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

Office of Information Technology
E-Government Services

February 13, 2001 to November 21, 2001

Richard L. Fair
State Auditor

New Jersey State Legislature

OFFICE OF LEGISLATIVE SERVICES
OFFICE OF THE STATE AUDITOR
125 SOUTH WARREN STREET
PO BOX 067
TRENTON NJ 08625-0067

ALBERT PORRONI
Executive Director
(609) 292-4625

RICHARD L. FAIR
State Auditor
(609) 292-3700
FAX (609) 633-0834

The Honorable James E. McGreevey
Governor of New Jersey

The Honorable John O. Bennett
President of the Senate

The Honorable Richard J. Codey
President of the Senate

The Honorable Albio Sires
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, E-Government Services for the period February 13, 2001 to November 21, 2001. If you would like a personal briefing, please call me at (609) 292-3700.

Richard L. Fair
State Auditor

May 20, 2002

Table of Contents

Office of Information Technology
E-Government Services

Scope

We have completed an audit of the Office of Information Technology's (OIT) E-Government Services for the period February 13, 2001 to November 21, 2001. Our audit evaluated the following selected general controls involved in the operation of the E-Government environment.

- Protection of state resources from unauthorized access, use and alteration through the internet.
- Changes over web and system software.
- Protection of citizens' privacy.
- Business continuity plans and data storage in the event of processing interruptions.

The web access provided by OIT also provides links to various state agency applications. Controls over these applications were not audited. The judicial and legislative branches of the state have assumed the responsibility for their own delivery of services via the web and are not subject to supervision by OIT. Therefore, those efforts are not a part of this audit.

Rapid innovations in technology have occurred in the last decade which have brought significant challenges. These challenges led state executive branch officials to develop a plan to make New Jersey the online state. The executive branch implemented a plan to develop web applications and built the technology infrastructure to deliver web enabled services to the business community as well as the general public. Within OIT, the Office of E-Government, the Production Services office, and the Network Infrastructure and Telecommunications office have been given the responsibility to build and

maintain the infrastructure. The Office of E-Government and the Office of Application, Development and Maintenance Services are responsible for developing web enabled applications.

IT governance is administered in the state at different levels. The highest level of responsibility is the state Chief Information Officer (CIO), who reports to the governor's office. The CIO serves as the chair of the Office of Information Technology governing board, which also consists of the State Treasurer, two members from executive branch agencies, and three members of the public. The board is tasked with guiding the direction of OIT. OIT is responsible for the day-to-day administration of information technology operations.

Objectives

The objectives of our audit were to determine the adequacy of selected general controls in place over OIT's E-Government Services.

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 *Assessing the Reliability of Computer-Processed Data* issued by the United States General Accounting Office and the *Risk Assessment Guidebook for e-Government* issued by the National Electronic Commerce Coordinating Council.

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 state web pages, and through our testing of access logs and change requests.

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

Conclusions

OIT management has recognized the importance of properly controlling the E-Government Services it provides. However, we have found several control weaknesses within this effort that, if not corrected, could contribute to failures to provide secure state services through the internet.

We have also provided OIT with a management letter containing a more detailed discussion of the computer control weaknesses.

Written Policies and Procedures

OIT management should continue their efforts in developing and disseminating policies and procedures.

To mitigate the higher risk involved with electronic government, policies and procedures regarding responsibility for and administration of data and network security and protection should be in place before E-Government infrastructures and applications are put in place. The governing board and OIT management are responsible for development and enactment of these policies and procedures. However, we found that some policies and procedures in these areas still need to be developed and enacted. Policies and procedures relating to the distributed server environment that supports E-Government do not exist for certain security, access, and business continuity functions as described below.

Recommendation

We recommend that the governing board and OIT management continue their efforts in developing and disseminating the necessary written policies and procedures to address these areas.

Auditee's Response

OIT is in the final approval phase of a security policy. This document should be published in August. Subsequent to approval the Security Working Group will begin developing standards and guidelines.

Security

OIT should take appropriate measures to strengthen security.

A well designed and implemented security plan ensures that data is protected against unauthorized use, disclosure, modification, or loss. The plan should provide for audit trails that would allow unauthorized activity to be identified and investigated in an efficient manner. Sufficient current technology should be used to achieve this goal.

Security procedures in the aforementioned areas can be improved, and we have provided OIT technical detail to allow them to address these issues.

Recommendation

We recommend OIT take appropriate measures to strengthen security.

