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

Department of Human Services
Information Systems Management

July 1, 2002 to June 17, 2004

Richard L. Fair
State Auditor
The Honorable James E. McGreevey
Governor of New Jersey

The Honorable Richard J. Codey
President of the Senate

The Honorable Albie 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 Human Services, Information Systems Management for the period July 1, 2002 to June 17, 2004. If you would like a personal briefing, please call me at (609) 292-3700.

October 26, 2004
# 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>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Information Technology Planning and Development</td>
<td>4</td>
</tr>
<tr>
<td>Operating System Security Administration</td>
<td>7</td>
</tr>
<tr>
<td>Server and Associated Product Acquisitions</td>
<td>8</td>
</tr>
<tr>
<td>Auditee Response</td>
<td>9</td>
</tr>
</tbody>
</table>
Scope

We have completed an audit of the Department of Human Services (DHS), Information Systems Management for the period July 1, 2002 through June 17, 2004. Our audit evaluated DHS’ management of information technology (IT) planning and development. We also evaluated selected general controls maintained by DHS’ Office of Information Systems (OIS) over its systems at Capital Place One, the location of the central office. OIS is responsible for the development, deployment, and integration of IT and telecommunications systems for DHS.

Objectives

The objectives of our audit were to determine the adequacy of DHS’ management of IT planning and development, and the adequacy of the general controls maintained by OIS for operating system security and business continuity.

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 Government Accountability Office and Control Objectives for Information and related Technology issued by the Information System Audit and Control Foundation. In preparation for our testing, we studied legislation, administrative code, executive orders, circular letters promulgated by the State Comptroller, and policies of the division. Provisions that we considered significant were documented and compliance with
those requirements was verified by interview, observation, and samples of transactions. We also interviewed DHS personnel to obtain an understanding of the operations and 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 operating system security, backup and recovery, and contingency planning and disaster recovery.

Conclusions

During the period of our review we found that management controls over IT planning and development were not adequate. We also found the general controls for operating system security and business continuity to be deficient. Details of our findings follow.
Properly managed and designed information systems are important in protecting the millions of dollars invested in this technology and to ensure the state’s clients are effectively served.

Overview

To achieve strong IT management, the National Association of State Chief Information Officers (NASCIO) recommends an enterprise resource management and architecture approach. This approach requires comprehensive, documented and continual IT planning for an entire organization. It is applicable to the state as a whole, and is also applicable at the departmental level, especially for a department as large as DHS.

The Information Systems Audit and Control Foundation, in its IT control publication COBIT, states “In placing the information services function in the overall organization structure, senior management should ensure authority, critical mass and independence from user departments”. The federal Government Accountability Office (GAO) has also advocated these centralized control approaches for federal technology management.

For the state, Executive Order #87, issued in 1998, was an attempt to address the reality of the need for strong centralized management. This order required the creation of the Office of Information Technology (OIT) in recognition of the need for statewide management, and mandated the appointment of a chief information officer (CIO) by the Governor, who develops and implements the Statewide Strategic Plan for Information Technology. The CIO “shall lead, coordinate, and integrate statewide information technology policies and activities.” In addition, per NJ Circular Letter No: 00-03-DPP, all IT procurements must conform with approved Departmental IT Strategic Plans, regardless of dollar amount.

The State of New Jersey’s “Shared IT Architecture” document, issued by OIT, states that “The Shared Server Infrastructure (SSI) is located at the HUB and River Road data centers. It is an area in each
computer room where servers are being centralized to offer a common location to manage the distributed environment.” It further states that “Optimizing key server resources through common logical and physical environments positions the State to properly plan, manage and control a growing server infrastructure.” In addition, this document also states that “The State manages two Storage Area Networks (SAN), one at River Road and one at the HUB. A SAN is a network whose primary purpose is the transfer of data between computer systems and storage elements.”

Therefore, any attempt by a department to isolate development and processing efforts from OIT can be counter-productive, inefficient, and contrary to state guidelines. However, this condition is what we found at the Department of Human Services (DHS).

**Information Technology Planning and Development**

DHS, through its Office of Information Services (OIS), is in the process of overseeing an ambitious initiative in support of the department. This new technology initiative involves the modernization of systems used by DHS and moving of applications away from the state’s legacy mainframe environment. In support of this initiative, the department has been making decisions and purchases to build their own data processing capabilities separate from OIT. They intend to house applications at a data center they have created at the central office instead of at the OIT data center, and were moving ahead without a comprehensive strategic plan, until one was developed in July 2004 to guide them.

The department is to be commended for their recent creation of a comprehensive IT strategic plan. However, it was not in place during the development discussed in this report. In addition, the strategic
The plan makes no mention of working in conjunction with OIT, which would provide the appropriate level of control that is necessary for these significant technology enhancements.

The most significant modernization effort currently being implemented is the Division of Youth and Family Services new case management system, SACWIS, which is expected to cost $30 million, including implementation and verification over a five-year period. The contract awarded was for a version of SACWIS designed to run on a Sun Solaris platform housed at OIT. However, DHS has insisted on having SACWIS run on IBM servers, requiring system modification. This modification is estimated by OIT’s management to require an additional three full-time technical support staff.

OIS has incurred approximately $10 million of DHS’ $60 million in IT expenditures over the last two fiscal years. Much of this was expended for the purchase and installation of servers at their main office. OIS has individual plans for which it has hired nine contractors to aid in the in-house development of 23 applications in addition to the SACWIS development. Until recently, these efforts have been undertaken without a department-wide strategic plan.

