



STATE OF TENNESSEE  
**COMPTROLLER OF THE TREASURY**  
DEPARTMENT OF AUDIT  
DIVISION OF COUNTY AUDIT  
SUITE 1500  
JAMES K. POLK STATE OFFICE BUILDING  
NASHVILLE, TENNESSEE 37243-0269  
PHONE (615) 401-7841

February 28, 2006

Houston County Mayor and  
Board of County Commissioners  
Houston County, Tennessee

To the County Mayor and County Commissioners:

In conjunction with the annual audit of Houston County, we have performed a limited review of the information systems in the Offices of County Mayor, Road Superintendent, Director of Schools, Trustee, Register, and Sheriff as of February 2, 2006. This letter transmits the results of our review.

Our audit of Houston County is required to be conducted in accordance with standards contained in Government Auditing Standards issued by the Comptroller General of the United States. These standards specify that we perform general and application control reviews of computer-based accounting and information systems to determine whether an entity's existing procedures and controls provide adequate assurance of data accuracy and financial and operating statement reliability.

Because of inherent limitations in any internal control structure, errors, irregularities, or control weaknesses may exist and may not be detected. However, our information system reviews performed in the Offices of Road Superintendent, Director of Schools, Trustee, and Register did not reveal any matters that we considered to be a reportable condition. Reportable conditions, however, were identified in the Offices of County Mayor and Sheriff. These reportable conditions may be included in the annual financial report of Houston County. These matters are also presented in detail in the enclosed Review of Internal Controls Regarding Information Systems Operations – Findings and Recommendations.

A brief summary of the reportable conditions by office is presented below:

**COUNTY MAYOR**

1. The Ambulance Service did not develop a disaster recovery plan.

Houston County Mayor and  
Board of County Commissioners  
February 28, 2006  
Page 2

**SHERIFF**

1. The office did not have formal policies and procedures for computer operations.
2. The office had deficiencies in computer system back-up procedures.
3. The office did not develop a disaster recovery plan.
4. The office did not implement adequate controls to protect its information resources.

Please contact Penny Austin, Information Systems Audit Manager, or me if you have any questions regarding our review of the information systems in the aforementioned offices of Houston County, Tennessee.

Sincerely,



Richard V. Norment  
Assistant to the Comptroller

RVN: pa

Attachment

cc: The Honorable Gary Booker, Road Superintendent  
The Honorable Cathy Harvey, Director of Schools  
The Honorable Annette Baggett, Trustee  
The Honorable Sherrill Moore, Register  
The Honorable Kenneth Barnes, Sheriff  
Mr. Norm Norment, West Tennessee Audit Manager

**HOUSTON COUNTY GOVERNMENT, TENNESSEE  
REVIEW OF INTERNAL CONTROLS REGARDING INFORMATION  
SYSTEM OPERATIONS — FINDINGS AND RECOMMENDATIONS  
AS OF FEBRUARY 2, 2006**

The review of controls over the information systems in the Offices of County Mayor and Sheriff indicated a need for improvement. It should be noted that this was the first information system review performed at the Ambulance Service which is under the supervision of the Office of County Mayor. It was also the first information system review performed in the Office of Sheriff. The following recommendations have been made to aid these offices in the implementation of controls to better secure their computer systems and the information contained therein. We reviewed these matters with management to provide an opportunity for their response. Management offered oral responses to these items but did not submit written responses. Oral responses have not been included in this report.

**OFFICE OF COUNTY MAYOR**

**RECOMMENDATION**

**THE OFFICE SHOULD DEVELOP A DISASTER RECOVERY PLAN**

Management of the Ambulance Service should develop and regularly update a disaster recovery plan defining procedures for personnel to follow in the event of a major hardware or software failure, or temporary or permanent destruction of facilities. The plan should contain provisions for a contingency operation site as well as the adequate backup of data files, system programs, user documentation, supplies, and computer hardware so that operations could continue as normally as possible. A copy of the plan should be kept in a secure area within the office as well as at a secure, off-site location.

---

**OFFICE OF SHERIFF**

**RECOMMENDATIONS**

1. **MANAGEMENT SHOULD FORMALLY DOCUMENT POLICIES  
AND PROCEDURES FOR COMPUTER OPERATIONS**

Management should prepare a computer policies and procedures manual. This manual should define policies and procedures for operations such as system startup/shutdown, application access, system access security, system backup and retention schedules, output distribution, hardware/software maintenance, and other general data processing functions. Upon completion, the manual should be distributed to all appropriate personnel.

2. **SYSTEM BACK-UP PROCEDURES SHOULD BE IMPROVED**

A secure, fireproof location should be used to store weekly and yearly backups. Some possibilities for an off-site storage location would be another county office building with a fireproof vault or a safe deposit box at a local bank. Furthermore, a current log of all backups that includes label descriptions, date of creation, contents, and storage location should be maintained.

3. **THE OFFICE SHOULD DEVELOP A DISASTER RECOVERY PLAN**

Management should develop and regularly update a disaster recovery plan. This plan should define procedures for personnel to follow in the event of a major hardware or software failure, or temporary or permanent destruction of facilities. The plan should contain provisions for a contingency operation site as well as the adequate backup of data files, system programs, user documentation, supplies, and computer hardware so that operations could continue as normally as possible. A copy of the plan should be kept in a secure area within the office as well as at a secure, off-site location.

4. **ADEQUATE CONTROLS TO PROTECT INFORMATION RESOURCES SHOULD BE IMPLEMENTED**

Adequate controls to protect information resources should be implemented. This recommendation does not identify specific vulnerabilities that could allow someone to exploit the office's information system or misuse county funds. Disclosing those vulnerabilities could present a potential security risk by providing the readers with information that might be confidential pursuant to Section 10-7-504(i), Tennessee Code Annotated. We provided the official with detailed information regarding the specific vulnerabilities we identified as well as our recommendations for improvement.

---

**PRIOR AUDIT RECOMMENDATIONS IMPLEMENTED**

(Ref: Review of Internal Controls Regarding  
Information System Operations as of October 31, 2003)

**OFFICE OF COUNTY MAYOR**

<b>Finding Number</b>	<b>Page Number</b>	<b>Subject</b>
1	1	Adequate inventory records were not maintained
2	1	The office did not have formal policies and procedures for computer operations

**OFFICE OF REGISTER**

<b>Finding Number</b>	<b>Page Number</b>	<b>Subject</b>
1	2	The office should develop formal policies and procedures for computer operations
2	2	System back-up procedures should be improved
3	2	A disaster recovery plan should be developed