Department of Labor and Workforce Development
Tax Revenue Systems

May 26, 2005 to February 28, 2006

Richard L. Fair
State Auditor
The Honorable Jon S. Corzine  
Governor of New Jersey

The Honorable Richard J. Codey  
President of the Senate

The Honorable Joseph J. Roberts, Jr.  
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 Labor and Workforce Development, Tax Revenue Systems for the period of May 26, 2005 to February 28, 2006. If you would like a personal briefing, please call me at (609) 292-3700.

James B. Patterson  
Assistant State Auditor  
July 17, 2006
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Objectives</td>
<td>1</td>
</tr>
<tr>
<td>Methodology</td>
<td>1</td>
</tr>
<tr>
<td>Conclusions</td>
<td>2</td>
</tr>
<tr>
<td>Overview</td>
<td>2</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>IT Planning</td>
<td>3</td>
</tr>
<tr>
<td>Service Continuity</td>
<td>4</td>
</tr>
<tr>
<td>Prior Audit Compliance (Security)</td>
<td>5</td>
</tr>
<tr>
<td>Auditee's Response</td>
<td>7</td>
</tr>
</tbody>
</table>
Department of Labor and Workforce Development
Tax Revenue Systems

Scope

We have completed an audit of the Department of Labor and Workforce Development, Tax Revenue Systems for the period May 26, 2005 to February 28, 2006. Our audit evaluated selected general controls related to these systems. The controls tested were information technology (IT) system planning and management, service continuity planning and validation, and information security administration and implementation.

Objectives

The objectives of the audit were to determine the adequacy of general controls over IT system planning and management, service continuity planning and validation, and information security administration and implementation. We also tested for resolution of the significant conditions noted in our prior report dated July 24, 2001.

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 conduct of the audit was provided by Control Objectives for Information and Related Technology issued by the IT Governance Institute.

In preparation for our testing, we studied 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. In addition, we obtained and reviewed the department’s administrative directives and procedures related to information technology.
Functions that we considered significant were documented and implementation of those processes was verified. We also interviewed agency personnel to obtain an understanding of the internal controls and to determine compliance with prior audit recommendations.

A nonstatistical sampling approach was used. Our tests of general controls were designed to provide conclusions about the adequacy of those controls in place for IT system planning and management, service continuity planning and validation, and information security administration and implementation. Sample transactions were judgmentally selected for testing.

**Conclusions**

Although our review disclosed that the selected general controls for IT system planning and management, and service continuity planning and validation were adequate, we noted certain items requiring improvement. In addition, prior audit reportable conditions related to information security administration and implementation still exist and require improvement.

**Overview**

The Tax Revenue Systems collect the wage data used to determine unemployment benefit eligibility, and record the employer and worker contributions used to fund the unemployment and the disability insurance programs. This data is also used to develop the employer experience rates which determine the amount of unemployment contributions by employers. We reviewed selected general controls for these systems.

General controls are those which apply to all or a large segment of an entity’s information systems to help ensure their proper operation. General controls related to the Tax Revenue Systems are primarily administered at the department level. The development and maintenance of these controls is the responsibility of the Division of Information Technology.
IT Planning

A critical success factor for managing IT projects is the development of, documentation of, and adherence to a plan. A sound project plan takes into consideration task breakdowns, cost and manpower budgets, and defines processes for quality assurance and for the transition from development to production. Short and long-term planning for the Employer Accounts System (EAS) is not adequate.

Inadequate planning has resulted in the delay of an upgrade in the data base management system and in the implementation of developed user interface enhancements for the EAS. Costs have been continuously incurred without achievement of an ultimate outcome as of the end of our audit period. The installation of a server acquired to improve processing capability was also delayed for one year. This delay was due to inadequate electrical and uninterruptible power supply capacity available at the department’s data center. The estimated server maintenance and software license costs paid for this period of inactivity was $131,000. Outside consultant costs incurred from fiscal years 2002 to 2005 for system maintenance and for the pending migration of the system’s data base management system version upgrade is estimated to be $3.4 million. In addition, program maintenance costs for active ongoing service requests to correct or enhance the EAS provided by the State’s Office of Information Technology (OIT) are estimated to be approximately $1.6 million. Furthermore, the estimated costs of user interface enhancements individually completed by an outside consultant and by OIT in calendar year 2003 were approximately $410,000 and $351,000, respectively. The completion of these projects before the data base management system upgrade will require retesting prior to implementation. The delayed migration of the data base management system upgrade also played a
significant part in prolonging the correction of known security deficiencies inherent to the older version.

