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

Department of Personnel
Information Technology Management

June 1, 2007 to January 11, 2008

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 Personnel, Information Technology Management for the period of June 1, 2007 to January 11, 2008. If you would like a personal briefing, please call me at (609) 292-3700.

Richard L. Fair  
State Auditor  
May 7, 2008
# 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>Network and PMIS Access</td>
<td>4</td>
</tr>
<tr>
<td>Network Monitoring and Maintenance</td>
<td>6</td>
</tr>
<tr>
<td>Network Services</td>
<td>7</td>
</tr>
<tr>
<td>Database Administrator</td>
<td>7</td>
</tr>
<tr>
<td>Disaster Recovery and Business Continuity</td>
<td>8</td>
</tr>
<tr>
<td>Computer and IT Related Inventory Control</td>
<td>8</td>
</tr>
<tr>
<td>Auditee Response</td>
<td>9</td>
</tr>
</tbody>
</table>
Department of Personnel
Information Technology Management

Scope

We have completed an audit of the Department of Personnel (DOP) Information Technology Management for the period June 1, 2007 to January 11, 2008. Our audit evaluated selected controls in place over the DOP network and systems that process and protect both public and private information. They are as follows:

- Business continuity plans in the event of processing interruptions.
- Protection of computer resources from unauthorized access, use, and alteration.
- Implementation and documentation of the change control process.
- Physical and logical security in place to protect the Information Technology (IT) infrastructure.
- IT strategic planning.

Objectives

The objectives of our audit were to determine the adequacy of controls over the computer network to minimize the risk of unauthorized physical or logical access, to provide for business continuity, to ensure changes are properly implemented and documented, and to provide for adequate planning.

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

Methodology

Our audit was conducted in accordance with Governmental Auditing Standards issued by the Comptroller General of the United States. Additional guidance for the conduct of the audit was provided by the Open-Source Security Testing Methodology Manual issued by the Institute for
Security and Open Methodologies, *The Gold Standard Benchmarks* issued by the Center for Internet Security, and *Control Objectives for Information and Related Technology* (COBIT) issued by the IT Governance Institute.

In preparation for our testing, we studied legislation, agency operation plans, procedural guidelines and flow charts, and industry and governmental standards for computer security and operation. Provisions that we considered significant were documented and compliance with those requirements was verified by interview of key personnel, observation and access of network infrastructure, and through other tests we considered necessary.

A nonstatistical sampling approach was used. Our samples were designed to provide conclusions about internal control attributes. Sample items were selected judgmentally.

Conclusions

DOP’s management has recognized the importance of security over the department network and the services it provides. We found controls in place and functioning to minimize the risk of unauthorized physical or logical access, to provide for business continuity, to ensure changes are properly implemented and documented, and to provide for adequate planning. However, in making these determinations we identified several control weaknesses merit management’s attention. We have also provided the DOP with a management letter containing a more detailed discussion of network security specifics.

Overview

The New Jersey Department of Personnel (DOP) was created in 1986 to replace the Department of Civil Service. Under the provisions of Title 11A of the New Jersey Statutes, the Department of Personnel administers a merit system of personnel management for the central agencies of state government, for more than 500 local jurisdictions in New Jersey including 20 of New Jersey’s 21 counties and nearly 200 municipalities and local autonomous agencies, and for career non-academic
employees at state colleges. The Department of Personnel acts in both a service and regulatory capacity.

The mission at the DOP is to attract, develop, and retain a high quality workforce for state, county, and municipal governments and to partner with management and labor to develop a fair, efficient human resource delivery system rewarding quality, merit, and productivity.
Network and PMIS Access

Control Objectives for Information and related Technology (COBIT) states: “Management should establish procedures to ensure timely action relating to requesting, establishing, issuing, suspending and closing of user accounts,” and “Management should have a control process in place to review and confirm access rights periodically.” The Department of Personnel does have formal procedures for establishing, issuing, suspending, and closing user accounts, yet not all divisions within the agency follow the procedures nor are user accounts reviewed jointly by the Network Operations unit and Human Resources.

Adequate control over a network requires proper administration of passwords and user accounts, compliance with accepted technical standards, and the granting of access privileges based on need.

Network and Directory Access

Our tests of 507 logon ids revealed the following:

- six percent have not accessed the network since 2006 or prior;
- another 17 percent have never accessed the network; and
- 97 percent have passwords that do not expire

Our tests of 507 users revealed the following:

- one user has retired but still has access to the network and
- two users are retired but have not been removed from the directory.
Password Administration

Password administration at the department is weak and network administration over passwords has conflicting rules. For example, one rule indicates 492 logon ids must change their passwords, yet another rule states these 492 passwords do not expire. Another rule dictating password life for logon ids is set to over 47,000 days which means users’ passwords will not expire for over 130 years.