Contributing to the condition is DHS’ creation of their own internal data center. OIS created this data center through the installation of several IBM servers and a storage area network in the central office’s network control room over the last four years. The basis for this action is to support the development of cross-divisional application systems. Currently, a portion of the capacity of two of three servers purchased for this reason have actually been used in support of two separate divisional application systems, General Assistance and Document Imaging. One cross-divisional application, the Unusual Incident Reporting System (UIRS), is in production and uses a portion of the capacity of these servers.
Half of the capacity of these two servers remain unutilized. The third server primarily supports various system management software products.

Our review of acquisitions for development of this central office data center identified contracted personnel costs to compensate for the lack of sufficient departmental staff to properly undertake this project. The cost of these services was $1.3 million. If the servers were placed at OIT data centers the need for consultants could be reduced.

In addition, this central office data center has insufficient backup cooling and no alternative processing facility to provide adequate business continuity and disaster recovery capabilities. A current information technology continuity plan identifying infrastructure requirements, an alternative processing facility and recovery procedures is not documented and regularly updated. Although data and system software back up tapes are produced and moved off site, insufficient periodic tests have been performed and documented to ensure the reliability and effectiveness of this process.

According to the Federal Information System Controls Audit Manual, published by the GAO, procedures should be in place to protect information resources and minimize the risk of unplanned interruptions and a plan to recover critical operations should be maintained in the event interruptions occur. These plans should be fully tested periodically to determine whether procedures will work as intended.

**Recommendation**

We recommend DHS regularly update their new strategic IT plan based on current business needs and development efforts, and available resources. DHS should modify this plan to recognize the need to coordinate their efforts with and through OIT. In addition, we recommend OIS site the acquired servers and future server purchases at the appropriate
OIT data center to permit the proper coordination of information processing activities which will result in the most effective and efficient use of the State's resources. Finally, OIS should address current facility deficiencies and establish procedures and guidelines in a manner which provides for the most efficient and effective use of existing statewide information technology resources by minimizing the service continuity requirements with regard to personnel, facilities, hardware, software, and equipment.

---

**Operating System Security Administration**

OIS has not developed and documented a computer security policy addressing the following areas: the assignment of privileges and the authorization of access to system resources; the review and resolution of unauthorized use or attempted use of system resources; and the request, review and authorization of system software installation and modification. We tested and found implementation of system security (for IBM’s AIX operating system) has been performed using incomplete and unapproved procedures and guidelines. The AIX servers process among other items, confidential information for the General Assistance program. Our evaluation revealed deficiencies in defining user account attributes, removing unnecessary system services, and implementing system configuration options. The account attributes omitted are critical in assuring proper user account administration and effective user account identification and authentication. For instance, blank passwords were allowed. The services remaining and options omitted increase the risk associated with providing access. Our tests further indicated noncompliance with the procedures and guidelines that were established.
A complete computer security policy identifies security objectives and operational security rules that support the derivation of appropriate implementation procedures and guidelines. According to the Federal Information System Controls Audit Manual, published by the GAO, a comprehensive policy for security planning provides the basis for the control structure which defines procedures for assessing risk, developing and implementing effective controls to reduce risk, and monitoring the effectiveness of these controls to reduce risk.

Recommendation

We recommend that the Office of Information Services (OIS) develop a comprehensive computer security policy which identifies the security objectives and operational security rules, assigns responsibilities, ensures compliance, and is supported by appropriate procedures and guidelines.

Server and Associated Product Acquisitions

Our review of selected server and associated product acquisitions with a total cost of $3.8 million, identified services costing $447,000 improperly coded under the contract. The desired consulting services should have been identified as “work station conversion services”.

Recommendation

We recommend that the OIS process acquisitions of information technology hardware, software and related services in accordance with the established state contract by providing the proper identification of items to be acquired.
Dear Mr. Fair:

This letter is in response to the OLS Audit Report of the Department of Human Services (DHS), Information Systems Management, dated September 23, 2004. The following identifies the audit finding as well as our response to the finding.

OLS Finding

The Department of Human Services has not created a comprehensive and updated strategic plan for managing its information processing resources, while they were creating their own internal data center.

Auditee Response

The Department developed an updated Strategic Plan which was finalized and approved in July, 2004. Prior to the approved Strategic Plan, and during the period of the audit, DHS had a documented strategic direction, and acted in partnership with OIT, which also reviewed and approved all technology solutions and procurements. Further, DHS did locate the entire SACWIS development, test and production equipment at the OIT HUB.

OLS Finding

Senior management has not adequately enforced and documented its computer security decisions.
Auditee Response

A wide range of IT written security related policies exist and have existed in DHS for years while DHS is in the process of consolidating its Information Technology security policies. These policies are regularly updated, and are in fact, available online. While they are available in many forms, we do not agree that the cited policies do not exist, or that the lack of a consolidated policy is the determinant of an effective security operation, particularly when every other administrative policy mechanism in the State of New Jersey relies on a multitude of circular letters, administrative orders, information memorandums and other written correspondence.

We believe DHS information is as or more secure than data anywhere else on the Garden State Network because of our rigorous use and enforcement of our security policies, made necessary by nature of the client and financially oriented business which DHS conducts daily. Access to the AIX operating system, which was tested during this audit, is completely unavailable to anyone outside of the AIX System and Database Administration Unit. It cannot be accessed by anyone else in DHS, OIT, or on the Internet. At no time were any actions taken or configurations set that put any data or security at risk. The findings identified by the auditors were corrected immediately and steps have been taken to ensure the corrective action is permanent.

OLS Finding

One information technology acquisition inaccurately coded one contract service.

Auditee Response

DHS agrees that the one service cited was inaccurately coded, but this service is allowable under the terms of the State contract, under alternative coding. DHS has implemented new procedures to ensure all procurements specify the correct contract terminology.

If you have any questions, do not hesitate to contact Jacob Eapen, Assistant Commissioner, at 2-7912.

Sincerely,

James M. Davy
Commissioner