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

June 28, 2006

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

To the County Mayor and Board of County Commissioners:

In conjunction with the annual audit of Jackson County, we have performed a limited review of the information systems in the Offices of County Mayor, Highway Superintendent, Director of Schools, County Clerk, Circuit and General Sessions Courts Clerk, Clerk and Master, Register, and Sheriff as of April 17, 2006. This letter transmits the results of our review.

Our audit of Jackson 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 County Mayor, Highway Superintendent, Director of Schools, County Clerk, Clerk and Master, Register, and Sheriff did not reveal any matters that we considered to be a reportable condition. Reportable conditions, however, were identified in the Office of Circuit and General Sessions Courts Clerk. These reportable conditions may be included in the annual financial report of Jackson 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 is presented below:

CIRCUIT AND GENERAL SESSIONS COURTS CLERK

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

Sincerely,

Richard V. Norment
Assistant to the Comptroller

RVN: pa

Attachment

cc: The Honorable Thomas E. Anderson, Highway Superintendent
The Honorable Joe Barlow, Director of Schools
The Honorable Belinda Ward, County Clerk
The Honorable Aaron Thomas, Circuit and General Sessions Courts Clerk
The Honorable Sherrie Osborne, Clerk and Master
The Honorable Kim Barham, Register
The Honorable Kenneth Bean, Sheriff
Mr. Carl Lowe, Mid-East Tennessee Audit Manager

JACKSON COUNTY, TENNESSEE
REVIEW OF INTERNAL CONTROLS REGARDING INFORMATION SYSTEM OPERATIONS — FINDINGS AND RECOMMENDATIONS AS OF APRIL 17, 2006

The review of controls over the information system in the Office of Circuit and General Sessions Courts Clerk indicated a need for improvement. The following findings and recommendations have been made to aid this office in the implementation of controls to better secure its computer system 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 CIRCUIT AND GENERAL SESSIONS COURTS CLERK

THE OFFICE DID NOT HAVE FORMAL POLICIES AND PROCEDURES FOR COMPUTER OPERATIONS

1. **FINDING**

The office did not have written policies and procedures for routine computer operations. Routine operations include system startup/shutdown, application access, system access security, system backup and retention schedules, hardware/software maintenance, output distribution, and other general data processing functions. Formal policies and procedures are necessary to ensure adequate management control over computer operations.

RECOMMENDATION

Management should prepare a computer policies and procedures manual that defines policies and procedures for operations such as system backups, security measures, and other general data processing functions. Upon completion, the manual should be distributed to all appropriate personnel.

THE OFFICE HAD DEFICIENCIES IN COMPUTER SYSTEM BACK-UP PROCEDURES

2. **FINDING**

The following weaknesses regarding computer system back-up procedures in the office were identified:

A. Daily backups were not stored in a secure location. Unsecured access to system backups exposes the data to environmental hazards, as well as to possible sabotage.

B. System backups were not stored off site. In the event of a disaster, all back-up data could be destroyed, resulting in costly delays in generating and recording information accounted for through the automated process.

C. A back-up log was not maintained. If system backups are not labeled and inventoried systematically, discrepancies may occur and affect the integrity of system backups in the event of a hardware or software failure.

RECOMMENDATION

Management should store daily backups in a secure, fireproof location. Weekly backups should be rotated off site on a weekly basis. Year-end backups should be stored off site and retained indefinitely. 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.

THE OFFICE DID NOT DEVELOP A DISASTER RECOVERY PLAN

3. FINDING

The office did not develop a disaster recovery plan to assist in re-creating its data processing environment in the event of a disaster. Without a formal, written plan, critical computerized applications could be disrupted indefinitely until the system could be repaired or a back-up facility could be found and made operational.

RECOMMENDATION

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 September 15, 2004)

OFFICE OF CIRCUIT AND GENERAL SESSIONS COURTS CLERK

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

PRIOR AUDIT RECOMMENDATIONS IMPLEMENTED

(Ref: Review of Internal Controls Regarding
Information System Operations as of September 15, 2004)

OFFICE OF COUNTY MAYOR

Finding Number	Page Number	Subject
1	1	Management should formally document policies and procedures for computer operations
2	1	The office should implement controls to protect its information resources
3	1	The office should develop a disaster recovery plan

OFFICE OF SHERIFF

Finding Number	Page Number	Subject
1	3	Management should formally document policies and procedures for computer operations
2	3	System back-up procedures should be improved
3	4	The office should develop a disaster recovery plan