Judiciary
Administrative Office of the Courts
Central Automated Bail System (CABS)

April 6, 1998 to December 31, 1998

Richard L. Fair
State Auditor
The Honorable Deborah T. Poritz  
Chief Justice of the Supreme Court  

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  


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

Richard L. Fair  
State Auditor  
March 24, 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>Security Policy</td>
<td>3</td>
</tr>
<tr>
<td>Logonids</td>
<td>4</td>
</tr>
<tr>
<td>Access to Security Classes</td>
<td>5</td>
</tr>
<tr>
<td>Record Modification</td>
<td>7</td>
</tr>
<tr>
<td>Programmer Error Correction</td>
<td>8</td>
</tr>
<tr>
<td>System Modifications</td>
<td>9</td>
</tr>
</tbody>
</table>
Scope

We have completed an audit of the Central Automated Bail System (CABS) computer application, within the Administrative Office of the Courts (AOC), for the period April 6, 1998 to December 31, 1998. Our audit evaluated application controls and selected general controls involved in the processing of bail data through CABS.

CABS is a statewide online mainframe based application, designed during fiscal year 1994 and implemented during fiscal year 1995 to coincide with the state takeover of the county court systems. CABS’ objectives were to automate the recording of the collection, disbursement, and reporting of bail, provide the ability to track modifications to the bail, support central disbursement of all bail funds via Treasury, and allow local and statewide bail inquiry. Since the implementation of CABS, there have been 247,000 bails issued, representing $1.7 billion.

Objectives

The objectives of our audit were to determine the adequacy of application controls and selected general controls as they related to asset safeguarding, bail data processing, and access to system data.

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 standards set forth in Control Objectives for Information and Related Technology (COBIT) by the Information Systems Audit and Control Association (ISACA), and the Handbook of IT Auditing, 1998 edition, by Warren, Edelson, Parker and Thrun.
In preparation for our testing, we studied legislation, Rules Governing the Courts of the State of New Jersey, and policies of the agency. In addition, we reviewed the manuals and documentation of the database product CA-IDMS; the security product CA-ACF2, and the CABS system. Provisions that we considered significant were documented and compliance with those requirements was verified by interview and observation and through our sample of bail transactions. We also interviewed agency personnel to obtain an understanding of the application, its environment and internal controls.

We performed tests at five vicinages. A nonstatistical sampling approach was used. Our samples of bail transactions were designed to provide conclusions about the internal control attributes. We selected sample items judgmentally.

**Conclusions**

Our review disclosed that some controls exist over computer processing of bail. However, control weaknesses meriting management’s attention exist.

**Auditee’s Response**

Thank you for the opportunity to comment on the CABS audit report. You will note that the AOC has begun the process of implementing several of your recommendations.

Thank you and your staff for a comprehensive audit and the opportunity to respond to the findings.
The AOC should implement their Information Security Standards policy. The AOC has not implemented a security policies and procedures manual for the Judicial Telecommunications Network. An Information Security Standards policy was written in May 1994, but was never approved, implemented and disseminated to users of the Judiciary Telecommunication Network. The policy has not been written into Judiciary’s Administrative Code and has been pending in Judiciary’s Policy Committee since May 1994.

Lack of security policies and procedures weakens the internal control environment throughout the organization. Some weaknesses noted were logonids and passwords affixed to employees’ monitors, employees sharing logonids and passwords, and terminated employees still having active logonids.

Recommendation

We recommend the Judiciary’s Policy Committee write the standards policy into the administrative code and that the AOC then disseminate the policy.

Auditee’s Response

The current Judicial security policies and procedures document will be updated and formalized for distribution to all Judiciary personnel. In addition, security policies will be emphasized during scheduled Vicinage Finance Manager policy and procedure review sessions.
Logonids

In a test of the Judicial Telecommunication Network’s logonids we found conditions which can allow unauthorized system access.

Five logonids with dates of last access of 00/00/00 (which never set their password) can be used to gain unauthorized system access to the CABS application. One of these has full access to the CABS application.

Thirty one logonids have not been canceled and six logonids have not been suspended in accordance with security deletion procedures covering non use. Thirteen had not accessed the system in over a year.

Ten employees who terminated employment from 1 to 2.5 years ago still have active logonids.

The AOC’s draft security deletion procedure states, “weekly, a report is produced of ids which have not been used in the last 90 days. This report is reviewed manually and any id which should be marked for deletions is SUSPENDED. Weekly a report is produced of all ids which are suspended. Sixty days after the ids are suspended . . . a batch job sweeps the ACF2 files and deletes any id which is still suspended.”

Furthermore, COBIT states, “Control over the IT process of ensuring systems security . . . to safeguard information against unauthorized use, disclosure or modification, damage or loss is enabled by logical access control which ensures that access to systems, data and programs is restricted to authorized users.”

The AOC has not implemented the Information Security Standards policy, leading to these weaknesses.

Recommendation

We recommend that AOC implement and disseminate their policies on the deletion of logonids of terminated employees, the suspension of logonids that are not used, and the initial issuance of logonids and subsequent follow up of their use.
Auditee's Response

The AOC Information Systems Division is in the process of implementing automated logonid maintenance procedures to ensure appropriate suspension and deletion of logonids.

Instructions will be incorporated into the security policies and procedures manual for supervisors of system users regarding initial issuance, monitoring and deletion of logonids.

