

## Table of Contents

	<b>Page</b>
Transmittal Letter .....	1
Scope .....	3
Objectives .....	3
Methodology .....	4
Conclusions .....	4
Findings and Recommendations	
Operational Continuity .....	4
Implementation and Administration of the Bull Security System	
Security Policies and Standards .....	5
Independent Security Administrator .....	6
Security System Options .....	7
Departmental Response .....	9

This page was intentionally left blank.

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 selected general controls for the Department of the Treasury, Office of Telecommunications and Information Systems (OTIS), HUB Data Center - BULL Operating Environment for the period July 22, 1996 to October 30, 1996.

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

Peter M. Guilfoyle  
Assistant State Auditor  
December 12, 1996

This page was intentionally left blank.

**Department of the Treasury**  
**Office of Telecommunications and Information Systems**  
**HUB Data Center - BULL Operating Environment**

***Scope***

We have completed an audit of the Department of the Treasury, Office of Telecommunications and Information Systems (OTIS), HUB Data Center-BULL Operating Environment for the period July 22, 1996 to October 30, 1996. Our audit included selected general controls over the protection of logical computer files for the operating system General Comprehensive Operating Supervisor 8(GCOS8) and the implementation and administration of the File Management Supervisor (FMS) security software. We also included the disaster recovery capabilities of the center's BULL operations. This audit was performed for processing environments installed on the data center's BULL mainframe computer, maintained to support the operation of production applications at this data center. The prime responsibility of the HUB Data Center - BULL Operating System is the provision of information processing service and support to the Department of Human Services. Several critical computer applications run in the BULL environment maintained at this data center. As a result, the assurances provided by the data center's internal control environment for application processing have a direct impact on the Department of Human Services' abilities to perform critical automated functions.

***Objectives***

The objectives of our audit were to determine whether management controls existed to provide for protection of data and files residing on the BULL mainframe computer. This included tests to determine if FMS was adequately implemented and administered, and whether data and files are recoverable in the event of a disaster. 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.

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 master catalogs 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.

## *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 Security policies and procedures should be developed and promulgated. These need to include proper segregation of duties.

Details of our findings and recommendations follow.

## **Operational Continuity**

**O**TIS needs to test its disaster recovery plan to assure continued processing in the event of a disaster at the HUB data center.

The OTIS Technical Service Standardization Plan states that a 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. OTIS contracted for a hot site at Billerica,

Massachusetts in August of 1996 and has developed a disaster recovery plan for its BULL operation. To date OTIS has not performed a test of its disaster recovery plan. The issuance of approximately 24,000 checks per day totaling over \$6.4 million that provide assistance services to vulnerable populations within the state, would be delayed for each day the computer applications are not operational.

We recommend OTIS perform its scheduled test of the BULL disaster recovery plan and comply with its own standard of yearly testing.

<sup>1</sup>/<sub>4</sub>/<sub>2</sub>

## **Implementation and Administration of the Bull Security System**

### *Security Policies and Standards*

OTIS is responsible for administering the access control environment for processing performed on the mainframe computers at its data centers. This includes the Bull computer system which resides at the Hub data center. Like the IBM and IBM compatible environments, the Bull system operates in a decentralized environment. This type of environment provides control at the user agency and is managed by the security system which resides in the GCOS 8 operating system.

An effective control environment requires the development and implementation of adequate security standards, policies and procedures.

**I**mplementing security standards is necessary to ensure the control environment protects access to the computer system.

OTIS has not disseminated formal policies and standards that specify how security over the Bull mainframe computer system and its resources is to be implemented. This increases risk due to the lack of computer security awareness. In a computer system environment that processed 9 million disbursement transactions totaling \$2 billion for the fiscal year 1996, a sound security policy is necessary to provide guidance for the protection of computer data and resources.

OTIS management should 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 include, but not be limited to, general security controls, administrative controls and logical access controls.

### *Independent Security Administrator*

The security administrator in a computer system environment is responsible for implementing, maintaining and enforcing computer security and its related policies of an organization. The security administrator is also involved in the preparation and testing of a disaster recovery plan.

An effective system of internal controls requires proper segregation of duties. Segregation of duties is necessary to help prevent or reduce the risk of unauthorized access and use of computer data and programs.

OTIS does not have an independent security administrator for the Bull computer system. Currently, the security administrator functions are performed by four systems programmers whose responsibilities also include maintaining and monitoring system software (programs and utilities). The system software controls the functions of the computer hardware and the interaction with the applications programs. The security administrators functions, including user id and access code administration, should not be performed

**D**esignating a security administrator who is independent of systems programmers strengthens the controls.

by systems programmers. By granting excessive access systems programmers, who have the technical expertise, could exploit program weaknesses. Additionally, unauthorized modifications or access to system data and resources may be performed and go undetected.

