. The Commissioner should also identify staff to be responsible for ongoing monitoring for compliance with all requirements and taking prompt action should exceptions occur.

Management's Comment

We concur. The Bureau of Health Services has drafted a policy that will standardize the forms and rules used to assure approved user access to the WIC voucher functions within PTBMIS. During the comment period for the draft security access policy, systems administrators and others were made aware of the need for improved documentation of WIC voucher direct access grant actions and began making appropriate changes to internal procedures. This policy is being finalized and will go into effect March 2006.

In addition, in January 2006, the Department's Health Executive Management Committee (HEMAC) approved a Tennessee Department of Health, Chief Information Security Officer (CISO) function that will reside in the Office of Information Technology. This functional leader will provide oversight for the development and implementation of enterprise security initiatives, security policies, and standards which align with the State of Tennessee information security policies.

3. The department has not assessed and mitigated the risks of misappropriation, misuse, or waste of vaccine associated with ineffective controls over the VACMAN computer system

Finding

As noted in the prior audit, the department's controls over access to the federal Vaccine Management System (VACMAN), which is the computer system that the department uses to place vaccine orders with the federal Centers for Disease Control (CDC), need improvement. The VACMAN system was first installed in 1994. Our review of the VACMAN system revealed that the department corrected one of the three weaknesses reported in the previous audit report by requiring management approval of provider agreements, but the following weaknesses were still noted:

- All employees in the department's Communicable and Environmental Disease Service (CEDS) section with access to VACMAN can enter new providers into the system and can generate orders for vaccine.

- CEDS staff did not reconcile the providers listed in the VACMAN system to the actual provider agreements.

Management concurred with the prior finding and stated:

We concur. The Immunization Program will take further steps to minimize the possibility of fraud or abuse. First, the Immunization Program will institute a process whereby a provider's medical license is verified as on file with the state and current before the provider is authorized to enroll in the program; this verification will be dated and initialed on the enrollment form. Additionally, the person responsible for verification and authorization of credentials will not generate orders in the VACMAN system. No orders will be generated until the credentials check and authorization are completed.

Purchases of vaccine off the federal contracts through the VACMAN 3 system are restricted to individuals who possess a CDC-issued digital certificate for VACMAN and a password – a two-factor authentication system. This security approach markedly enhances physical security of the software/hardware.

Management did implement the procedures outlined in its response to the prior-year finding. However, these steps are not sufficient to prevent a CEDS employee, if he or she chose to deviate from management's established procedures, from misappropriating or misusing the department's vaccines. Any CEDS employee with access to the system can add new providers, place orders for vaccine, and distribute the vaccine to the provider. Thus, vaccine could be used for something other than intended purposes.

Recommendation

The Commissioner should ensure that the CEDS Director requires reconciliations of providers listed in the VACMAN system with provider agreements. In addition, the Commissioner and the CEDS Director should consider utilizing department personnel outside CEDS, if necessary, in any reconciliation process or any compensating controls that are developed.

The Commissioner should ensure that risks identified in this finding are adequately assessed in the department's documented risk assessment activities. The Commissioner should identify specific staff to be responsible for the design and implementation of internal controls related to the VACMAN system to prevent and detect exceptions timely. The Commissioner should also identify staff to be responsible for ongoing monitoring for compliance with all requirements and taking prompt action should exceptions occur.

Management's Comment

We concur. The Immunization Program will take further steps to minimize the possibility of fraud or abuse. The Immunization Program Manager will be responsible for the design and implementation of internal controls related to the VACMAN system to prevent exceptions and assure timely detection of any exceptions that may occur.

No CEDS staff member outside of the Immunization Program has access to the VACMAN system; access to this system requires two passwords: the log on password for the computer on which the program is installed and the password to enter the VACMAN program itself. For this reason, reconciliation and oversight of internal control procedures will be conducted by a CEDS administrator outside the Immunization Program. The Administrative Services Assistant (ASA) 5 in the CEDS Administration Section responsible for CEDS contract monitoring will fill this role. Before the end of April each year, following the end of the annual provider re-enrollment period, he/she will reconcile provider agreement forms with the providers listed in the VACMAN system. At this time, he/she also will monitor the Immunization Program's compliance with all requirements for VACMAN control procedures and will take prompt action should exceptions occur.

