Office of the State Auditor

Audit Report

Department of the Treasury
Office of Telecommunications and Information Systems
River Road and Barrack Street Data Centers

March 6, 1995 to September 30, 1995
# Audit Report

## Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Transmittal Letter</td>
<td>1</td>
</tr>
<tr>
<td>Scope</td>
<td>3</td>
</tr>
<tr>
<td>Objectives</td>
<td>3</td>
</tr>
<tr>
<td>Methodology</td>
<td>4</td>
</tr>
<tr>
<td>Conclusions</td>
<td>4</td>
</tr>
<tr>
<td>Findings and Recommendations</td>
<td></td>
</tr>
<tr>
<td>Operational Continuity</td>
<td>5</td>
</tr>
<tr>
<td>Preservation of Operating System Software Integrity</td>
<td>6</td>
</tr>
<tr>
<td>Implementation and Administration of ACF2 Security Software</td>
<td>7</td>
</tr>
<tr>
<td>Departmental Response</td>
<td>10</td>
</tr>
</tbody>
</table>
We have completed an audit of selected general controls for the Department of the Treasury, Office of Telecommunications and Information Systems (OTIS), River Road and Barrack Street Data Centers for the period March 6, 1995 to September 30, 1995. The objectives of our audit were to determine whether management controls existed to provide for operational continuity and preservation of operating system software integrity. We also tested to determine if security software was adequately implemented and administered, and whether related issues noted in our prior report on the HUB Data Center were resolved.

In each of these areas we noted improvements which should be made. The continued processing of vital applications can be threatened if disaster recovery preparedness is not strengthened. In addition, the operating system software integrity could be compromised if proper segregation of duties is not maintained in the change process. We also found that the risk of improper access should be reduced. Details of the findings and recommendations are included in our report.
This audit was conducted pursuant to the State Auditor’s responsibilities as set forth in Article VII, Section 1.6 of the State Constitution and Title 52 of the New Jersey Statutes.

Richard L. Fair
State Auditor
Scope

We have completed an audit of the Department of the Treasury, Office of Telecommunications and Information Systems (OTIS), River Road and Barrack Street Data Centers for the period March 6, 1995 to September 30, 1995. Our audit included selected general controls over the preservation of system integrity for the operating system MVS/ESA 4.2.2 and implementation and administration of security software (ACF2). We also included the disaster recovery capabilities of the centers. This audit was performed for processing environments installed on the data centers’ IBM and IBM compatible mainframe computers, maintained to support the operation of production applications at these data centers. The prime responsibility of the River Road and Barrack Street Data Centers is the provision of information processing service and support to client agencies. Several critical client agency computer applications run in the IBM and IBM compatible environments maintained at these data centers. As a result, the assurances provided by the data centers’ internal control environment for application processing have a direct impact on the client agencies’ abilities to perform critical automated functions.

Subsequent to our audit period, implementation of the operating system MVS/ESA 5.1.0 was completed for all OTIS IBM and IBM compatible operations. This condition does not impact those areas requiring improvement as noted in this report and is being disclosed to identify its exclusion from this audit.

Objectives

The objectives of our audit were to determine whether management controls existed to provide for operational continuity and preservation of system integrity. We also tested to determine if ACF2 was adequately implemented and administered, and whether related issues noted in our prior report on the HUB Data Center were resolved. This audit was conducted pursuant to the State Auditor’s responsibilities as set forth in Article VII, Section 1.6 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.

In preparation for our testing, we studied circular letters promulgated by the State Comptroller and policies of the agency. Provisions we considered significant were documented and compliance with those requirements was verified by interview and observation and through our analytical processes and attribute samples. We also read vendor supplied manuals and interviewed agency personnel to obtain an understanding of the software programs installed and the related internal control structure.

A nonstatistical sampling approach was used. Our samples of system files and records were designed to provide conclusions about the adherence to internal control and compliance attributes. Sample items were selected based on auditor’s judgment.

To ascertain the status of findings included in our prior report on the HUB data center, we identified corrective action, if any, taken by the agency and walked through the system to determine if the corrective action was effective.

Conclusions

In each of the areas tested, we noted improvements which should be made. These improvements include the following:

C Annual testing of the policies and procedures maintained for disaster recovery should be performed;

C Proper segregation of duties, evidence of supervisory approval and related documentation of events within the system software change control process should be maintained.

We also found that the agency has not resolved all of the issues noted in our prior report on the HUB Data Center. Matters related to the issuance of formal security policies and standards, the assignment of powerful system access privileges, and disaster recovery have not been resolved. These issues have been updated and restated in our current report, as they also affect these data centers.

Details of our findings and recommendations follow.
Operational Continuity

OTIS maintains a disaster recovery plan for its data centers. This is necessary to ensure that crucial applications experience very little interruption in the event of a disaster. We found that procedures for the resumption of emergency processing in the event of a disaster have not recently undergone required annual testing.

The OTIS Technical Service Standardization Plan states that the disaster recovery plan must be exercised at each OTIS data center at least once a year to insure that it will in fact satisfy a 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 in fact enable recovery.

This condition was noted in our prior report on the HUB Data Center. OTIS has partially resolved the conditions presented in that audit report. In doing so, the agency has identified that it does not maintain the required back-up hardware to recover all applications defined as supporting critical client functions. These functions include major revenue collection processing and public safety information dissemination. As a result, OTIS may not be able to recover timely from an interruption of data processing services in the event of a disaster at one of its data centers.

