New Jersey State Legislature
Office of Legislative Services
Office of the State Auditor

Department of the Treasury
Office of Telecommunications and Information Systems
Division of Taxation's Computer Systems (TAXNET)

October 1, 1997 to June 9, 1998

Richard L. Fair
State Auditor

LEGISLATIVE SERVICES COMMISSION

SENATOR
DONALD T. DiFRANCESCO
Chairman

ASSEMBLYMAN
JACK COLLINS
Vice-Chairman

SENATE

BYRON M. BAER
JOHN O. BENNETT
GERALD CARDINALE
RICHARD J. CODEY
WYNONA M. LIPMAN
ROBERT E. LITTELL
JOHN A. LYNCH

GENERAL ASSEMBLY

JOSEPH CHARLES, JR.
PAUL DIGAETANO
JOSEPH V. DORIA, JR.
NICHOLAS R. FELICE
NIA H. GILL
LEONARD LANCE
LORETTA WEINBERG

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

ALBERT PORRONI
Executive Director
(609) 292-4625

RICHARD L. FAIR
State Auditor
(609) 292-3700
FAX (609) 633-0834

The Honorable Christine Todd Whitman
Governor of New Jersey

The Honorable Donald T. DiFrancesco
President of the Senate

The Honorable Jack Collins
Speaker of the General Assembly

Mr. Albert Porroni
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Division of Taxation's Computer Systems (TAXNET) for the period October 1, 1997 to June 9, 1998. The systems are operated by the Office of Telecommunications and Information Systems within the Department of the Treasury.

If you would like a personal briefing, please call me at (609) 292-3700.

Richard L. Fair
State Auditor
July 17, 1998

Table of Contents

Page

Scope 1

Objectives 2

Methodology 2

Conclusions 2

Findings and Recommendations

System Security

System Access 3

System Monitoring 3

User Authorization 4

Operational Continuity 5

Department of the Treasury
Office of Telecommunications and Information Systems
Division of Taxation's Computer Systems (TAXNET)

Scope

We have completed an audit of the Division of Taxation's Computer Systems (TAXNET) for the period October 1, 1997 to June 9, 1998. Our audit evaluated application controls and general controls over operational continuity and year 2000 readiness involved in the processing of taxation data.

TAXNET is a compilation of mainframe data systems developed during the 1980's. The premise behind the various components was to develop an integrated tax administration environment. The most significant components are as follows:

- Taxation Unremitted Liability Inventory Plotting System (TULIPS). TULIPS is the division's case tracking system. It is used to provide caseworkers with a consolidated view of taxpayer liabilities, generate taxpayer notifications, and provide management with various activity reports. TULIPS interfaces with the other components of TAXNET and provides a consolidation of taxpayer information.

- Generic Tax Systems (GENTS). GENTS contains the detail return and monetary transaction information for each tax. GENTS provides for on-line, real-time updates. The system is used to perform batch and transaction edit corrections, as well as generating billing notifications.

- Taxpayer Registration System (TAXREG). TAXREG was developed to replace the Unified Taxpayer File for businesses and Taxpayer Gross Income for individuals. TAXREG is used to generate the mailing of tax returns based upon tax eligibilities, identify taxpayers that have not filed returns, and provide address information for the division mailings.

Objectives

The objectives of our audit were to determine the adequacy of application controls and certain general controls in place related to asset safeguarding, taxpayer data processing, and access to system data.

This audit was conducted pursuant to the State Auditor's responsibilities as set forth in Article VII, Section 1, Paragraph 6 of the State Constitution and Title 52 of the New Jersey Statutes.

Methodology

Our audit was conducted in accordance with *Government Auditing Standards* issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by *Assessing the Reliability of Computer-Processed Data* issued by the United States General Accounting Office and *Auditing Computer Applications* issued by Auerbach.

In preparation for our testing, we studied system user, operation, and facility guides, circular letters promulgated by the State Comptroller, and policies of the Division of Taxation. Provisions that we considered significant were documented and compliance with those requirements was verified by interview and observation and through our sampling of system transactions.