Access to Security Classes

Access to CABS is divided into nine currently used security class codes based on the accounting function needed to process the bail as defined by the Data Base Administration and Security team. Employees, however, are routinely assigned either “inquiry only” access or “full” access to the CABS system. Only 35 percent (66 out of 191) of CABS users with more than “inquiry only” access have their CABS access authorities limited, based on their job duties and accounting functions, by Vicinage Bail Managers, who request access for their employees from their Vicinage Information System Representative.

Also, we noted 179 users with access codes of 02 (the entering/modifying of bail information) and 10 (refund of bail) have the ability to change critical data such as the address of a surety, bail dollar amounts, bail type or the status of a bail. There are no on-line edits, edit reports or reviews by supervisors that will detect improper changes of critical data. This creates a weak environment subject to unauthorized use of bail funds.

Further analysis of access to security class codes revealed that 63 percent (120 out of 191) of vicinage CABS users with more than “inquiry only” access have access to security class 06 (the Disbursement Maintenance screen) used to void disbursements by Judiciary’s Cash Control Unit. The CABS training guide states that disbursement maintenance is not accessible to vicinage personnel. Vicinage CABS users with access to security class 06 have the ability to void disburse-
ments and create opportunities to make multiple disbursements from one bail account. We found 216 void disbursements processed by vicinage staff since the inception of CABS.

**Recommendation**

We recommend that the AOC management mandate a statewide effort by Vicinage Bail Managers to scrutinize CABS system access and develop a uniform assignment of security class codes granted to CABS users based on their specific job duties and accounting functions. This will assist in providing proper segregation of duties for enhanced internal control. We further recommend creating a separate security level for demographic changes to bail refunds and assigning this level to only one or two persons in each vicinage. Additionally, system changes should be made to provide edit reports detailing address changes for supervision review. Finally, we recommend that the 120 vicinage users with access to security class 06 have that access removed by the AOC.

**Auditee’s Response**

The vicinages are in the process of consolidating financial duties and responsibilities under a single manager who will provide financial supervisory oversight of the Bail Units. AOC financial management and the Judiciary Vicinage Finance Division Managers will review the current list of CABS users and their job duties and identify the need to realign security class codes, as appropriate. This will ensure adequate segregation of duties. Security class 06 will be removed from vicinage users.
Record Modification

Improvements to current input controls can reduce the risk of unauthorized transactions.

CABS will allow the surety name and address fields to be changed in any bail status other than refund. The ability to change name and address information provides the opportunity for fraudulent transactions. System controls provide that the changes are noted in the surety portion of the bail record, however, there are no procedures for supervisory review of these changes.

When a defendant appears for trial, the surety is due a refund of the bail posted; failure to appear will result in forfeiture of the bail. The initial step in processing a bail refund or forfeiture is the issuance of a notification which is generated by CABS. There are over 3000 bails totaling $6.8 million which are in refund pending status and 3900 forfeitures pending totaling $34 million. Bails remain in the refund pending status until the surety contacts the vicinage office or for ten years at which time the funds are escheated to the state. Bails remain in forfeiture until there is either a judgment or the surety has the forfeiture set aside. Both of these actions require intervention by vicinage staff. Funds in both states are at risk because there are no controls to prevent material changes to the data, such as the changing of surety names or addresses. These changes could result in an improper disbursement of bail funds. Good internal controls require system edits to prevent or detect unauthorized changes to system data.

Additionally, in order to process bails that were posted to county records prior to the state unification on January 1, 1995, AOC created a feature to CABS named backloading. Analysis and testing of this feature disclosed that adjustments and modifications to backloaded bails are not included in the daily bail activity journal and are therefore not subject to management review.

Recommendation

We recommend the AOC establish procedures that provide adequate authorization for any changes to surety name or address. In addition, system edits should be established to automatically change the status of any bail that remains in the refund pending or forfeiture status for more than 120 days. Any further processing
of these bails should be processed by a control unit within AOC. The practice of back-loading bails should be restricted to a minimum of AOC central staff and require management approval.

Auditee’s Response

As mentioned above, AOC financial management and the Judiciary Vicinage Finance Division Managers are reviewing the Bail Security classes. In addition, AOC and vicinage finance division managers have recently formed a Bail workgroup which will be addressing needed financial enhancements to CABS, including the establishment of management control of changes to sensitive information such as surety name and address and longstanding bails pending refund.

Programmer Error Correction

Our review of CABS disclosed that a lack of segregation of duties existed in the error correction procedures. AOC only recently developed an online function for use by the Criminal Practice staff to correct bails when the status is erroneously set to refund pending. Previously, system programmers were responsible for resetting the bail status to facilitate the continued processing of bails in certain situations. In addition, we noted that any changes made to database records by programmers did not appear within the bail history records and were therefore not subject to review. Although this responsibility was removed from system programmers, the ability to reset bail status was not, resulting in a lack of segregation of duties.

Recommendation

We recommend that AOC remove the ability to reset bail status from system programmers.

Auditee’s Response

The AOC has identified the need to expand the online correction capability. Until this capability is in place, programmer assistance is necessary to initiate corrective entries when bails are forfeited, discharged or transferred.
System Modifications

System modifications can lead to a more efficient and effective operation.

Analysis of approved system modifications requested by CABS users disclosed that no action has been taken. CABS has procedures which allow users to request system modifications. The process has identified 36 projects which are pending programmer action dating back to December 1995. CABS is not given a high priority for AOC programming resources. Several of the changes requested could expedite operations at the vicinage level and others could improve AOC’s ability to monitor and control system operations.

Recommendation

We recommend that AOC review the status report of pending CABS modifications and assign the necessary resources to complete priority program changes.

Auditee’s Response

A CABS sub-committee is currently being organized. This committee will identify CABS modification priorities and the need for resources.