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

Department of the Treasury
Office of Management and Budget
New Jersey Comprehensive Financial System

June 1, 2002 to May 6, 2005

Richard L. Fair
State Auditor
The Honorable Richard J. Codey  
Acting Governor of New Jersey

The Honorable Richard J. Codey  
President of the Senate

The Honorable Albie Sires  
Speaker of the General Assembly

Mr. Albert Porrini  
Executive Director  
Office of Legislative Services

Enclosed is our report on the audit of the Department of the Treasury, Office of Management and Budget, for the period of June 1, 2002 to May 6, 2005. If you would like a personal briefing, please call me at (609) 292-3700.

Richard L. Fair  
State Auditor  
September 1, 2005
# 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>Users with Excessive Privilages</td>
<td>3</td>
</tr>
<tr>
<td>Circumvention of the Approval Process</td>
<td>4</td>
</tr>
<tr>
<td>Undocumented Command</td>
<td>5</td>
</tr>
<tr>
<td>Security Logs</td>
<td>5</td>
</tr>
<tr>
<td>Unnecessary Approval Authority</td>
<td>6</td>
</tr>
<tr>
<td>Auditee Response</td>
<td>8</td>
</tr>
</tbody>
</table>
Department of the Treasury  
Office of Management and Budget  
New Jersey Comprehensive Financial System

Scope

We have completed an audit of the Department of the Treasury, Office of Management and Budget (OMB), New Jersey Comprehensive Financial System (NJCFSS) for the period June 1, 2002 to May 6, 2005. Our audit evaluated selected general and application controls related to this system. The selected controls included application maintenance, system backup and recovery, system security, and off-line processing data integrity.

The NJCFS is the central accounting system for the various state departments' accounting records. Its primary function is the recording and processing of financial transactions. A secondary function is to provide reliable accounting data for use in the preparation of financial statements and analysis of financial information.

Objectives

The objectives of the audit were to determine the adequacy of selected general and application controls. These controls include policies and procedures to manage and maintain the system; edits and validations to ensure appropriate data input, processing and output; user authentication to provide system security; and tested backup and recovery methods to enable system 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 was provided by Control Objectives for Information and related Technology issued by the Information System Audit and Control Foundation.
In preparation for our testing, we studied circular letters promulgated by the State Comptroller and policies of the agency. Provisions that we considered significant were documented and compliance with those requirements was verified by interview, observations, and tests of controls. In addition, we obtained and reviewed system administration, security and user manuals. Functions that 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 selected general and application controls were designed to provide conclusions about the adequacy of those controls in place for application maintenance, system backup and recovery, system security, and off-line processing data integrity. Sample transactions were judgmentally selected for testing.

Conclusions

Our review disclosed that general and application controls were in place and functioning for application maintenance, system backup and recovery, and off-line processing data integrity. However, general and application controls for system security require improvements.
Users have the ability to enter, change and apply all levels of approval to a transaction.

Users with Excessive Privileges

NJCFS provides 176 users not only the ability to approve all levels of at least one transaction, but also the ability to enter and change the same transaction type. Our analysis of seven transaction types identified 52 users who processed 73,565 transactions between June 3, 2002 and June 24, 2004 by individually applying all required approval levels. Although the system does not identify who created these transactions, the potential exists for both the entry and approval of these transactions by the same user. The net amount of these transactions was a credit of $1.5 billion, the majority of which were Cash Receipts (CR).

Control Objective for Information and related Technology (CobIT) PO4.4 states that "Roles should be designed with consideration to appropriate segregation of duties. No one individual should control all key aspects of a transaction or event." In accordance with this concept, OMB Circular Letter 95-11 states the following concerning exemptions from the policy requiring segregation of duties: "Any person who is granted this exemption to apply three levels of approval to a transaction will not be allowed to enter or change that transaction." Currently, the department relies on the integrity of the employee granted this exemption not to enter, change or completely approve a transaction. It is believed that no one person will perform the entire transaction; rather, the individual with the exemption will only apply the remaining required approvals for a given transaction. Maintaining such reliance creates the potential for fraudulent or erroneous transactions to go undetected by management. There is a function in the system which, if implemented, will prohibit users from approving a transaction that they enter. A security table option, the R approval action, is available that will prevent a user who entered a batch or a document from applying or removing approvals to those transactions.
Recommendation

We recommend OMB implement the R approval action security option to prevent users who have the ability to apply all levels of approval from being able to perform this task for a transaction which they have also entered, in accordance with the circular letter.

Circumvention of the Approval Process

Users are circumventing the approval process through improper control of passwords.

