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

May 12, 2005

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

To the County Mayor and County Commissioners:

In conjunction with the annual audit of White County, we have performed a limited review of the information systems in the Offices of Trustee, County Clerk, Circuit and General Sessions Courts Clerk, Clerk and Master, Register, Sheriff, and Finance Director as of April 7, 2005. This letter transmits the results of our review.

Our audit of White 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 Trustee, Circuit and General Sessions Courts Clerk, Clerk and Master, Register, and Finance Director did not reveal any matters that we considered to be a reportable condition. Reportable conditions were identified in the Offices of County Clerk and Sheriff. These reportable conditions may be included in the annual financial report of White County. These matters are also presented in detail in the enclosed Review of Internal Controls Regarding Information System Operations — Findings and Recommendations.

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

COUNTY CLERK

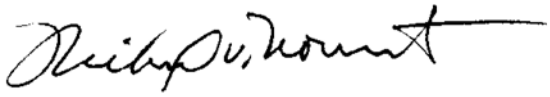
1. The office did not implement adequate controls to protect its information resources against unauthorized modification.

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.

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

Sincerely,



Richard V. Norment
Assistant to the Comptroller

RVN: pa

Attachment

cc: The Honorable Brenda Officer, Trustee
The Honorable Connie Jolley, County Clerk
The Honorable Henry Foster, Circuit and General Sessions Courts Clerk
The Honorable Lynda McCoy, Clerk and Master
The Honorable Gary Brogden, Register
The Honorable James O'Conner, Sheriff
Mr. Mark Farley, Finance Director
Mr. Carl Lowe, Mid-East Tennessee Audit Manager

WHITE COUNTY, TENNESSEE
REVIEW OF INTERNAL CONTROLS REGARDING INFORMATION SYSTEM OPERATIONS — FINDINGS AND RECOMMENDATIONS
AS OF APRIL 7, 2005

The review of controls over the information systems in the Offices of County Clerk and Sheriff indicated a need for improvement. It should be noted that this is the first information system review performed in the Office of Sheriff. The following finding and 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 a written response. We did not include oral responses in this report.

OFFICE OF COUNTY CLERK

THE OFFICE DID NOT IMPLEMENT ADEQUATE CONTROLS TO PROTECT ITS INFORMATION RESOURCES AGAINST UNAUTHORIZED MODIFICATION

1. **FINDING**

The office did not implement adequate controls to protect its information resources against unauthorized modification. The failure to provide such controls increases the risk that individuals could inappropriately access and manipulate the county's sensitive information.

This finding 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.

RECOMMENDATION

The office should ensure that adequate controls over information systems and the resources associated with those systems are implemented. Also, the office should take steps to establish or improve any compensating controls until these conditions are remedied.

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. SYSTEM BACK-UP PROCEDURES SHOULD BE IMPROVED

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

1. Daily system back-up procedures should be improved. A backup labeled for each day of the week should be maintained. These backups should be stored 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 complete systems backup should be performed at fiscal year-end. These backups should be stored off site.
4. 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.
5. 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 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 operations 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.

PRIOR AUDIT RECOMMENDATIONS NOT IMPLEMENTED

(Ref: Review of Internal Controls Regarding Information System Operations as of August 18, 2003)

OFFICE OF COUNTY CLERK

Finding Number	Page Number	Subject
1	1	The Office Did Not Implement Adequate Controls to Protect Its Information Resources Against Unauthorized Modification