Department of the Treasury
Division of Pensions and Benefits
State Health Information Processing System (SHIPS)

May 26, 1998 to December 17, 1998
The Honorable Christine Todd Whitman
Governor of New Jersey

The Honorable Donald T. DiFrancesco
President of the Senate

The Honorable Jack Collins
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 the Treasury, Division of Pensions and Benefits State Health Information Processing System (SHIPS) for the period May 26, 1998 to December 17, 1998.

If you would like a personal briefing, please call me at (609) 292-3700.

Richard L. Fair
State Auditor
January 22, 1999
# 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>Documentation</td>
<td>3</td>
</tr>
<tr>
<td>Change Control</td>
<td>4</td>
</tr>
<tr>
<td>Segregation of Duties</td>
<td>5</td>
</tr>
<tr>
<td>CANOES</td>
<td>6</td>
</tr>
<tr>
<td>Access Security</td>
<td>7</td>
</tr>
<tr>
<td>Operational Continuity</td>
<td>8</td>
</tr>
</tbody>
</table>
Scope

We have completed an audit of the Division of Pensions and Benefits, State Health Information Processing System (SHIPS) for the period May 26, 1998 to December 17, 1998. Our audit evaluated application controls and general controls involved in the processing and maintaining of health benefit coverages. Due to limited documentation, we chose not to review some job streams, edits and transaction processes.

SHIPS was developed in 1997 to handle health benefits administration and accounting for state and participating local employers. SHIPS was also designed to provide efficient and secured access to benefits information for state and local benefit administrators, carriers, and members of the State Health Benefits Program (SHBP). SHIPS maintains the health benefit information for over 280,000 employees and retirees for 1200 payroll locations, and calculates billing of the employers and payments to third party administrators and insurance carriers. Annual billings processed by SHIPS approximate $1.3 billion.

Objectives

The objectives of our audit were to determine the adequacy of application controls and certain general controls relating to the computer processing and maintenance of health benefit coverages.

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, Auditing Computer Applications issued by Auerbach, the Handbook of EDP Auditing issued by Coopers & Lybrand, and Control Objectives for Information and Related Technology (COBIT) issued by the Information Systems Audit and Control Foundation.

In preparation for our testing, we studied available system user, operation, and facility documentation. We also reviewed circular letters promulgated by the State Comptroller, and policies of the Division of Pensions and Benefits. Provisions that we considered significant were documented and compliance with those requirements was verified by interview and observation and through our sampling of system transactions.

A nonstatistical sampling approach was used. Our samples of access privileges, program changes, input and billing processes, and output reports were designed to provide conclusions about the internal control attributes. We selected sample items judgmentally.

Conclusions

Our audit disclosed that some controls exist over computer processing of health benefits data through SHIPS. However, control weaknesses meriting management’s attention exist.

Auditee’s Response

We welcome and appreciate the review that occurred and will act to ensure that the recommendations are expeditiously addressed.
Documentation

Program manuals and documentation should be developed and maintained.

Formal user documentation has not been developed; application documentation is incomplete and limited; and not all job streams currently in production have corresponding descriptions. Program documentation is limited to short narrative descriptions in the body of the source code and does not include program structure and logic flow. Programming change documentation is limited and comprehensive test data and results are not retained.

Management indicated that as a result of the ongoing implementation of SHIPS, user and program documentation is not a priority. Industry experience and accepted business practices dictate that systems and their operational features be documented and protected. COBIT, a framework of desired information technology control objectives, further specifies that adequate user procedure manuals, operations manuals and training materials be prepared as part of every information development, implementation or modification project. Additionally, documentation of the testing of that application should be retained. This documentation is necessary for system maintenance, modification and recovery. When documentation is not created or maintained, the risk of processing errors increases and application changes may be difficult, expensive or impossible to make.

Recommendation

The division and OIT should fully document the application to minimize future maintenance costs and reduce the risk of potential processing errors.

Auditee’s Response

As this application was developed using Joint Application Design (JAD) and Rapid Application Development (RAD) methodologies, documentation for these sessions does exist in the form of JAD notes, data model, program function list and business flow diagrams.
The Office of Information Technology (OIT) recognizes the need for formal documentation at the program level. In the future, as program changes are requested and occur, OIT will include documentation as part of the signoff criteria; or it may be developed as a separate all inclusive request. Nonetheless, OIT will be expanding existing documentation to fulfill the Audit Report recommendation.

Change Control

Our review of the SHIPS change control process noted that in most cases, the only form of documenting programming changes made by the Office of Information Technology (OIT) staff is by entering a brief description of the change, the date and the programmer’s initials in the program header. User manuals with documented procedures for the processing of all changes made to the application are not available and changes are not properly tracked for management and control purposes. COBIT dictates that an application be properly documented and changes tracked to reduce the risk of errors and unauthorized changes to the application.

Our audit tests disclosed that of the eleven items tested, five could not be traced back to the task list, ten did not have the change control test results documented, ten did not have documentation regarding the original client request identifying the problems encountered and four did not have an adequate description of the changes made. We also noted that the tracking numbers assigned to a change control request are not unique and are reused for new requests.