Password ages were also stratified and revealed 76 percent of users have not changed passwords in one year or more.

Personnel Management Information System (PMIS) Access

Our tests of 1,686 logon ids for PMIS access revealed the following:

- 68 logon ids have not accessed the PMIS application since 2006 or prior; and
- another ten logon ids have never accessed the PMIS application.

Our tests of 1,629 PMIS users revealed the following:

- 153 users have retired and still have access to the PMIS application; and
- 57 users have duplicate logon ids of which 21 users had their access levels changed.
- Six of the 21 users with changed access levels can now process a PMIS transaction in its entirety with final approvals.
DOP should strengthen controls over these areas. We have provided management with the technical details on these matters.

**User Identification Naming Conventions**

The Department of Personnel's network operations unit does not use the names shown on the Personnel Management Information System (PMIS) when adding users to the NJDOP network domain. PMIS names are utilized to match against state databases to determine if a user is a current, transferred, retired, or deceased employee. Until the implementation of a unique employee identification number, this is the only way to match users against state databases to analyze their access to the NJDOP network.

**Recommendation**

We recommend management take steps to ensure network and system access is properly limited and controlled, and the network operations unit utilize users' names as shown on PMIS to facilitate such control.

---

**Network Monitoring and Maintenance**

Strong network administration requires the recording and monitoring of activity to prevent unauthorized system access and usage, and the timely updating of network software to close security holes. We have provided management with the details pertaining to their specific security weaknesses.

**Recommendation**

We recommend the department take the necessary steps to strengthen network monitoring and maintenance.
Network Services

The NJDOP network has open services through logical connections between computers that are not necessary. Leaving these services open increases the risk of unauthorized access and network disruption. We have provided the department with the necessary technical details to correct this weakness.

Recommendation

We recommend network administrators turn off unnecessary services and regularly monitor the network to ensure none are improperly enabled in the future.

Database Administrator

Database security administration procedures are not formally documented nor administered and a database administrator has not been identified.

Recommendation

We recommend that database security administration procedures be formally documented, a database administrator be hired, and security, audit, and violation evidence logs be reviewed and maintained for database security.
Disaster Recovery and Business Continuity

The Department of Personnel (DOP) is responsible for issuing notices of state, county, and municipal job vacancies, and the collection of civil service applications, résumés, and exam fees. It is also responsible for administering civil service exams. The capability to process, store, and record these transactions and data is important to state operations. Therefore, procedures must be in effect to safeguard information resources, minimize the risk of unplanned interruptions, and enable the recovery of critical operations in the event such interruptions occur. This comprehensive business continuity plan should address all potential disruptions to division operations.

We found the department’s business continuity and disaster recovery plan to be adequate, but the department has never tested the plan to determine its adequacy in the event of a disaster.

Recommendation

We recommend the DOP regularly test its disaster recovery plan for the department’s network.

Control over computer and IT related inventory should be strengthened.

Computer and IT Related Inventory Control

Treasury Circular Letter 91-32-OMB requires the maintenance of a fixed asset inventory for all items with a value of $1,000 or greater and that the list be updated annually.

Our testing of computer and IT related inventory at the Department of Personnel noted that there is a central repository and responsibility for inventory control, yet the listing is not accurate and updated on a consistent basis. Thirty percent of the assets tested had inventory tags and serial
numbers which did not agree with the inventory listing and 25 percent were not in the locations stated on the inventory listing.

Failure to maintain accurate records increases the risk of assets being stolen or lost without detection.

**Recommendation**

We recommend that inventory records be corrected and regularly tested.
Thursday, April 21, 2008

To: Richard L. Fair – State Auditor

Subject: Department of Personnel Network Security Audit Response

After reviewing the recommendations of the OLS Network Security Audit conducted 6/1/07 – 1/11/08, ITM has collaborated to determine the actions to be taken by the department to enhance and security our IT network. Below are the details of these actions.

**Network and PMIS access**

**Network and Directory access –**

Since the conclusion of the Security Audit, DOP has improved our ENS (Employee Notifications System) which requires business units to communicate personnel changes with Facilities, ITM, application administrators and HR. Meetings were held with divisional delegates and management emphasizing the importance of the ENS procedures.

The network team installed the same tool as used by the Audit team for user ID discovery. We experienced similar results. These user accounts flagged by the software include any separated users which have been disabled and left in the “separation” folder, user accounts for email or application purposes only, and service accounts. The plan is to remove the separated user accounts from Active Directory. The service accounts and accounts for email purposed are needed for our daily use.
Password Administration –

In anticipation of the Network Security Audit’s findings, ITM implemented a password policy on March 3, 2008. The policy is listed below:

**Password policy 3/08:**
The following are password policy requirements enforced through Active Directory:

1. Enforce Password history – the last 3 passwords remembered (prevents users from reusing the same password)
2. Maximum password age – 90 days (same as CAMPS)
3. Minimum password age - 5 days (must wait to change, prevents users from reusing the same password)
4. Minimum password length - 6 characters
5. Account Lockout threshold - 5 invalid logon attempts (prevents hackers from brute-force attacks)

Our domain controller local policies will be tightened to comply with our recently enforced password policy.