Auditee's Response

Funding for enterprise IDS is available and a complete IDS design and implementation for host and network will be in place this fiscal year.

As stated above the OIT security policy will be out shortly. This will be followed up by standards and guidelines.

Since OIT recognizes & supports an enterprise security approach, we have developed an Executive Order to address security across all 3 branches of government. The CIO will be proposing this Executive Order to the Governor. This order would result in a task force comprised of all 3 branches of government. The product developed by this task force will include a statewide approach to security and governance over the management of enterprise security.

Disaster Recovery and Data Back Up

OIT management should implement a complete disaster recovery plan.

A business continuity plan and data back-up procedures should be in place and tested periodically to give the organization the ability to recover the necessary data and continue operations in the event of a processing interruption or disaster. Our review noted that no disaster recovery plan exists for the distributed server environment. We also noted that back-up data are not maintained at a remote location. OIT is aware of these weaknesses and is evaluating a disaster recovery plan recommended by a consultant.

Recommendation

We recommend OIT management implement a disaster recovery plan. They should also develop a plan to store back-up data at a remote location.

Auditee's Response

OIT has committed to the development of an alternate high availability site. This site will provide disaster recovery capabilities for the wide area network, shared server infrastructure including all e-gov mission critical servers. In addition, this may be used for vaulting of mainframe data.

Since this alternate site will take at least 24 months to develop, we will continue to build high availability/disaster recovery into the current infrastructure using the River Road and Hub Facilities. The majority of shared server infrastructure has already been built with high availability capabilities. The high availability design supports a large part of the disaster recovery capability.

The disaster recovery/contingency plan document is being developed by OIT to address recovery of all key infrastructures. A draft of the document will be developed by the end of September.

Change Management

The production environment should be properly protected.

A strong system of internal control over system changes mandates that the development and change functions be segregated from the production function in order to minimize the likelihood of an error or irregularity occurring and going undetected. Also, changes to application software or hardware should be documented to create an adequate audit trail.

Some developers and testers are not prohibited from accessing the production environment through the internet. Also, hardware and software changes are not always documented due to the cumbersome

nature of the current documentation system, Info/Man.

Recommendation

We recommend OIT prevent developers and testers from accessing the production environment through the current internet process. In light of the cumbersome nature of the Info/Man System, an alternate means of documenting hardware and software changes should be considered.

Auditee's Response

An effective change management policy has been in use at OIT practically since its existence. The purpose of this policy is to manage changes to our production environments in order to maintain or increase the level of service to our client community.

The current OIT change methodology applies to production hardware, software and environmentals. This process includes risk assessment, scheduling and back out procedures. Approval authority for changes to application software is segregated from the actual change function.

In order to address the cumbersome nature of InfoMan, OIT is in the process of implementing Peregrine Service Center (SC), a sophisticated, state-of-the-art, user-friendly problem and change management system. It is planned that Service Center will replace InfoMan for both problem and change management in the near future.

When Service Center is fully implemented, all groups within OIT that engage in changes that impact the delivery of service to our clients will be required to use change management. As this process evolves, change management services will also be offered to the client community.

After migration to the new WAN / Internet environment, the test and production environments will be different entities. The migration is scheduled for completion November, 2002.

Privacy Notice

A comprehensive privacy notice is important to strengthening users' confidence.

To strengthen users' confidence in E-Government, a written and approved privacy notice should communicate how cookies are used as well as the safeguards taken to protect the confidentiality of personal information. The privacy notice should be able to be viewed by a direct link in any agency web site accessed. The provision of this link is the responsibility of the agency.

We noted that 49 of 58 web sites reviewed did not have a direct link to a privacy statement. Some sites do link to a privacy statement, but this statement has not been approved by the OIT governing board.

Recommendation

We recommend that OIT continue its efforts in finalizing the draft privacy statement for approval and distribution, and the CIO strongly encourage all agencies to establish links to this statement on their web sites.

Auditee's Response

As stated, this is a work in progress being coordinated by the Chief Technology Officer's office.

Glossary of Terms

Distributed Server Environment	A network of non-mainframe computers that provide for distributed processes in a multi-tier environment. These tiers include web applications and database servers and communicate with each other by way of ethernet cable or some other method of communication.
Production Environment	The environment where all programs and services run in real time. It should be separate from the development and testing environments.
Cookies	Messages given to a Web browser by a Web server. The browser stores the message in a text file called cookie.txt. The message is then sent back to the server each time the browser requests a page from the server.