4. The department did not assess and mitigate the risks associated with inadequate policies and procedures governing the follow-up and corrective action of monitoring deficiencies in the SAPT program

Finding

The department did not assess the risks of inadequate policies and procedures for proper follow-up and corrective action of monitoring deficiencies identified when the department performed monitoring activities of subrecipients for the Block Grants for Prevention and Treatment of Substance Abuse (SAPT) program.

The department's Office of Internal Audit performs subrecipient monitoring activities for the SAPT program and reports the deficiencies in writing to the subrecipients. The Office of Internal Audit requires the subrecipients to submit a Corrective Action Plan for resolving the deficiencies noted. However, it is ultimately the Bureau of Alcohol and Drug Abuse Services' responsibility to ensure that a subrecipient's deficiencies are properly resolved.

Office of Management and Budget Circular A-133, "Audits of States, Local Governments, and Non-Profit Organizations," Subpart D, Section 400, states,

A pass-through entity shall . . . Monitor the activities of subrecipients as necessary to ensure that Federal awards are used for authorized purposes in compliance with laws, regulations, and the provisions of contracts or grant agreements and that performance goals are achieved.

A key component of these monitoring responsibilities is that the pass-through entity perform appropriate follow-up duties to ensure that the subrecipient takes corrective action to address the deficiencies discovered during the monitoring procedures.

We reviewed a sample of 20 subrecipient monitoring reports for monitoring activities performed by the department for the year ended June 30, 2005. Our review revealed that:

- For 20 of 20 subrecipient monitoring reports tested (100.0%), either Corrective Action Plans submitted by SAPT subrecipients were not followed up by bureau staff or the Office of Internal Audit had no evidence that the required Corrective Action Plans were received.

Based on discussions with the Director of the Alcohol and Drug Addiction Treatment Program and the Director of the Office of Internal Audit, management agreed that the policies and procedures for the follow-up and corrective action of deficiencies identified by the department SAPT subrecipients were inadequate. The lack of adequate policies and procedures to ensure the resolution of monitoring deficiencies noted could result in unauthorized program expenditures which may result in questioned costs and/or sanctions by the U.S. Department of Health and Human Services.

Recommendation

The Commissioner should ensure that policies and procedures are developed to ensure that staff perform follow-up of subrecipients' deficiencies and that those deficiencies are corrected. The Commissioner should ensure that staff take immediate action to follow up on the 20 subrecipient monitoring reports identified in the finding.

The Commissioner should ensure that risks such as these noted in this finding are adequately identified and assessed in management's documented risk assessment activities. Management should identify specific staff to be responsible for the design and implementation of controls over compliance requirements to prevent and detect exceptions timely. Management should also identify staff to be responsible for ongoing monitoring and taking prompt action should exceptions occur.

Management's Comments

We concur and steps have already been taken to ensure that the Corrective Action Plans are received, approved, and followed up on.

A&D Comment

The Bureau of Alcohol and Drug Abuse Services (BADAS) and the Office of Internal Audit (OIA) have developed procedures to follow up on monitoring deficiencies with the SAPT Block Grant subrecipients. During the auditing period, a great deal of fluctuation was occurring

in Department of Health (DOH) due to the return of the PAR function from the Department of Finance and Administration; specifically, where the monitoring functions would reside within DOH. These transition issues likely caused the problems noted in the audit. In April 2005, OIA assumed responsibility for the receipt of CAPs and has developed a procedure to ensure that the CAPs are received and timely transmitted to the responsible bureau.

Internal Audit Comment

During the time in question, much fluctuation was occurring in the return of the PAR function from Finance and Administration to the Department and where the monitoring functions would reside within the Department. These transition issues likely caused the problems noted. In April 2005 the Office of Internal Audit assumed responsibility over the receipt of the CAPs and has steps in place to ensure that the CAPs are received and timely transmitted to the responsible bureau. The responsible bureau is responsible for ensuring that the CAP is appropriate and properly implemented.

