

Department of Personnel

**For the Year Ended
June 30, 1996**

Arthur A. Hayes, Jr., CPA

Director

Charles K. Bridges, CPA

Assistant Director

Debra D. Bloomingburg, CPA

Audit Manager

Patricia L. Wakefield, CPA

In-Charge Auditor

Kris Birdine

Jim Collums

Bob Rice, CISA

Britt Wood

Staff Auditors

Leslie Bethea

Editor

June 23, 1997

The Honorable Don Sundquist, Governor
and
Members of the General Assembly
State Capitol
Nashville, Tennessee 37243
and
The Honorable Eleanor E. Yoakum, Commissioner
Department of Personnel
Second Floor, James K. Polk Building
505 Deaderick Street
Nashville, Tennessee 37243

Ladies and Gentlemen:

We have conducted a financial and compliance audit of selected activities of the Department of Personnel for the year ended June 30, 1996.

We conducted our audit in accordance with generally accepted government auditing standards. These standards require that we obtain an understanding of management controls relevant to the audit and that we design the audit to provide reasonable assurance of the Department of Personnel's compliance with the provisions of laws, regulations, contracts, and grants significant to the audit. Management of the Department of Personnel is responsible for establishing and maintaining the internal control structure and for complying with applicable laws and regulations.

Our audit disclosed a finding which is detailed in the objectives, methodologies, and conclusions section of this report. The department's administration has responded to the audit finding; we have included the response following the finding. We will follow up the audit to examine the application of the procedures instituted because of the audit finding.

We have reported other less significant matters involving the department's internal controls and/or instances of noncompliance to the Department of Personnel's management in a separate letter.

Very truly yours,

W. R. Snodgrass
Comptroller of the Treasury

WRS/cr
97/063

State of Tennessee

Audit Highlights

Comptroller of the Treasury

Division of State Audit

Financial and Compliance Audit
Department of Personnel
For the Year Ended June 30, 1996

AUDIT SCOPE

We have audited the Department of Personnel for the period July 1, 1995, through June 30, 1996. Our primary focus was on management's controls and compliance with policies, procedures, laws, and regulations in the areas of expenditures and equipment. The audit was conducted in accordance with generally accepted government auditing standards.

AUDIT FINDING

Inadequate Protection of Datasets

The State Employees Information System datasets were not adequately protected by the state's computer security system. These datasets contain the employee database, social security history, payroll codes database, payroll report database, and position history database, along with other information. Failure to maintain adequate system security could allow these datasets to be improperly updated, altered, or destroyed (page 5).

"Audit Highlights" is a summary of the audit report. To obtain the complete audit report which contains all findings, recommendations, and management comments, please contact

Comptroller of the Treasury, Division of State Audit
1500 James K. Polk Building, Nashville, TN 37243-0264
(615) 741-3697

Audit Report
Department of Personnel
For The Year Ended June 30, 1996

TABLE OF CONTENTS

	<u>Page</u>
INTRODUCTION	1
Post-Audit Authority	1
Background	1
AUDIT SCOPE	2
OBJECTIVES, METHODOLOGIES, AND CONCLUSIONS	2
Expenditures	2
Equipment	4
EDP Review	4
Finding - The State Employees Information System datasets were not adequately protected	5
PRIOR AUDIT FINDINGS	6
Resolved Audit Findings	6
APPENDICES	7
Divisions and Allotment Codes	7
Charts (Unaudited)	
Funding Sources—Fiscal Year Ended June 30, 1996	8
Expenditures by Allotment and Division—Fiscal Year Ended June 30, 1996	8
Funding Sources—Fiscal Year Ended June 30, 1995	9
Expenditures by Allotment and Division—Fiscal Year Ended June 30, 1995	9

Department of Personnel For The Year Ended June 30, 1996

INTRODUCTION

POST-AUDIT AUTHORITY

This is the report on the financial and compliance audit of the Department of Personnel. The audit was conducted pursuant to Section 4-3-304, *Tennessee Code Annotated*, which authorizes the Department of Audit to “perform currently a post-audit of all accounts and other financial records of the state government, and of any department, institution, office, or agency thereof in accordance with generally accepted auditing standards and in accordance with such procedures as may be established by the comptroller.”

Section 8-4-109, *Tennessee Code Annotated*, authorizes the Comptroller of the Treasury to audit any books and records of any governmental entity that handles public funds when the Comptroller considers an audit to be necessary or appropriate.

BACKGROUND

The department, one of the staff agencies of the executive branch, is under the Commissioner of Personnel. The department serves in an advisory capacity to the Governor, assisting him in formulating and executing all personnel policies and procedures for employees in state service and applicants for positions. It administers the provisions of the Civil Service Act, prescribes rules and regulations governing state employees, and strives to establish a modern and effective system of personnel management. It also coordinates the Governor’s Affirmative Action Plan, which ensures that women and all minority persons are given an opportunity for equal employment in all state agencies in the executive branch. The department comprises the Divisions of Technical Services, Human Resources, and Executive Administration.

Technical Services Division - This division is responsible for maintaining state personnel records, administering civil service examinations, monitoring the civil service appointment process, and auditing the state payroll.

