Office of Information Technology
myNewJersey Portal

March 17, 2008 to April 24, 2009
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 Office of Information Technology, myNewJersey Portal for the period of March 17, 2008 to April 24, 2009. If you would like a personal briefing, please call me at (609) 292-3700.

Stephen M. Eells
Assistant State Auditor
August 5, 2009
# 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>Background</td>
<td>1</td>
</tr>
<tr>
<td>Objective</td>
<td>1</td>
</tr>
<tr>
<td>Methodology</td>
<td>2</td>
</tr>
<tr>
<td>Conclusions</td>
<td>2</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>Monitoring of Applications Accessed Through the Portal</td>
<td>3</td>
</tr>
<tr>
<td>Portal Hardware and Software Documentation</td>
<td>4</td>
</tr>
<tr>
<td>Auditee Response</td>
<td>5</td>
</tr>
</tbody>
</table>
Office of Information Technology
myNewJersey Portal

Scope

We have completed an audit of the Office of Information Technology (OIT), myNewJersey Portal for the period March 17, 2008 through April 24, 2009. Our audit evaluated selected general and application controls related to this project. Our tests of general controls included portal project management planning, development, and operation. Our tests of application controls included user authentication and authorization procedures to provide secure access to the portal. However, our tests of portal security were performed on a limited sample basis since the ability to fully replicate production in a test environment has inherent configuration limitations. The listing of user access roles provided to our audit team was only secured in December of 2008 due to indicated complications associated with its production. Therefore we did not test to determine that application access through the portal, once established, continued to be properly limited.

Background

The myNewJersey Portal is an identity enabled portal server solution. It provides all the user, policy, and identity management to enforce security, single sign-on, and access capabilities to end user communities while combining key portal services such as personalization, aggregation, security, integration, and search capabilities. Unique capabilities that enable secure remote access to internal applications round out a complete portal platform for deploying robust government-to-employee, government-to-government, and government-to-business applications.

Objective

The objective of the audit was to determine the adequacy of selected general and application controls. These controls included policies and procedures to plan, develop, and maintain the portal; and user authentication and authorization to provide portal security.
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 (CobiT) issued by the IT Governance Institute.

In preparation for our testing, we studied circular letters promulgated by the Department of Treasury, and policies and guidelines of the agency. Provisions that we considered significant were documented, and compliance with those requirements was verified. In addition, we obtained and reviewed portal requirements and design documentation, and development and operational procedures. Functions we considered significant were documented and implementation of those features was verified. We also interviewed agency personnel to obtain an understanding of the internal controls.

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 portal project management planning, development, and operation. Our tests of application controls were designed to provide conclusions about the adequacy of those controls in place for user authentication and authorization.

**Conclusions**

Our review disclosed that while OIT's myNewJersey Portal staff has established appropriate general and application controls over the portal project management planning, development, operation, and security, improvement is needed to ensure that these controls are adhered to and documented accordingly.
Monitoring of Applications Accessed Through the Portal

The myNewJersey Portal requires users to be authenticated and authorized. Through authentication, a user identifies himself by logging into the portal. Authorization indicates that the user has the proper role for a given application. The web application being accessed calls the portal to determine if the user has been authenticated and if the user is authorized to use the application. It is through the use of roles that access to portal applications is accomplished for authorized users. Some roles may be configured to limit access to specific information. The permissions to perform certain operations are controlled by the resource being accessed. The granting of roles is delegated to Role Managers designated by the resource owner. Management of individual user access requires the assignment of the appropriate role to each user.

Portal staff is not always made aware of changes to the applications and access allowed through the portal, since privileges and access are granted by the security staff of the owners of the applications. This may impact the myNewJersey Portal's efficiency by increasing the demand created by the addition of an application. This may also result in more access being granted than originally intended. Testing could not be performed to verify these potential risks. There are 110 roles providing access to resources residing on agency owned and administered servers. This represents 25.7% of the roles maintained by the portal which are not monitored by OIT.

Recommendation

Portal staff should consider actively reviewing applications being accessed to curtail the potential impact on portal efficiency and security.
The documentation provided to us has not been updated to illustrate the features of the current version of the portal.

**Recommendation**

The myNewJersey Portal staff should update the documentation of the portal project in a timely manner to adequately reflect the current version of the portal hardware and software and its current features.
July 24, 2009

Mr. Stephen M. Eells  
Assistant State Auditor  
Office of the State Auditor  
PO Box 067  
Trenton, NJ 08625-0067  

RE: myNewJersey Portal Audit Response

Dear Mr. Eells:

With regard to your audit report on the myNewJersey Portal, we would like to provide the following comments:

Monitoring of Applications Accessed Through the Portal
Your recommendation states, “Portal Staff should consider actively reviewing applications being accessed to curtail the potential impact on portal efficiency and security.”

Response:
The Office of Information Technology has an integrated planning process in place that performs oversight, approval and reporting of all new or significantly updated systems deployed into our infrastructure at defined stages of project design. The Business Case Review defines the business need, high-level scope, solutions and risks. The Logical System Architecture Review (SAR) develops a logical design of the project architecture with no regard to technology or physical platform. The Physical SAR determines the physical technology and platform requirements. The reviewers in these processes include representatives from all operational areas of OIT: Project Management Office, network, storage, security, server administration, application hosting, database, portal and infrastructure.

Any system destined to run through the myNewJersey portal is subject to this process, including systems to be deployed onto agency servers.

OIT recognizes that more closely monitoring enhancements and extensions to agency systems would benefit the State. To this end, we are now performing a major modification in our Information Security Compliance Monitoring policy. In the updated policy we will establish a compliance monitoring methodology for the State of New Jersey Executive Branch that complies with published information security standards, policies and procedures. This exercise is currently underway.

Portal Hardware and Software Documentation
Your recommendation states: “The myNewJersey Portal staff should update the documentation of the portal project in a timely manner to adequately reflect the current version of the portal hardware and software and its current features.”
Response:
As was discussed and agreed upon with the audit team, the documentation OIT provided for the myNewJersey system was substantially complete and up-to-date.

However, several sections of the “myNewJersey System Requirements” and “Portal 6 / Identity / Directory Project Requirements: Use Cases” documents referred to items that OIT decided not to implement when the project scope was changed in 2005.

Although OIT does not plan to update those documents, we recognize the usefulness of keeping future requirements documents up-to-date, and/or annotating them to preserve the historical record while making clear which items are currently applicable.

In this way, we can preserve the accuracy of the current records and still include the pertinent information provided by these outdated sections.

We are appreciative of your efforts in helping us.

Very truly yours,

Adel Ebeid
Chief Technology Officer