We recommend that management provide the necessary capacity to allow for the annual testing of the disaster recovery plan to ensure that all applications supporting critical client functions can resume emergency processing at an alternate site in the event of a disaster at any of its data centers.
Preservation of Operating System Software Integrity

OTIS has established a Change Management System for the purpose of effectively managing changes made to the production systems. This system uses the Change Management facility of a program named Information/Management to create change records which identify and track activities necessary to properly implement a requested change. In our review of this system, we found the controls do not provide assurance that a change has been made in accordance with established policies and procedures.

During the change process, controls must be employed to assure that modifications are properly requested, tested, documented and authorized for production. In designing controls, the fewer users with multiple capabilities, the more control over a change record and its data. Proper segregation between assignment, installation, approval and implementation should be maintained. In addition, adequate tracking data should be maintained about change activities, responsibilities and timing. This data should provide a chronological view of the change so as to identify and perform the activities necessary to implement the change.

The change control policies and procedures established by OTIS in conjunction with the Change Management facility of Information/Management do not provide for the proper segregation of duties, do not require evidence of supervisory review and do not define a standard for complete documentation of the process. Specifically, we noted that:

C Users assigned to all privilege classes established for the Change Management facility have the authority to assign, enter, update and close a change record owned by the respective class.

C Only 32 change records, representing four percent of change records with an implementation date occurring during the audit period contained documented approvals.

C In a sample of 34 change records, only four utilized activity records to describe the activities associated with a change.

As a result unauthorized changes could be made without timely detection.
We recommend that management define user capabilities in accordance with the tasks to be performed to provide for the proper segregation of duties. In addition, management should establish the appropriate procedures to ensure that all changes are properly approved and change activities are documented.

Implementation and Administration of ACF2 Security Software

Security Policies and Standards

OTIS is responsible for administering the access control environment for processing performed on the mainframe computers at its data centers. A decentralized environment, which establishes control at the user agency and is managed by security software, is currently maintained.

An effective control environment requires security software to be used in accordance with policies and procedures. A security policy is necessary to determine the correct functioning of the access control environment. Maintaining adherence with developed standards and procedures ensures that defined control objectives are met and the desired level of access is sustained.

As reported in our audit of the HUB Data Center, OTIS lacks formal policies and standards that specify how security over mainframe computer data and resources is to be implemented. To date, a 1990 draft document entitled “Information Security Standards and Guidelines,” establishing appropriate standards for this critical area has not been approved by management. In addition, no documented operating procedures exist for the administration of the security software. Management’s failure to provide formal policies and standards and the lack of documented operating procedures increases the risk that improper use of data and resources may occur without immediate detection.

We recommend that OTIS management:

C Develop and promulgate policies and standards to enforce security and enhance controls. The policy should be disseminated as an authoritative directive or circular letter to the client agencies. This directive should provide guidelines to client agencies regarding...
mainframe security and define responsibility for its related administration.

C Develop and maintain operating procedures to ensure the effective administration of access to data and resource processing performed on OTIS’ mainframe computers.

Access to System Data and Resources

The Access Control Facility (ACF2) version 6.1 is the current data security software installed on the state’s IBM and IBM compatible mainframe computers operating at the OTIS data centers. ACF2 provides protection against unauthorized destruction, disclosure, or modification of system data and resources. ACF2 operates as an extension of the operating system and provides this protection by default. All access requires explicit authorization. A logon ID and password are used to authenticate the person accessing the system. The level of access is dependent on the ACF2 rules and privileges granted to a logon ID. ACF2 has defined powerful privileges that grant wide access to data and can allow for the changing of other users’ access rules and privileges.

During our review of ACF2, we noted the following conditions which appear because management has not adequately restricted certain privileges.

C Industry standards recommend that Security and Account privileges be mutually exclusive to ensure proper separation of functions. Our audit noted high instances at both the River Road and Barrack Street Data Centers where users were granted both Security and Account privileges. In total, there were 44 users at Barrack St. and 57 users at River Road with both Account and Security privileges. Such privileges give the user the ability to establish, modify or delete a logon ID record while granting access to data.

C An excessive issuance of Noncancel privileges was noted at each data center. In total, 45 individuals have a logon ID that includes the Noncancel attribute. The Noncancel attribute prevents the user from being canceled from a session due to security violations. This privilege gives the user the ability to read, write to and execute any system or application program or file. The fewer users with such privileges the greater the control.
Users with the Restrict attribute do not require a password for verification and there should be a compensating control over their access. A number of these logon IDs do not have this additional controlling attribute that would properly restrict its usage. This condition was noted at both data centers. Out of 651 users listed at Barrack Street and 602 users listed at River Road, 38 and 32 of the respective users do not have the appropriate compensating control.

These conditions increase the risk that improper or unauthorized access and use of restricted computer system data and resources may occur without immediate detection.

**We recommend** that OTIS management:

- Assign Security and Account privileges in a manner consistent with industry standards which recommend that these privileges be mutually exclusive.

- Reduce the number of users who have been assigned the powerful Noncancel privilege.

- Assign the appropriate controls to users with the Restrict attribute in order to compensate for the lack of password verification.