Human Resources Division - This division is responsible for coordinating and conducting training courses for state employees, implementing the state’s affirmative action program, and supporting employee relations. It administers the state employee Sick Leave Bank, coordinates the state’s Employee Suggestion Program, provides administrative support for the Civil Service Commission, and ensures compliance with provisions of the Americans with Disabilities Act.

Executive Administration Division - This division is responsible for the fiscal management of the department and for developing and maintaining technically sound personnel management programs to assist state managers and supervisors. This division is represented by the commissioner, who also serves as secretary to the Civil Service Commission.

An organization chart of the department is on the following page.

AUDIT SCOPE

We have audited the Department of Personnel for the period July 1, 1995, through June 30, 1996. Our primary focus was on management's controls and compliance with policies, procedures, laws, and regulations in the areas of expenditures and equipment. The audit was conducted in accordance with generally accepted government auditing standards.

OBJECTIVES, METHODOLOGIES, AND CONCLUSIONS

EXPENDITURES

The objectives of our review of the expenditures controls and procedures in the Department of Personnel were to determine whether

- the department used direct purchase authority in accordance with applicable guidelines, and
- the department performed and documented reconciliations of contract payments with the State of Tennessee Accounting and Reporting System (STARS).

We interviewed key department personnel to gain an understanding of the department's procedures and controls over the use of its direct purchase authority and over the reconciliation of contract payments with STARS. We also reviewed supporting documentation and tested payments made using the department's direct purchase authority. We had no findings related to expenditures.

EQUIPMENT

The objectives of our review of the equipment controls and procedures in the Department of Personnel were to determine whether

- the department located and deleted from the Property of the State of Tennessee system (POST) equipment included on the POST Exception Report, and
- the department conducted an annual inventory of equipment leased from the Office of Information Resources (OIR) and submitted the results to OIR.

We interviewed key department personnel to gain an understanding of the department's procedures and controls over the inventory of equipment owned by the department and over equipment leased from OIR. We reviewed supporting documentation and tested nonstatistical samples of equipment included on the POST Exception Report and equipment leased from OIR. We had no findings related to equipment.

EDP REVIEW

As part of the audit of the state's Comprehensive Annual Financial Report (CAFR), we reviewed the controls and procedures over the State Employees Information System (SEIS). The objective of the CAFR was to render an opinion on the State of Tennessee's general-purpose financial statements. As part of our audit of the CAFR, we are required to gain an understanding of the state's internal control structure and determine whether the state complied with laws and regulations that have a material effect on the state's general-purpose financial statements. To address the objective of the audit of the CAFR, we interviewed key department employees, reviewed applicable policies and procedures, and tested representative samples of transactions. In the process of gaining an understanding of the internal controls, we found that SEIS datasets were not adequately protected from unauthorized access by the security system that protects programs and data files on the State's central computer system as discussed in the following finding.

The State Employees Information System datasets were not adequately protected

Finding

Resource Access Control Facility (RACF) is the security system that protects programs and data files on the state's central computer system. Though RACF was designed to protect employee information, the "WARNING" specification was set to "YES." Even though the "YES" setting warns the user that access is not authorized and sends a warning message to the security administrator's log, the system then gives the user access to the datasets. These datasets contain the employee database, social security history, the payroll codes database, the payroll report database, the position history database, and other information. A RACF "WARNING" specification of "YES" is normally used temporarily to test and verify access when an application is first installed or has been extensively modified. However, the "YES" specification is inappropriate for an established system such as the State Employee Information System (SEIS) because it can permit unauthorized access to the datasets.

The SEIS security administrator is employed by the Department of Personnel even though the payroll is administered by the Department of Finance and Administration. Regardless of organizational structure, good information system management requires that datasets be protected against unauthorized access. Failure to maintain adequate system security could allow improper updates, alterations, or destruction of datasets.

Recommendation

The Department of Personnel's management should ensure that the SEIS security administrator sets the RACF "WARNING" specification to "NO" for these datasets. In addition, the security administrator should ensure that RACF security is promptly and fully activated when data systems are installed. The security administrator should also continue to ensure that RACF security is appropriately maintained and periodically reviewed for proper access controls over the department's datasets.

Management's Comment

We concur. The Department has implemented the recommendations to protect the State Employee Information System (SEIS) datasets.

The RACF warning specification for the SEIS datasets are now all set to "NO". In addition, the security administrator will ensure that all new applications have the proper RACF security installed before implementation. The RACF security file has been reviewed and is currently up-to-date. The security administrator will maintain this file as new appointments and separations occur and perform periodic reviews as necessary.

PRIOR AUDIT FINDINGS

Section 8-4-109, *Tennessee Code Annotated*, requires that each state department, agency, or institution report to the Comptroller of the Treasury the action taken to implement the recommendations in the prior audit report. The Department of Personnel is scheduled to file its report with the Department of Audit on March 1, 1997. A follow-up of all prior audit findings was conducted as part of the current audit.

RESOLVED AUDIT FINDINGS

The current audit disclosed that the Department of Personnel has corrected previous audit findings concerning compliance with its direct purchase authorization and reconciliation of contract payments with STARS reports, and compliance with the Department of Finance and Administration's policy on reviewing long distance telephone calls.

APPENDICES

DIVISIONS AND ALLOTMENT CODES

Department of Personnel divisions and allotment codes:

319.01	Division of Executive Administration
319.02	Division of Human Resources
319.03	Division of Technical Services
319.99	Sick Leave Bank