**Recommendation**

A plan identifying short and long-term task breakdowns, cost and manpower budgets, and defining processes for quality assurance and for the transition from development to production should be prepared, documented, and followed. The development and maintenance of this plan should be performed by the department’s Division of Information Technology.

---

**Service Continuity**

An incomplete IT continuity plan could result in a prolonged recovery of critical business applications in the event of the loss of the department’s data center. The business processes supported by the Employer Accounts System (EAS) would experience indefinite interruption and employer account information would be inaccessible.

The ability to ensure continuous service is enabled by having an operational IT continuity plan. A reliable continuity plan documents external organizational responsibilities and modifications based on the results of regular testing. The continuity plan for the EAS does not provide for an alternate processing facility and test executions of the plan have not been performed.

**Recommendation**

The IT continuity plan should identify and contain an agreement for an alternate processing facility. Periodic tests of the plan should also be conducted to ensure its adequacy.
Prior Audit Compliance (Security)

The Division of Employer Accounts has not resolved all issues disclosed in the previous audit dated July 24, 2001. Various conditions still exist regarding information security administration and implementation and user authentication.

An update of prior exceptions and the results of current sampling disclosed that 19 user accounts have not been removed even though the user is not a current employee or consultant; six users have multiple accounts, when only one should be provided; two group accounts have been provided to users instead of a user specified account; 39 users have been assigned privileges in excess of their specified need; ten users have been assigned privileges incompatible with their job responsibilities; and 36 user accounts have passwords equal to their user name.

An additional analysis of all user accounts as of January 2006 disclosed that of the 1,025 user accounts established, 308 user accounts have never been used and 226 user accounts have not accessed the system since calendar year 2001. User accounts no longer necessary, which diminish the security of the processed information, should be removed.

Management should monitor the effectiveness of security controls in the normal course of operations through management and supervisory activities and other routine operations. Privileges should be assigned in a manner that would reduce the possibility of a single individual undermining a critical business process. Passwords should be changed periodically to prevent guessing and to maintain confidentiality.

The division does not conduct periodic reviews of user rights. In addition, the division has not established an adequate segregation of duties between individuals responsible for system
support, administration, and information entry and use. Procedures to ensure the timely removal of user accounts are not followed. Limitations inherent to the current version of the data base management system inhibit the implementation of user password management.

**Recommendation**

Management should establish and maintain a control process to review and confirm access rights periodically and ensure compliance with established procedures. In addition, management should evaluate the options available with the upgraded version of the data base management system and implement those which ensure effective authentication and access mechanisms.
July 13, 2006

Mr. Richard L. Fair
State Auditor
Office of Legislative Services
Office of the State Auditor
125 South Warren Street
P.O. Box 067
Trenton, New Jersey 08625-0067

Dear Mr. Fair:

We have received your audit report titled "Department of Labor and Workforce Development Tax Revenue Systems" which covered the period May 26, 2005 to February 28, 2006.

The Employer Accounts System (EAS) is a very complex and large IT system which processes millions of transactions involving over 600,000 employer accounts. We are pleased that your audit was able to document and verify the implementation of functions that you considered significant to the EAS, and that selected controls reviewed were adequate.

We also note those areas where your report recommends certain improvements. The attachment to this letter addresses those matters.

Thank you for the opportunity to respond to this report and for the recommendations which are intended to further improve the operation of the EAS.

Sincerely,

[Signature]
COMMISSIONER

Attachment
Finding and Recommendation

Planning for Employer Account System needs improvement.

NJDLWD Response

The department will work to develop and maintain a plan for the Employer Accounts System that addresses issues raised in the audit. We will draw upon our experience gained in planning the UI Modernization project to update and maintain an improved Employer Accounts System plan. To the extent feasible and practical, changes will be incorporated.

Finding and Recommendation

IT continuity plans for the Employer Accounts System need improvement and should identify an agreement for an alternate processing facility.

NJDLWD Response

The department will review the IT continuity issue.

While we agree that the establishment of an alternate site processing facility is the ideal plan, it may not be cost effective. Our review of our continuity needs will determine if we should pursue an alternate site after considering the cost and related benefits.

Finding and Recommendation

Security administration and user authentication need improvement. Access rights should be reviewed and confirmed periodically.

NJDLWD Response

We concur. The department has already commenced with corrective action. Since February 2006, user accounts in the Employer Accounts System have been reduced by 26%. In addition, users that have not logged into the Employer Accounts System in 2006 have been locked and procedures are being developed for timely removal of inactive accounts.