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

Office of Information Technology
Data Center

May 18, 2009 to June 18, 2010

Stephen M. Eells
State Auditor
The Honorable Chris Christie
Governor of New Jersey

The Honorable Stephen M. Sweeney
President of the Senate

The Honorable Sheila Y. Oliver
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 Data Center for the period of May 18, 2009 to June 18, 2010. If you would like a personal briefing, please call me at (609) 292-3700.

Stephen M. Eells
State Auditor
September 8, 2010
# 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>Conclusion</td>
<td>2</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>Physical Access Controls</td>
<td>3</td>
</tr>
<tr>
<td>Computer Inventory</td>
<td>5</td>
</tr>
<tr>
<td>Auditee Response</td>
<td>8</td>
</tr>
</tbody>
</table>
Office of Information Technology
Data Center

Scope

We have completed an audit of the Office of Information Technology (OIT) Data Center for the period May 18, 2009 through June 18, 2010. Our audit evaluated selected general controls in place at the HUB, River Road, and the OIT Availability and Recovery Site (OARS). Our tests of general controls included those concerning backup and recovery; business continuity and disaster recovery; and logical and physical security. Operations and production control were excluded from our scope.

Background

The HUB data center houses the Bull mainframe computer and client servers, as well as providing state printing processes. The River Road data center contains the IBM mainframe computer and a server farm for clients. It also includes the Network Control Center and the System Control Center, which is the help desk for all state departments. Both facilities process various mission critical applications for the state. OARS serves as the state’s backup and recovery, and business continuity and disaster recovery site. Each facility is integral in the processing of applications that are vital to the functioning of the state and for providing electronic services to its citizens.

Objective

The objective of the audit was to determine the adequacy of selected general controls. These controls included policies, standards, and procedures to properly maintain and safeguard the data centers and the related hardware, software, and information assets and resources.

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 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 documentation and procedures pertaining to internal controls over the data centers’ security, maintenance, and continuity. 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 backup and recovery; business continuity and disaster recovery; and logical and physical security.

Conclusion

While OIT staff has established appropriate general controls over the data centers’ maintenance and protection, our review disclosed that improvement is needed to ensure that these controls are adhered to and regularly updated.
Physical Access Controls

Access to the HUB, River Road, and Office of Information Technology (OIT) Availability and Recovery Site (OARS) data centers is controlled by card readers requiring access card badges encoded with the necessary access level for entry into these facilities. The access control system, Compass 4-E, is the responsibility of the Department of Treasury, Office of Treasury Technology, Interdepartmental Security Unit (ISU). ISU controls the security infrastructure of all Department of Treasury owned and leased property. OIT issues the access badges to those individuals requiring entry into the River View Plaza location, as well as the data centers. Access levels granted to these individuals were established at the time of inception of the Compass 4-E system as part of the Y2K initiative. OIT does not have the ability to directly revise these access levels or monitor access into their facilities without ISU’s involvement. ISU is responsible for administering all door card readers and access levels. Periodic communication or reporting has not been established which would enable OIT to examine access to ensure that its facilities are adequately controlled.

Several weaknesses were found during our audit. Doors to sensitive areas in the data centers were found to be unsecured either by being unlocked or by card readers not functioning. For example, of the four doors allowing access to the computer room at the HUB data center with card access to control admittance, two doors were able to be opened without using a key card. In addition the card reader for the door to the telecommunications room was turned off and the door was left unlocked.

Of the 1,511 badges OIT has issued, there are 1,507 unique names on these badges. Some employees have multiple badges accounting for the difference. All but eight of these badges
initially had access levels allowing admittance into the computer room at the River Road Data Center. After discussion with facilities management, ISU was notified and the access level was corrected. Presently, 499 badges have the ability to gain access to the River Road data center's computer room; 525 can access the HUB data center computer room; and 280 can access the OARS data center computer room. Access to at least one of the three data centers is provided on 544 badges. An analysis of the 544 badges is presented in the following table.

