



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

November 17, 2005

Hartsville/Trousdale County Government Executive and  
Board of County Commissioners  
Hartsville/Trousdale County Government, Tennessee

To the County Executive and County Commissioners:

In conjunction with the annual audit of Hartsville/Trousdale County Government, we have performed a limited review of the information systems in the Offices of County Executive, Highway Superintendent, Director of Schools, Trustee, Register, and Sheriff as of September 22, 2005. This letter transmits the results of our review.

Our audit of Hartsville/Trousdale County Government 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 Highway 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 Executive and Register. These reportable conditions may be included in the annual financial report of Hartsville/Trousdale County Government. 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 EXECUTIVE**

1. The Water and Sewer Department had deficiencies in computer system back-up procedures.
2. The Water and Sewer Department did not implement adequate controls to protect its information resources.

Hartsville/Trousdale County Government Executive and  
Board of County Commissioners  
November 17, 2005  
Page 2

**SHERIFF**

1. The office did not have formal policies and procedures for computer operations.
2. The office did not develop a disaster recovery plan.
3. The office had deficiencies in computer system back-up procedures.

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 Hartsville/Trousdale County Government, Tennessee.

Sincerely,



Richard V. Norment  
Assistant to the Comptroller

RVN: pa

Attachment

cc: The Honorable Charles Beasley, Highway Superintendent  
The Honorable Margaret Oldham, Director of Schools  
The Honorable Kay Celsor, Trustee  
The Honorable Mary Holder, Register  
The Honorable Ray Russell, Sheriff  
Mr. Kenny Patterson, Water and Sewer Department Director  
Mr. Carl Lowe, Mid-East Tennessee Audit Manager

**HARTSVILLE/TROUSDALE COUNTY GOVERNMENT, TENNESSEE  
REVIEW OF INTERNAL CONTROLS REGARDING INFORMATION  
SYSTEM OPERATIONS — FINDINGS AND RECOMMENDATIONS  
AS OF SEPTEMBER 22, 2005**

The review of controls over the information systems in the Offices of County Executive and Sheriff indicated a need for improvement. It should be noted that this was the first information system review performed in the Water and Sewer Department which is under the supervision of the Office of County Executive and 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 EXECUTIVE**

**RECOMMENDATIONS**

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

The following procedures regarding the system back-up process at the Water and Sewer Department should be implemented:

1. 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.
2. A current log of all backups that includes label descriptions, date of creation, contents, and storage location should be maintained.

**2. THE OFFICE SHOULD IMPLEMENT ADEQUATE CONTROLS  
TO PROTECT ITS INFORMATION RESOURCES**

The Water and Sewer Department should implement adequate controls to protect its information resources. 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.

## OFFICE OF SHERIFF

### RECOMMENDATIONS

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

Management should prepare a computer policies and procedures manual that defines 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. **THE OFFICE SHOULD DEVELOP A DISASTER RECOVERY PLAN**

Management 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.

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

The following procedures regarding the system back-up process should be implemented:

1. Management should store daily backups in a secure, fireproof location.
2. In addition to daily system backups, a weekly system backup should be performed, and two copies of this backup should be maintained. These backups should be rotated off site on a weekly basis.
3. 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.
4. A current log of all backups that includes label descriptions, date of creation, contents, and storage location should be maintained.