5. Management has not assessed and mitigated the risks associated with unauthorized program changes to the department's Alcohol and Drug Abuse Management Information System, which contains confidential patient information; management has also failed to test and approve a disaster recovery plan

Finding

The Department of Health does not have written system policies and procedures governing program changes to the Alcohol and Drug Abuse Management Information System (ADMIS), and management did not approve program changes made to ADMIS during the audit period. In addition, although the department developed a disaster recovery plan for ADMIS, the plan has not been tested or approved by top management.

The department's Bureau of Alcohol and Drug Abuse Services serves as the single state authority for receiving and administering federal block grant funding from the U.S. Department of Health and Human Services, Substance Abuse and Mental Health Services Administration. The bureau contracts with community-based agencies for the provision of treatment and prevention services and utilizes ADMIS to record confidential data received each month from the services providers. Top management relies on this system data to disburse funds to service providers and to monitor contract compliance.

Testwork revealed that bureau and information system management had not approved any of the 15 program changes made to ADMIS during the audit period. Although these system changes (including changes to contract dates, corrections of errors, modification of queries, addition of fields, adjustments of column totals, and the modification of reports and forms) did not affect payments to service providers, the risk is increased that unauthorized system changes could result in unauthorized payments to providers. Management's inadequate consideration of patient confidentiality may result in the violation of federal alcohol and drug patient confidentiality laws.

Furthermore, management is responsible for establishing a disaster recovery plan to ensure adequate processes are in place to safeguard data and to recover data in the event of a disaster. Without a proper disaster recovery plan, the department runs the risk of losing electronically protected health information in the event of a disaster.

Recommendation

The Commissioner should ensure that appropriate and adequate written policies and procedures are developed as soon as possible for program changes. The Commissioner should ensure that management appropriately authorizes system changes before changes are made to the ADMIS system by assigning specific responsibility for these activities and taking steps to ensure these important steps are taken. A Disaster Recovery Plan for ADMIS should be tested and should be approved by the proper personnel.

In addition, the Commissioner should also assign specific responsibility to someone in management over the Information Systems operations to take appropriate steps to reasonably ensure that staff over the information technology operations are knowledgeable about the significant risks to the department's information technology operations and the significance, importance, and need for appropriate disaster recovery controls. These steps should include documenting these risk assessments and assigning staff to design and implement effective controls. The controls should be fully documented and should include assignment of specific staff to regularly monitor operations to ensure controls are operating effectively and are being regularly and formally tested. The individual who is assigned the responsibility of monitoring activities should document the monitoring activities. If any issues are identified in the monitoring process, the individual should advise a member of management who has been designated by upper management, to be responsible for following up on such matters. Management should seek clarification of any terms, comments, or observations as necessary before adopting the risk assessments and related controls.

Management's Comments

A&D Comment

Management partially concurs. In May 2002, the Bureau of Alcohol and Drug Abuse Services (BADAS) developed a policy on the responsibilities of application systems management and the protection of information technology resources. The policy states that the "application system change request forms must be completed and submitted to the agency system administrator. Once finalized, the application system change request is submitted to the agency management team for review and approval." An informal procedure was developed to track changes to the Alcohol and Drug Abuse Management Information System (ADMIS). In July 2005, management reviewed the policy and revised the procedure to include a "formal" document.

In April 2005, a Disaster Recovery Plan was submitted to the Office of Information Technology. BADAS will test and approve the plan.

OIT Comment

OIT has changed control procedures in place that cover ADMIS-Insight on the AS/400. These are the procedures that were implemented July 1, 2005. The data on the AS/400 is backed up daily.

Auditor's Comment

As noted in the finding, the Department of Health's Bureau of Alcohol and Drug Abuse Services did not provide documentation of its approval for any of the program changes made to ADMIS during the audit period. Furthermore, management acknowledges in its response that a revised procedure was necessary and as of July 2005 includes a formal document for program changes.

STATUS OF PRIOR AUDIT FINDINGS

State of Tennessee *Single Audit Report* for the year ended June 30, 2004

Audit findings pertaining to the Department of Health were included in the *Single Audit Report*. The updated status of these findings as determined by our audit procedures is described below.