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>OIT</td>
<td>293</td>
</tr>
<tr>
<td>Consultants, Auditors, and Vendors</td>
<td>81</td>
</tr>
<tr>
<td>State Police</td>
<td>80</td>
</tr>
<tr>
<td>Another Agency</td>
<td>46</td>
</tr>
<tr>
<td>Not on State Directory</td>
<td>31</td>
</tr>
<tr>
<td>Retired</td>
<td>7</td>
</tr>
<tr>
<td>General (e.g. &quot;cleaning people&quot;)</td>
<td>4</td>
</tr>
<tr>
<td>Temporary</td>
<td>2</td>
</tr>
</tbody>
</table>

It is questionable whether these badges only allow admittance to those users whose job responsibilities require access. As the table above shows, there are active badges belonging to retired employees. There are also many badges active for consultants, auditors, vendors, and staff of other agencies where access might not be warranted.

Valuable assets and information resources for the state and its citizens are at risk of being lost, damaged, or misappropriated. In accordance with CebiT control objectives, procedures should be defined and implemented to grant, limit, and revoke access to premises, buildings, and areas according to business needs, including emergencies. Access to premises, buildings, and areas should be justified, authorized, logged, and monitored. This should apply to all persons entering the premises, including staff, temporary staff, clients, vendors, visitors, or any other third party. Written policies and procedures addressing the issuance, removal, and monitoring of access badges have not been developed. The current access levels do not adequately limit access to
these high-risk facilities. In addition, the designed control of the card readers has been circumvented through their disconnection to the system in some instances.

**Recommendation**

OIT should further revise the access levels in order to properly restrict access to the data centers to personnel whose function requires them to have access to these high-risk facilities. Policies and procedures should be instituted instructing the security staff on the proper protocol for granting access to these buildings. With the current lack of resources to procure a new physical access security system, OIT needs to actively monitor the present system in order to determine that access is appropriate.

---

**Computer Inventory**

In order to provide an assurance of the security of the hardware at the data centers, we requested a listing of hardware to sample items at the respective data centers. We obtained information from the Office of Information Technology’s (OIT) asset management system, the Fixed Asset Inventory Reporting System (FAIRS). This is an automated on-line system providing access to a database of OIT’s hardware and software inventory records. The FAIRS database consists of individual detail records for all of OIT’s data processing hardware, mainframe software, and client-owned terminal equipment connected to the OIT network. Each record consists of more than 40 data fields that define and locate the equipment and provide other information needed for OIT’s purposes and for those organizations with which OIT interfaces. An assessment of the asset inventory is performed on an annual basis at which time any changes are entered into FAIRS. In addition, OIT does not currently have a central, comprehensive list of applications and their respective platforms on which they run. However, they are in the process of populating...
the Automated Server Application Inventory (ASAI) of applications currently processed on the servers.

Although we did not perform an audit of FAIRS, it was through our attempt to obtain a hardware inventory listing that weaknesses surfaced concerning OIT's asset management system. In order to accurately account for the hardware and software assets, it is vital to have a system in place that will properly record the asset and track it through its life cycle. In accordance with CobiT objectives, asset tracking and monitoring of individual IT assets help protect them and prevent theft, misuse, and abuse. In addition, a comprehensive listing of applications and the platform on which they are run will ensure that mission critical applications are documented to help prevent the applications from experiencing interruptions and to optimize the equipment as best as possible.

FAIRS may not provide an accurate representation of assets and their value because of inconsistencies in how assets are actually recorded in this system. This could lead to potential misappropriation of assets if they are not properly recorded. OIT may also not possess complete knowledge as to what assets they truly have and where they are located. Lack of a central, comprehensive application listing makes administering the servers that they are run on more difficult, especially when an upgrade is necessary. Without this complete listing, it may be difficult to determine what applications will be affected by a change. Optimization of equipment cannot be achieved if current information on what applications are on which servers is not readily available to the server administrators.

**Recommendation**

OIT needs to accurately record their assets for proper valuation and location. This can be accomplished through a revision of their current system or utilizing another means in order to perform this task. OIT must also make the completion of the ASAI spreadsheet a priority in
order to have a comprehensive listing of all applications and their respective platforms.
August 27, 2010

Stephen Eells  
State Auditor  
Office of Legislative Services  
Office of the State Auditor  
PO Box 067  
Trenton, NJ 08625-0067

Re: OIT Data Center Audit May 18, 2009 to June 18, 2010

Dear Mr. Eells:

With regard to your audit report recommendations on the Data Center facilities at OIT, we would like to provide the following comments:

**Accountability of Assets Recording Their Proper Valuation and Location**

Your recommendation states, "OIT needs to accurately record their assets for proper valuation and location. This can be accomplished through a revision of their current system or utilizing another means in order to perform this task. OIT must also make the completion of the ASAI spreadsheet a priority in order to have a comprehensive listing of all applications and their respective platforms."

