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

Department of Treasury
Division of Taxation
Public Access Systems

December 10, 2001 to July 31, 2002

Richard L. Fair
State Auditor

LEGISLATIVE SERVICES COMMISSION

SENATE
BYRON M. BAER
JOHN O. BENNETT
ANTHONY R. BUCCO
RICHARD J. CODEY
NIA H. GILL
BERNARD F. KENNY, JR.
ROBERT E. LITTELL
ROBERT W. SINGER

GENERAL ASSEMBLY
PETER J. BIONDI
FRANCIS J. BLEE
ALEX DECROCE
PAUL DIGAETANO
JOSEPH V. DORIA, JR.
JOSEPH J. ROBERTS, JR.
ALBIO SIRES
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 James E. McGreevey
Governor of New Jersey

The Honorable John O. Bennett
President of the Senate

The Honorable Richard J. Codey
President of the Senate

The Honorable Albio Sires
Speaker of the General Assembly

Mr. Albert Porroni
Executive Director
Office of Legislative Services

Enclosed is our report on the audit of the Department of Treasury, Division of Taxation, Public Access Systems for the period December 10, 2001 to July 31, 2002.

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

Richard L. Fair
State Auditor

December 11, 2002

Table of Contents

Page

Department of Treasury
Division of Taxation

Scope

We have completed an audit of the Department of the Treasury, Division of Taxation - Public Access Systems for the period December 10, 2001 through July 31, 2002. Our audit evaluated selected application and general controls related to the automated systems available to taxpayers through the internet or the telephone. The application and general controls reviewed included those in place for transaction processing data integrity, data security, and application maintenance.

The prime responsibility of the Department of the Treasury, Division of Taxation is the administration of the State's tax laws, which includes ensuring compliance, collecting taxes, and providing assistance. Therefore, the division has increased taxpayer convenience by offering automated options to file returns or applications, pay tax liabilities, inquire as to refund or rebate status, and view account information. This has been accomplished through the deployment of various internet and telephone-based systems.

Objectives

The objectives of the audit were to determine the adequacy of selected application controls over transaction processing data integrity and selected general controls over data security and application maintenance.

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 *Federal Information System Controls*

Audit Manual issued by the United States General Accounting Office and *Control Objectives for Information and Related Technology* issued by the Information Systems Audit and Control Foundation.

In preparation for our testing, we studied legislation, administrative code, circular letters promulgated by the State Comptroller, and policies of the agency. Provisions that we considered significant were documented and compliance with those requirements was verified by interview, observation, and through our samples of transactions. We also interviewed agency personnel to obtain an understanding of the programs and the internal controls.

A nonstatistical sampling approach was used. Our tests of application and general controls were designed to provide conclusions about the adequacy of those controls in place for transaction processing data integrity, data security, and application change management. Sample transactions were judgmentally selected for testing.

Conclusions

Our review disclosed that while selected application controls were in place for transaction processing data integrity, the selected general controls for data security and application maintenance require improvements.

System Documentation / Change Management

Adequate system documentation should be maintained.

An understanding of an application's functionality and operational relationships requires sufficient system documentation and consistently documented application maintenance. Developing and maintaining application software is enabled by the definition of functional and operational requirements. These include: input, processing, and output; platform interfaces; and application controls and security requirements. Managing application software changes is accomplished by a system that identifies and tracks changes made to the existing architecture. This minimizes the likelihood of disruption, unauthorized alterations and errors.

The division does not maintain system documentation identifying the information architecture supporting its public access systems. Additionally, procedures governing all phases of the change management process for its public access systems are not formalized.

Recommendation

The division should require the development and maintenance of adequate system documentation identifying the information architecture for its public access systems. In addition, the division should establish written application software change procedures and require their use.

Auditee's Response

The Division does have an established procedure for change requests once an application is put into production. A written request for data processing services (SPPC Request) is prepared and submitted to OIT for completion. There are instances; related to emergency requests; where changes are accomplished without using the full documentation usually required.

The procedures for the development of an Internet application also includes a formal initial request.

However, much of the detail design and/or subsequent changes that occur during the development effort are established during meetings or through email and telephone conversations between the appropriate analysts within Taxation and OIT. In the interest of efficiency, these additions to the initial request are often not formalized.

The Division of Taxation will review the System Documentation/Change Management and Interface Program Security recommendation with OIT management with the goal of improving the documentation.

⋙➤◂⋘

Interface Program Security

Confidential data on the state's internet web server is available to employees not requiring access.

While appropriate controls prevent the alteration of recorded data, confidential data stored on the state's internet web server is readily transferable to unauthorized platforms by various state employees. This information includes taxpayer identification numbers and personal identification numbers (PINs) used to control access to available taxation internet services.

The web server's internal internet protocol (IP) address, and the user identification and password used to transmit data between systems both appear in clear text in jobs and so are available to all employees with access to these jobs. After being granted access to the state's internal network, we used this IP address and user identification to obtain unauthorized access to taxpayer identification numbers and PINs. Using this information, we were able to obtain electronic filer bank routing and account numbers through the division's internet application.

Recommendation

The division should require that the web server IP address and related user identification be properly

safeguarded through placement in a secured library with limited access.

Auditee's Response

The Division should required that the web server IP address and related user identification be properly safeguarded through placement in a secured library with limited access.

The Division also reviewed this recommendation with OIT with the goal being implementation of the recommendation.