NJCFS requires multiple levels of approval to be applied to a transaction in order for it to process. These different levels are split between multiple employees as part of the internal control process. One major factor which can prevent an internal control system from being effective is circumvention of controls through collusion. An analysis of applied approvals was performed to assess the effectiveness of this internal control. This analysis identified 12,086 transactions in which the applying of approvals occurred within a short time frame of each other. We tested 3,052 of these transactions by comparing the 102 users involved in these transactions with their leave records to see if a user was out the day an approval was applied under his identifier. We found that in 157, or five percent of the transactions tested, 16 users had seven or more hours of leave time charged in the Time and Leave Reporting System (TALRS) on the day their identifier was used to apply approvals. Of these questionable items, 108 required no other approvals. These 108 transactions were comprised of 76 debits totaling $2.5 million and 50 credits totaling $21 million. These test results indicate user passwords are either intentionally shared or used without the owner's knowledge.
Recommendation

We recommend that OMB reinforce that users are responsible for transactions processed utilizing their identifiers; password sharing is strictly prohibited; and misuse may result in loss of system privileges.

Undocumented Command

NJCF5 contains an undocumented command allowing unauthorized changes to data.

NJCF5 has a command which can be used to override the restriction against changing table data. A user with associated change privileges, using this command, can change data contained in some tables that would otherwise be restricted from changes. There are 1,823 users granted this capability. System security prevents certain tables from being changed by defining change capability as an excluded action for that table. However, the NJCF5 security configuration does not restrict use of the change override O command. This command was not apparent to staff and therefore not included in the excluded actions used to control table data modification. Any user with access to certain restricted tables and authorized to make changes can override the change restriction using this command, thereby allowing unauthorized changes to certain fields. The system does not identify the usage of this command.

Recommendation

We recommend that OMB immediately define the O command as an excluded action on all change restricted tables to prevent its use.

Security Logs

The audit trail for NJCF5 is not adequately secured and monitored.

Various logs are kept to provide an audit trail of users’ actions on NJCF5. The Security Log (SLOG) records user security violations. The SLOG’s access configuration allows users with proper permissions to change and delete violation
entries. Changes and deletions of SLOG entries would corrupt the reliability of the information maintained on user security violations. Access to this log should be restricted to prevent alteration.

The Master Table Inquiry log (MLOG) records table modifications. The MLOG is only kept as a file for five days as a by-product of application backup processing. Printed reports are distributed to individuals originating the logged activity without an independent review. Audit logs need to be maintained for a sufficient period of time to provide proper user accountability. Failure to maintain sufficient information on modifications to table data weakens the audit trail for assuring the integrity of financial data produced by the system.

**Recommendation**

We recommend appropriate restrictions be implemented preventing change and deletion of SLOG entries. In addition, the MLOG should be kept for a sufficient period of time and independently reviewed to allow detection and investigation into table modifications that appear questionable.

>>>

**Unnecessary Approval Authority**

Analyses of approval utilization were performed to evaluate the reasonableness of access afforded to users. We found that during the period July 1, 2002 to June 25, 2004 there were 2,595 users with the ability to partially approve at least one transaction type. Of these users, 894 or 34 percent had not approved a transaction of any type during this period.

In addition, we reviewed the period June 3, 2002 to June 24, 2004 to determine the number of times a user with the ability to apply all levels of approval to a transaction used this capability. We found 820 instances where a user had the ability...
to enter, change, and fully approve a specified transaction type. In 469 or 57 percent of these instances, the user had not approved the specified transaction type during the period analyzed. Some of these instances occur when a user is assigned all levels of approval for a security group covering more than one transaction type, but only has a need to approve selected transactions in that group.

This situation violates the concept of "least privilege". The National Institute of Standards and Technology, Technology Administration, U.S. Department of Commerce Special Publication 800-53 entitled Recommended Security Controls for Federal Information Systems provides us with a standard on least privilege (AC-6): "The information enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks." When an organization does not communicate and enforce a "least privilege" policy, the system becomes more vulnerable.

Currently, there is no process to monitor whether a user with approval capabilities actually uses them. Although there may be an infrequent need for a user to approve a transaction, many agencies could reduce the total number of users with approval capabilities and also reduce the approval levels of other users.

Recommendations

We recommend that OMB perform a review of users with approval authority to determine if approval capabilities should be reduced or removed. Users with all levels of approval for a security group who do not process all of the specified transaction types should have their access reduced to only the transaction types required.
August 26, 2005

Mr. James B. Patterson  
Assistant State Auditor  
Office of Legislative Services  
Office of the State Auditor  
PO Box 067  
Trenton, New Jersey 08625-0067

RE: Departmental Audit Response – Department of the Treasury  
Office of Management and Budget  
New Jersey Comprehensive Financial System

Dear Mr. Patterson:

The Office of Management and Budget (OMB) appreciates the efforts of your staff in their review of the New Jersey Comprehensive Financial System (NJCF). We are working to resolve the findings noted in the audit report and we would like to thank you for giving us an opportunity to comment on the report. The response to the audit team's recommendations follows:

**Users with Excessive Privileges**

*Audit Recommendation* - We recommend OMB implement the R approval action security option to prevent users who have the ability to apply all levels of approval from being able to perform this task for a transaction which they have also entered, in accordance with the circular letter.