The potential for errors and the chance for unauthorized changes is greater with each subsequent change, impacting the effectiveness and efficiency of the application.
**Recommendation**

We recommend that the division and OIT properly document the change control process to minimize the potential for errors and unauthorized changes.

**Auditee’s Response**

Procedures for tracking production support vs. programming enhancements differ. Generally, production support tasks are placed on the task list if they are deferred or if the effort is estimated to exceed ½ day.

For enhancements or user-generated maintenance changes, starting in August, 1998, interim procedures requiring unique identifying numbers as well as written requests were implemented. The Health Benefits Bureau and OIT will start using the complete change control methodology in the first quarter of 1999.

---

**Segregation of Duties**

Producers should not have access to production data.

Seven programmers have access to transaction processing and are called upon to process failed transactions in production. Due to the dissimilarity between the production and test environments, programmers can not replicate application errors in the test environment. As a result, programmers investigate and fix data errors while in production.

When an agency establishes a data processing organization, proper recognition should be given to internal control, including adequate segregation of duties. The current condition exposes the application to manipulation in that several people have both operational knowledge and access to processing and programs.

**Recommendation**

We recommend the number of programmers with access to production files be reduced and monitored, and the use of program-level security be increased to limit a programmer’s access to the specific programs relative to their responsibilities. We also recommend
the differences between the test and production environments be resolved, so that access to production by programmers can be eliminated.

**Auditee’s Response**

The SHIPS system, as with any new system of this size and complexity, still is encountering some on-line problems. Programmer / analysts have access to production menu functions and are called upon to investigate failed transactions in production. Because the OIT Client Services programming group is off-site at the Riverview complex, they are unable to examine the same results as agency personnel when the problem happens. At this point, they still need this production access to be able to ‘duplicate’ the failed transaction in production.

With the capability that has been given the programmer/analysts, access to information is still restricted by program level security which is tailored and applied in many cases. Every effort will be made to satisfy the recommendation with the end result being that update access to SHIPS information by programmers is eliminated.

---

**CANOES**

Bypassing system edits should be discontinued.

There are five users who have been granted access to a “back door” in the application called CANOES. Of those five, three have access to nine different programs providing for maintenance and update.

All data processed should be required to pass the built-in edits to ensure validity. Currently, some documents that should be successfully processed are rejected by system edits. CANOES was designed to circumvent system edits. The likelihood of improper data and erroneous reporting is increased when information that has not been subjected to normal edits is processed through the application.
**Recommendation**

We recommend management prioritize the correction of the edits and the use of CANOES be eliminated. In the interim, CANOES usage should be limited to a unique management logon id and monitored.

**Auditee’s Response**

As designed, the CANOES system is a short-term maintenance system for handling of exceptional conditions. This need will diminish with the implementation of enhancements to existing production online programs, and this sub-system will eventually be eliminated.

**Access Security**

Inactive logon ids are not entirely deleted. In order to gain access to SHIPS, a user must be granted four different access privileges. They are ACF2, SHIPS Front End, Natural and SHIPS Back End. Our review of the various security tables disclosed that they are not synchronized with one another. We found 16 inactive or terminated logon ids that had only their ACF2 access revoked. Therefore they only need their ACF2 privilege reactivated in order to have access to SHIPS.

We also noted that there are 15 terminated users that still have access to SHIPS. The control in place to determine inactive logon ids is not always being followed. Each month the division’s ISR prepares and sends a security report to each section supervisor. The supervisors do not always return these reports in a timely manner. As a result, inactive logon ids are not being identified, terminated and deleted in a timely manner and may lead to the unauthorized access to and compromising of critical programs and data.

**Recommendation**

We recommend that management ensure the timely identification, termination and deletion of inactive logon ids from all security tables.
Auditee’s Response

All security access for the SHIPS Systems will be reviewed and deficiencies will be corrected by February 1st, 1999.

Operational Continuity

OIT needs to revise and test its disaster recovery and backup plan.

OIT’s predecessor maintained a technical standard mandating that a disaster recovery plan be exercised at the River Road Data Center at least once per year to ensure that it will satisfy the site’s processing requirements. The functions of such tests are to determine the ability to recover key processing components based on a documented set of instructions and assure that the measures in place will enable recovery. OIT has not performed such a test on this application. One primary cause is the lack of sufficient resources. This condition was noted in our prior report on the Year 2000. In the event of an emergency or natural disaster, the state’s ability to restore computer operations and/or recover data will be substantially weakened resulting in the inability of OIT to provide critical SHIPS’ services.

Recommendation

We recognize OIT is in the process of awarding a contract for a hot site, and we recommend that management and the Purchase Bureau expedite the awarding of this contract.

Auditee’s Response

An award should be made to a vendor for a disaster recovery ‘hot site’ by the end of January and a disaster recovery testing schedule will be developed based on application priorities.