OTIS management should assign the duties of security administrator for the Bull computer system to a person who is separate from systems programmers. The function of the security administrator should be performed by an independent person or centralized unit within the OTIS organization. In addition to normal duties, the security administrator should be delegated the authority to monitor and scrutinize

Bull system access and to deny or terminate privileges and logon id's when they violate reasonable standards for proper control.

### *Security System Options*

Implementing effective security options in an environment that relies on a computer to run complex applications and process critical transactions is an effective control element necessary to ensure access and use of the computer system and its resources are protected and attempts to breach system security is detected.

In the Bull environment, security begins with the operating system and continues with the FMS (File Management Supervisor). There are also additional optional security packages. FMS's structure provides the most basic security control while optional packages provide additional centralized control over system access; protection of classified data, resources and processes; remote batch security; and logging and recording of security violations.

An effective control system in a computer processing environment requires the design and implementation of adequate logical access controls designed to protect the system against unauthorized admission and use. Security software automates access controls by identifying and verifying user attempts to gain access to computer data and its resources.

OTIS lacks Bull security options that would assist management in providing effective protection of the computer system. The system security in place does not provide non-displaying or obliterating of passwords, encryption of passwords and provide system output of logged security events. This increases the risk that the computer system may not be free from improper access and use and attempts to breach system security may go undetected.

We recommend that OTIS management evaluate the current security system in place and add options that would ensure computer data and its resources are protected and attempts to breach security do not go undetected.

This page was intentionally left blank.

**State of New Jersey**  
OFFICE OF THE TREASURER  
CN-002  
TRENTON, NJ 08625-0002

**CHRISTINE TODD WHITMAN**  
Governor

**BRIAN W. CLYMER**  
State Treasurer

DEPARTMENTAL RESPONSE

December 9, 1996

**TO:** Richard L. Fair  
State Auditor

**FROM:** Brian W. Clymer  
State Treasurer

**SUBJECT:** Comments on Audit Report - Hub Data Center  
Bull Operating Environment

I appreciate your independent review of OTIS relative to whether management controls exist to provide protection of the data and files residing on the BULL mainframe environment, the general controls over the protection of logical computer files for the operating system and the implementation and administration of the security software, and whether data and files are recoverable in the event of a disaster.

Your audit report has been reviewed in detail, and I would like to provide the following comments.

**OPERATIONAL CONTINUITY**

OTIS recognizes the importance of being able to recover processing in the event of a disaster. We have also commented previously to audit findings and recommendations concerning operational continuity. The major issue with backup and recovery begins with funding. With the Bull environment, as indicated in your report, we recently completed the acquisition of a hot site in Massachusetts to accommodate testing of our plans and to be our disaster recovery site.

During the period of December 3 through 9, 1996 we are performing our initial test of the Integris hot site at Billerica, Massachusetts. Our efforts in this test contain the migration of data bases, the linking of a network to connect Trenton facilities with Billerica, and to process data with a return to the HUB to verify performance and accuracy. A report will be issued approximately December 15, 1996, detailing those results and to assess the performance of this facility as a disaster site.

*New Jersey Is An Equal Opportunity Employer - Printed on Recycled Paper and Recyclable*

Richard L. Fair  
December 9, 1996  
Page 2

## IMPLEMENTATION AND ADMINISTRATION OF THE BULL SECURITY SYSTEM

### Security Policies and Standards

OTIS agrees the implementation of security standards is necessary to ensure that the control environment protects access to the computer system. The OTIS Security Standards are now assessable statewide on the INFOMENU. We will continue to review the security area and will develop appropriate policies and guidelines on the Bull environment, particularly after we have had an opportunity to review the results of the Billerica test.

### Independent Security Administrator

The appointment of an independent security administrator is a desirable approach, but is limited by some key issues involving technical knowledge, funding, and working relationships.

OTIS is aware of the need for security administration. We will continue to address the security administration issue. Much of the security software, within the Bull environment, has been developed by our systems programming staff due to the lack of availability of extensive BULL and third party software. This adds to the complexity of this security administration position. This is especially apparent in the teleprocessing monitor area.

### Security System Options

The availability of security software is much more limited in the BULL world, especially in the teleprocessing monitor area. OTIS will continue to monitor vendor offerings for suitable security software for the BULL environment.

rg