**Personnel Management Information Systems (PMIS) access –**

DOP will distribute reports to the State agency ISRs to emphasize access procedures, especially in regard to the PMIS IDs. The ID identified in the audit will be reviewed and removed as needed.

**User Identification Naming conventions –**

ITM is notified by the divisional clerical staff roughly 1 week in advance through the ENS application when a user has been hired by the department. They provide the user’s preferred name, which sometimes is not their legal name. The network account and the ID are created based on this information in order to prepare the computer profile and application access prior to the start date. A small percentage of the accounts may differ from the PMIS record.

An alternative would be to have the divisional reps provide the name based exclusively on the PMIS record. This would require agreement from the Directors and or HR. ITM also discussed having the network IDs automatically created based on the PMIS record. This could cause a delay in processing the computer profile set-up. DOP will review and take the best course of action.
Network monitoring and maintenance

Some of the tools used in the audit were a network vulnerability scanner and other software capable of monitoring the network in real time. These are fairly expensive applications that require training and dedicated resources to configure and monitor. DOP will consult with OIT for recommendations, evaluate the various applications and add the purchase and training to our IT plan for next fiscal year.

Network services

DOP ITM will be taking several steps to increase network security by tightening possible security risks in our production servers. We will utilize several tools to analyze possible risks and take the necessary actions.

First, ITM network team will update all servers and apply the necessary security updates, optional patches, and service packs. Servers will be classified into four categories:

- class A for OIT application/web servers,
- class B for DOP mission critical servers,
- class C for DOP non-critical servers, and
- class V for servers with 3rd party applications.

Classifications will distinguish the timing of reboot and if any consulting is necessary from 3rd party vendors.

Second, ITM will ‘harden’ the server by scanning for unneeded services and ports. We will be utilizing a security scanner and baseline security analyzer. These applications will help ITM pinpoint possible security risks and backdoors.

Servers will continue to be monitored using Windows Update Server to identify Critical and Security updates needed on each server class. Once tested, each patch will be applied using WUS to automate our patching routine.
Database Administrator

Currently, our database administration basic tasks are handled by our Unix administrators. We’ll continue to request for the position of Database Administrator.

Disaster Recovery and Business Continuity

Mainframe systems (PMIS, EXAMS, etc) – mainframe systems are housed at the OIT Hub in West Trenton on IBM mainframe computers. OIT is responsible for the data backups, which is synchronized with the OARS (OIT Availability and Recovery Site) facility. DOP will verify OIT’s DR mock-up schedule and process.

DOP network (Exchange, File server, etc) – Our Exchange servers are configured as an active-passive cluster to provide redundancy in case of hardware failure. Also, ITM routinely receives requests from users to restore files and email. We are able to accommodate these requests demonstrating the ability to recover data on request. Testing a full-scale restore for our mail or file server would require a significant amount of time and resources.

DOP recently engaged a 3rd party vendor (Recall) to handle the storage of off-site backup media. This provides a secure neutral location for storing our mission critical backup media.

Web application servers – Currently, we maintain redundant clustered servers for the web and application servers housed at the OIT server farm. We also have web and application UAT (testing) servers at this facility. These UAT servers require only slight configuration changes to make them production ready. We also have a set of test and development servers at DOP SP, which could be production ready in a short amount of time.

OARS (OIT Availability and Recovery Site - future) – the plan for the future DRBC is to house equipment at the OIT OARS site. With data replication performed nightly, we would have a duplicate system at a remote facility that is production ready in case of a disaster or failure. This is a costly endeavor (hardware, dedicated fiber and configuration, etc), but would provide secure off-site data storage and a redundant hardware set for mission critical production continuity.
Computer and IT related Inventory control

To better manage our inventory, DOP has developed an in-house, Asset Management Application. It is a web based application utilizing SQL server as backend Database Management System. As of March 08, all the asset information has been ported from a previous Inventory Control Excel spread-sheet into this application.

DOP asset information is also downloaded into OITs Statewide Technology Asset Reporting & Tracking (START) System on a quarterly basis starting April 08. During this period, DOP will review the inventory data conducting sample inventory audits to ensure inventory accuracy.

Respectfully submitted,

[Signature]

Joseph Gambino
CIO & Director of DITM

C: Rolando Torres, Commissioner
Marjorie Schwartz, Deputy Commissioner
Bari Simpkins, Chief of Staff