



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

August 14, 2006

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

To the County Mayor and Board of County Commissioners:

In conjunction with the annual audit of Dyer County, we have performed a limited review of the information systems in the Offices of County Mayor, Road Supervisor, Director of Schools, Trustee, County Clerk, Circuit and General Sessions Courts Clerk, Clerk and Master, Register, and Sheriff as of July 26, 2006. This letter transmits the results of our review.

Our audit of Dyer 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, Road Supervisor, Director of Schools, Trustee, County Clerk, Clerk and Master, and Register did not reveal any matters that we considered to be a reportable condition. Reportable conditions, however, were identified in the Offices of Circuit and General Sessions Courts Clerk and Sheriff. These reportable conditions may be included in the annual financial report of Dyer 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:

CIRCUIT AND GENERAL SESSIONS COURTS CLERK

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

Dyer County Mayor and
Board of County Commissioners
August 14, 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.
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 Dyer County, Tennessee.

Sincerely,



Richard V. Norment
Assistant to the Comptroller

RVN: pa

Attachment

cc: The Honorable Jeff Jones, Road Supervisor
The Honorable Dwight Hedge, Director of Schools
The Honorable Judy Patton, Trustee
The Honorable Diane Moore, County Clerk
The Honorable Tom Jones, Circuit and General Sessions Courts Clerk
The Honorable John Hoff, Clerk and Master
The Honorable Danny Fowlkes, Register
The Honorable Jeff Holt, Sheriff
Mr. Norm Norment, West Tennessee Audit Manager

DYER COUNTY, TENNESSEE
REVIEW OF INTERNAL CONTROLS REGARDING INFORMATION
SYSTEM OPERATIONS — FINDINGS AND RECOMMENDATIONS
AS OF JULY 26, 2006

The review of controls over the information systems in the Offices of Circuit and General Sessions Courts Clerk and Sheriff indicated a need for improvement. It should be noted that this was the first information system review performed in the Office of Sheriff. 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. The oral responses have not been included in this report.

OFFICE OF CIRCUIT AND GENERAL SESSIONS COURTS CLERK

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. Weekly backups were not performed. These backups would ensure the restoration of system data if problems occurred.
- 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

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. 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. 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. 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. 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.

3.

SYSTEM BACK-UP PROCEDURES SHOULD BE IMPROVED

A backup labeled for each day of the week should be maintained. In addition to daily system backups, a weekly system backup should be performed. 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.