



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

December 4, 2006

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

To the County Mayor and County Commissioners:

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

Our audit of Bedford 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 Highway Superintendent; Director of Schools; Trustee; County Clerk; Circuit, General Sessions, and Juvenile Courts Clerk; and Register did not reveal any matters that we considered to be reportable conditions. Reportable conditions were identified in the Offices of County Mayor and Sheriff. These reportable conditions may be included in the annual financial report of Bedford 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 office had deficiencies in computer system back-up procedures.
2. The office did not implement adequate controls to protect its information resources.

Bedford County Mayor and
Board of County Commissioners
December 4, 2006
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.

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 Bedford County, Tennessee.

Sincerely,



Richard V. Norment
Assistant to the Comptroller

RVN: pa

Attachment

cc: The Honorable Stanley Smotherman, Highway Superintendent
The Honorable Ed Gray, Director of Schools
The Honorable Peggy Bush, Trustee
The Honorable Kathy Prater, County Clerk
The Honorable Thomas Smith, Circuit, General Sessions, and Juvenile Courts Clerk
The Honorable John Reed, Register
The Honorable Randall Boyce, Sheriff
Mr. Jeff Bailey, Middle Tennessee Audit Manager

BEDFORD COUNTY, TENNESSEE
REVIEW OF INTERNAL CONTROLS REGARDING INFORMATION
SYSTEM OPERATIONS - FINDINGS AND RECOMMENDATIONS
AS OF NOVEMBER 17, 2006

The review of controls over the information systems in the Offices of County Mayor and Sheriff indicated a need for improvement. The following findings 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 written responses. We did not include the oral responses in this report.

OFFICE OF COUNTY MAYOR

THE OFFICE HAD DEFICIENCIES IN COMPUTER
SYSTEM BACK-UP PROCEDURES

1. FINDING

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

- A. Daily backups were not performed on a routine basis. Inadequate back-up procedures could result in the loss of data in the event of a hardware or software failure. Without current backups, the cost of re-creating data could be substantial.
- B. Weekly and fiscal year-end backups were not performed on a regular basis. These backups would ensure the restoration of system data if problems occurred.
- C. System backups were not stored in a secure off-site location. 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.
- D. 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 implement daily system back-up procedures. A backup labeled for each day of the week should be maintained. Management should store these backups in a secure, fireproof location. 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. A complete systems backup should also be performed at fiscal year-end. These year-end backups should be stored off site and retained for three years. 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 IMPLEMENT ADEQUATE CONTROLS
TO PROTECT ITS INFORMATION RESOURCES**

2. FINDING

The office did not implement adequate controls to protect its information resources. 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.

OFFICE OF SHERIFF

**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 DID NOT DEVELOP A DISASTER RECOVERY PLAN

2. 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 March 7, 2005)

OFFICE OF SHERIFF

Finding Number	Page Number	Subject
2	2	Management should formally document policies and procedures for computer operations
3	2	The office should develop a disaster recovery plan

PRIOR AUDIT RECOMMENDATIONS IMPLEMENTED

(Ref: Review of Internal Controls Regarding
Information System Operations as of March 7, 2005)

OFFICE OF COUNTY MAYOR

Finding Number	Page Number	Subject
1	1	The office had deficiencies involving its warrant-signing machine

OFFICE OF COUNTY MAYOR - AMBULANCE SERVICE

Finding Number	Page Number	Subject
1	1	The office should develop a disaster recovery plan

OFFICE OF SHERIFF

Finding Number	Page Number	Subject
1	2	System back-up procedures should be improved