The Fixed Asset Inventory Reporting System (FAIRS) is quite outdated. It has outlived its original intent of OMB Circular Letter compliance, depreciation accounting for federal recovery and GASB reporting purposes, and as a planning tool for maintenance requirements. Lack of resources for programming support, the transient nature of the server world and weak Change Controls in FAIRS (e.g. heterogeneous data entry) have made asset accounting, and its management, more difficult using this system.

OIT is currently in the process of improving accountability for inventory assets. OIT is evaluating, and will be strengthening and implementing a workflow of asset accountability. First Data Management Services (DMS) is scheduled to convene with Financial Management to review the various issues associated with the data in the FAIRS database. The meeting will concentrate on the segregation and the archiving of FAIRS dormant asset entries. This dormant inventory portion is to be reconciled by ownership, value and location; and, will likely be closed out. The active inventory portion will remain open and reconciled as to ownership, value and location.

Automated Server and Application Inventory (ASAI) records presently record ownership and data center configuration for the hardware portion of the asset inventory. In the coming calendar year the same practical approach will be evaluated for the application software portion of asset inventory. Once the hardware and software records are made current a software tool such as Tivoli Storage Manager could then be used for both inventory Hierarchal Space Management and addressing inventory queries.

Also, as part of a larger and longer-termsed Change Management and Compliance initiative, OIT will review Financial Management asset management, ASAI and Software Compliance processes, data, and functions to create a cohesive inventory environment that addresses data center asset management, software compliance, change management, and financial management requirements.
Re: OIT Data Center Audit
Page 2

Corrective Actions for Physical Access Controls

The audit report recommendation states, “Doors to sensitive areas in the data centers were found to be unsecured either by being unlocked or by card readers not functioning.” Policies requiring the securing of doors in the data center have been strengthened and are being enforced in a proactive manner. Additionally, the card readers that are not functioning have been reported to the Division of Property Management and Construction (DPMC) in the Treasury Department and are scheduled to be repaired in the near future. OIT will be vigilant in identifying future equipment malfunctions which will be reported to the DPMC immediately, as applicable.

The audit report further states, “Of the 1,511 badges OIT has issued...Access to at least one of the three data centers is provided on 544 badges.” The breakdown in the audit report for these 544 badges reveals that 500 of them are assigned to the following areas:

1. **OIT**
2. **Consultants, Auditors and Vendors**
3. **State Police**
4. **State Agencies other than OIT and the State Police**

The breakdown of the remaining 44 badges is distributed in the following manner:

1. **Not on a State of NJ Directory**
2. **Retired**
3. **General (e.g., “Cleaning People”)**
4. **Temporary**

The first group, “Not on a State Directory” has all been identified. They consist of the Security Staff requiring 24/7 access to all facilities as well as employees whose names were misspelled, usually by only a letter or two, and therefore were not able to be located in State Directories. The Security Staff are now recorded by individual name and the misspellings have been corrected to agree with the State Directories.

The “Retired” group badges are now also retired from the badge access tables and their badges will be reassigned to current employees.

The “General” group has been identified as belonging to four high level access individuals whose responsibilities cover these areas:

1. **Overall OIT Data Center Management**
2. **Property Owner Building Management**
3. **DPMC Facilities Management**
4. **Verizon Technical Network Support**

The two “Temporary” badges are now the responsibility of specific individuals to both distribute and retrieve in a timely manner.

I appreciate the cooperative manner in which you and your staff conducted this audit. Your recommendations are well accepted as OIT is committed toward continual improvement. If you have any further comments, please contact our I.T. Audit Manager, Kenneth Herbst at (609) 633-9194. He will be available to expedite any communications throughout OIT.

Sincerely,

[Signature]

Adel Ebeid  
Chief Technology Officer

C. D. Gerard  
K. Herbst  
A. Timmons  
S. Dragert  
H. Hottmann

New Jersey Is An Equal Opportunity Employer * Printed on Recycled and Recyclable Paper