A nonstatistical sampling approach was used. Our samples of access privileges were designed to provide conclusions about the security of the data and internal control attributes.

Conclusions

Our audit disclosed that controls in place related to the computer processing of taxpayer data, access to system data, and the safeguarding of assets are adequate. In making this determination, we noted certain internal control weaknesses meriting management's attention.

System Security

SYSTEM ACCESS

Improvements to current internal controls can reduce the risk of unauthorized transactions or access.

The current authorization process used to grant access for TAXNET applications dictates that the section supervisors obtain access through the Office of Technical Support (OTS). The OTS procedures do not require a review to determine if conflicts exist between users' privileges and their official responsibilities. We noted individuals whose duties require them to receive cash payments and who have system privileges allowing the adjustment of account balances for which the cash was received.

The final responsibility for determining what access is granted to whom rests with the supervisors. However, the requesting individual may not be aware or disregards that the specific access requested creates a possible conflict.

Recommendation

We recommend that the division institute procedures requiring the supervisors to review the requested access to TAXNET applications and the users' job functions to determine whether conflicts exist, and certify the access is appropriate.

Auditee's Response

The Division has modified the procedure for requesting system access. A standardized form has been established, requiring that the supervisor sign the request verifying that the request has been reviewed and is appropriate. The form will be available for distribution and the new method implemented August 1, 1998.

SYSTEM MONITORING

OTS procedures do not require the periodic monitoring of ACF2 logon violations. The unit receives daily online reports which detail all failed logon attempts. The data is voluminous and may account for the lack of review. Good security procedures require that violation reports be reviewed. Even though logon failures

pose no threat to system data, repeated failures may indicate unauthorized attempts.

Recommendation

We recommend that OTS enact procedures to resume the systematic review of ACF2 logon violations.

Auditee's Response

While this report is not considered a productive indicator of attempted security breaches, analysis of the structure of the logon violation report is currently underway. Changes will be developed which will make periodic review of this report feasible. Systematic review will commence as modifications to this report are completed.

USER AUTHORIZATION

The GENTS User Authorization File contains the security entries that determine a user's system access privileges within the application. Our review disclosed that six individuals in OTS have the authority to update user security profiles, including their own. One of these individuals also performs transaction edits and updates on the GENTS system. This could allow the processing of improper transactions with a reduced probability of detection.

As a result of discussions with management, the number of employees within OTS that have the ability to grant update authority for GENTS conversations through the User Authorization File has been reduced to two.

Recommendation

We recommend that, in addition to the above modifications, the division devise policies and procedures limiting the number of individuals with this high level of authority. The policy should state that, as situations arise requiring additional employees to have this authority level, it should be for a limited time only. The ability to modify authorization privileges within the application should also be limited to those individuals who cannot also perform online transactions.

Auditee's Response

As detailed in the audit report, the ability to grant update authority for GENTS conversations has been reduced to two individuals. The policy within OTS now limits the number of employees with this access to two, with any requested exceptions require to be submitted for approval to the Chief, Office of Technical Support. This written request must include the justification for the access as well as the intended duration. In addition, any employee with the ability to assign or modify user authorization privileges will not be authorized to perform on-line transactions.

Thank you for the opportunity to respond and include our comments with your audit report.

Operational Continuity

OTIS needs to test its disaster recovery plan to assure continued processing in the event of a disaster at its data center.

The Office of Telecommunications and Information Systems (OTIS) Technical Service Standardization Plan states that a disaster recovery plan must be exercised at each OTIS data center at least once a year to ensure that it will in fact satisfy a site's processing requirements. The functions of such tests are to determine the ability to recover key processing components based on a documented set of instructions and assure that the measures in place will in fact enable recovery. OTIS has not performed a test of its disaster recovery plan for the TAXNET applications. One of the primary causes of this is the lack of sufficient resources. This condition was noted in our prior report on the River Road and Barrack Street Data Centers. The processing of tax revenues would be seriously hampered if the TAXNET applications were not operational.

Recommendation

We recommend management provide the necessary capacity to allow for the testing of the disaster recovery plan for TAXNET applications in compliance with their Technical Service Standardization Plan.