*Response* – OMB's opinion is that the information contained in the first paragraph of the report under the heading "Users with Excessive Privileges" is misleading and does not take into consideration other controls that are in place. Of the 73,565 transactions, 63,027 were processed by OMB - Cash Accounting to record dishonored checks, electronic fund transfer failures and bank error corrections in order to reconcile bank statements to NJCFS records. In addition, 95% of the 63,027 transactions were processed by OMB - Cash Accounting staff who are not responsible for the bank reconciliation process; therefore, allowing for proper segregation of duties.

In addition to the 63,027 processed by OMB – Cash Accounting, the OMB - Accounting staff processed 3,250 documents related to interfaces and uploads for either departments or outside third party processors. These transactions are initiated by parties outside OMB and documentation supporting the transaction is required prior to approval in NJCFS.
Also, there were 2,766 transactions processed by employees who have been given an exemption to the circular letter. The exemption is granted based on the requirement stated in the letter granting the exemption that “proper documentation, containing at least one additional authorized signature, must be maintained for all transactions approved by the above individual(s).”

And, there were 708 transactions processed by OMB - Accounting and Financial Reporting staff. These transactions comprise year end adjustments, transfers between the General Fund and agency/trust funds, entries to reconcile grants and other miscellaneous items which are unique and not “assigned” to a department. In this category are the monthly transfers of funds from the Lottery Agency Fund to the General Fund for the Lottery proceeds that support General Fund appropriations. The transfer is initiated by Lottery personnel and the cash receipt is recorded in the General Fund by OMB – Financial Reporting staff. These receipts are reconciled by OMB – Cash Accounting thus providing “checks and balances.” The Lottery receipts comprised a significant portion of the cash receipts credit of $1.5 billion.

The transactions explained thus far total 69,751. OLS was not able to provide detailed information on the remaining 3,813 transactions; consequently, OMB was unable to address them.

In summary, all approval level access is limited to OMB staff or agency personnel through the exemption process for which other controls are in place to compensate for this access. To remove all approval levels in these circumstances would incur undue inefficiency in operations without an appreciable benefit for the increased personnel effort needed to process the transactions. Therefore, OMB will not be implementing the audit recommendation at this time.

**Circumvention of the Approval Process**

*Audit Recommendation* – We recommend that OMB reinforce that users are responsible for transactions processed utilizing their identifiers; password sharing is strictly prohibited; and misuse may result in loss of system privileges.

*Response* - To address this issue, OMB will be changing the system authorization access form to include that statement for the undersigned, “I understand that access to the NJCFS requires the use of User IDs and passwords that are confidential information and are not to be shared. I am responsible for any transaction associated with my User ID.” In addition, periodically the CFS message board and newsletter will remind users that they are responsible for transactions processed under their system identifier and that password sharing is strictly prohibited. Attendees at CFS training sessions will also be reminded of this.

**Undocumented Command**

*Audit Recommendation* – We recommend that OMB immediately define the O command as an excluded action on all change restricted tables to prevent its use.

*Response* – This recommendation has been implemented.
Security Logs
Audit Recommendation – We recommend appropriate restrictions be implemented preventing change and deletion of SLOG entries. In addition, the MLOG should be kept for a sufficient period of time and independently reviewed to allow detection and investigation into table modifications that appear questionable.

Response – The recommended changes in the SLOG have been implemented. The MLOG is currently retained for seven years. OMB believes that this time frame is adequate and it is consistent with most items on the OMB records retention schedule. The majority of the entries on the MLOG report are vendor table updates. These updates are reviewed by the supervisor of the Vendor Control Unit. In addition, documents supporting the table updates are also maintained. All non-vendor table updates on the MLOG are reviewed by the CFS security administrator.

Unnecessary Approval Authority
Audit Recommendation - We recommend that OMB perform a review of users with approval authority to determine if approval capabilities should be reduced or removed. Users will all levels of approval for a security group who do not process all of the specified transactions types should have their access reduced to only the transaction types required.

Response – While OMB agrees theoretically with the recommendation, the current configuration of the security groups within NJCFS have reached the maximum allowed. Since it is not possible to establish security by individual transaction types, users must be given access to all transaction types within a specific group even though they may only use one transaction type. OMB will initiate a security review by department to determine, to the extent possible, reduction in access or approval capability that is currently not being used.

OMB currently receives reports on employees that have separated from state service or have been transferred between departments. The NJCFS security administrator deletes access to NJCFS for separated employees. For employees that are transferred between departments, security access to the “leaving” department is removed. The “receiving” department must submit a system access request to establish access for the transferred employee.

Sincerely,

[Signature]
Charlene M. Holzbaur
Director

ciq