Resolved Audit Findings

The current audit disclosed that the Department of Health has taken action to correct the following audit findings:

- the department has issued WIC vouchers to individuals who appeared not to be eligible based on the information contained in the PTBMIS system;
- management could not provide adequate assurances that no improper program changes and modifications had occurred;
- the department does not have information systems policies and procedures;
- the department lacks segregation of duties over the issuance of food vouchers to participants in the Special Supplemental Nutrition Program for Women, Infants, and Children (WIC);

- the department did not monitor the required percentage of local agencies or clinics for the WIC program;
- the Department of Health has not followed its policy to identify and prevent dual participation in the WIC and CSFP programs;
- the department understated expenditures for the Immunization Grants program on the Schedule of Expenditures of Federal Awards for fiscal year ended June 30, 2004, by 4.7 million; and
- the department did not comply with program requirements and special test provisions for the Immunization Grants program for fiscal year ended 2004.

Repeated Audit Findings

The current audit disclosed that the Department of Health has not corrected the previous audit findings concerning

- adequate monitoring of a high-risk WIC vendor;
- the department's risks of unauthorized access to the Patient Tracking and Billing Management Information System; and
- the department's ineffective controls over the VACMAN computer system.

Most Recent Financial and Compliance Audit

Audit report number 04/064 for the Department of Health, issued in February 2005, contained certain audit findings that were not included in the State of Tennessee *Single Audit Report*. These findings were not relevant to our current audit and, as a result, we did not pursue their status as a part of this audit.

OBSERVATIONS AND COMMENTS

MANAGEMENT'S RESPONSIBILITY FOR RISK ASSESSMENT

Auditors and management are required to assess the risk of fraud in the operations of the department. The risk assessment is based on a critical review of operations considering what frauds could be perpetrated in the absence of adequate controls. The auditors' risk assessment is limited to the period during which the audit is conducted and is limited to the transactions that the auditors are able to test during that period. The risk assessment by management is the primary method by which the department is protected from fraud, waste, and abuse. Since new programs may be established at any time by management or older programs may be discontinued, that assessment is ongoing as part of the daily operations of the department.

Risks of fraud, waste, and abuse are mitigated by effective internal controls. It is management's responsibility to design, implement, and monitor effective controls in the department. Although internal and external auditors may include testing of controls as part of their audit procedures, these procedures are not a substitute for the ongoing monitoring required of management. After all, the auditor testing is limited and is usually targeted to test the effectiveness of particular controls. Even if controls appear to be operating effectively during the time of the auditor testing, they may be rendered ineffective the next day by management override or by other circumstances that, if left up to the auditor to detect, will not be noted until the next audit engagement and then only if the auditor tests the same transactions and controls. Furthermore, since staff may be seeking to avoid auditor criticisms, they may comply with the controls during the period that the auditors are on site and revert to ignoring or disregarding the control after the auditors have left the field.

The risk assessments and the actions of management in designing, implementing, and monitoring the controls should be adequately documented to provide an audit trail both for auditors and for management, in the event that there is a change in management or staff and to maintain a record of areas that are particularly problematic.

FRAUD CONSIDERATIONS

Statement on Auditing Standards No. 99 promulgated by the American Institute of Certified Public Accountants requires auditors to specifically assess the risk of material misstatement of an audited entity's financial statements due to fraud. The standard also restates the obvious premise that management, and not the auditors, is primarily responsible for preventing and detecting fraud in its own entity. Management's responsibility is fulfilled in part when it takes appropriate steps to assess the risk of fraud within the entity and to implement adequate internal controls to address the results of those risk assessments.

During our audit, we discussed these responsibilities with management and how management might approach meeting them. We also increased the breadth and depth of our inquiries of management and others in the entity as we deemed appropriate. We obtained formal assurances from top management that management had reviewed the entity's policies and procedures to ensure that they are properly designed to prevent and detect fraud and that management had made changes to the policies and procedures where appropriate. Top management further assured us that all staff had been advised to promptly alert management of all allegations of fraud, suspected fraud, or detected fraud and to be totally candid in all communications with the auditors. All levels of management assured us there were no known instances or allegations of fraud that were not disclosed to us.