ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

October 20, 2003

Mr. Michael McCormack
Director
Office for Technology
Empire State Plaza
Albany, NY 12220-0062

Re: General Controls at the Consolidated State Data Centers
Report 2002-S-46

Dear Mr. McCormack:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution and Article II, Section 8 of the State Finance Law, we have audited the policies and procedures used by the Office for Technology (OFT) to provide appropriate security controls over the operation of the State's computer data centers. Our audit covered the period January 1, 2002 through February 28, 2003.

A. Background

The Data Center Consolidation Plan was developed in January 1998 to merge New York State's agency-specific mainframe data centers into a unified, centrally managed data center operation to support agency customer service applications. Prior to the consolidation, each State agency was responsible for the maintenance and operation of its own data center, including the provision of adequate security over those centers. Through the operation of its data centers, OFT is the primary provider of computer services for over 20 State agencies. Consolidating these operations was expected to save about $18 million per year.

The three consolidated data centers, which are located in Albany and operated by the Office for Technology (OFT), support the data processing requirements of over 150 State agency computer applications. Many of these applications contain personal information about New York State citizens and other information that is confidential or sensitive in nature. This information includes driver license, vehicle registration, traffic and parking violation information; birth and death certificates; marriage licenses; drug prescription and Medicaid information; certain patient treatment information; and personal and corporate State income tax data.

At the three data centers, there are over 30 mainframe computers, approximately 500 computer servers, and four major print centers. OFT officials estimate that approximately 450 computer servers comprise the State's Human Services Network that supports the State's Child and Public Welfare programs. The remaining servers are primarily dedicated to supporting agency e-mail systems, web-based applications that are part of the State's electronic commerce initiative, and file storage. More than 300 OFT employees staff the three data centers, each of which presently has its own command center. OFT is in the process of creating a single command center to support all three data centers. OFT also maintains a separate disaster recovery site that currently supports only specific aspects of the State's Medicaid system.

OFT enters into Service Level Agreements (SLAs) with its State agency customers for the provision of data center services, including mainframe systems that provide computing capability for agencies' applications; back-up services; report preparation; and data and system recovery services in the event of disaster. According to the SLAs, security will be provided to agency customers at a level not less than that required by Federal and State law, regulation or policy. OFT is responsible for keeping data center agency systems available 24 hours a day. Customer agencies are responsible for, among other things, authorizing access rights to their applications, and maintaining and controlling lists of authorized users. These agency customers rely on OFT to ensure that general controls (i.e., information system security controls and disaster preparedness) at data centers are adequate to protect the integrity of their systems and data.

B. Audit Scope, Objectives and Methodology

Our audit examined controls over the processing of electronic data on mainframe computers and servers at OFT's data centers for the period of January 1, 2002 through February 28, 2003. The objectives of our performance audit were to determine whether OFT has instituted security controls that effectively protect the integrity of data centers' computer systems and data, and whether OFT has developed an adequate plan to ensure the continuous processing of critical data in the event of a disaster at the data centers. The scope of our audit did not include doing a vulnerability assessment of the data centers' systems by using a commercial vulnerability assessment product, or by attempting to hack in and infiltrate data center systems.

To accomplish our objectives, we interviewed OFT officials and reviewed pertinent OFT policy and procedures relating to the overall computer operations of the data centers. We also reviewed relevant information and reports related to security and service continuity planning at the data centers. In addition, we interviewed select agency officials about their procedures for backing up critical agency data. Our review covered controls over organization and management, system software and hardware, and security related to data center operations.

We did not review controls over the data centers' customer agency applications. Individual agencies are responsible for establishing effective application controls (e.g., security administration over on-line access to agency systems; system development and maintenance; input and output controls) over their systems that are operating at the data centers. For example, the Department of Motor Vehicles is responsible for developing and implementing application controls over the Driver's License Issuance System.

We conducted our audit in accordance with generally accepted government auditing standards. Such standards require that we plan and perform our audit to adequately assess the OFT operations included in our audit scope. Further, these standards require that we understand OFT's internal control structure and its compliance with those laws, rules and regulations that are relevant to the operations included in our audit scope. An audit includes examining, on a test basis, evidence that supports transactions recorded in the accounting and operating records and applying any other auditing procedures we consider necessary in the circumstances. An audit also includes assessing the estimates, judgments and decisions made by agency management. We believe our audit provides a reasonable basis for our findings, conclusions and recommendations.

We use a risk-based approach when selecting activities to be audited. This approach focuses our audit efforts on those operations that have been identified through a preliminary survey as having the greatest probability for needing improvement. Consequently, by design, we use finite audit resources to identify where and how improvements can be made. We devote little audit effort to reviewing operations that may be relatively efficient or effective. As a result, our audit reports are prepared on an "exception basis."

C. Results of Audit

Detailed results of our audit were provided to OFT officials during the conduct of our audit. The details of our findings and recommendations are not identified here due to the sensitivity of the information and potential risk associated with release of such information. As part of our audit, areas for improving security and disaster readiness were identified and presented to OFT, and OFT officials indicate that they are making efforts to improve the areas identified by the audit. Further, OFT officials indicate that they will meet regularly with us to discuss their strategies for addressing the audit recommendations. Their comments have been considered in the preparation of this report and are included as Appendix A.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Director of the Office for Technology shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and where recommendations were not implemented, the reasons why.

Major contributors to this report were Brian Reilly, Michael Farrar, Mark Ren, Jason Kearney, Alex Marshall, Jessie Wright and Nancy Varley.

We wish to thank the management and staff of the Office for Technology for the courtesies and cooperation extended to our auditors during the audit.

Very truly yours,

Steven E. Sossei
Audit Director

cc: Deirdre A. Taylor, DOB

George E. Pataki
Governor

STATE OF NEW YORK
OFFICE FOR TECHNOLOGY
STATE CAPITOL, ESP
PO BOX 2062
ALBANY, NY 12220-0062

James T. Dillon
Chief Information Officer

Michael McCormack
Director

October 9, 2003

Mr. Steven Sossei
Audit Director
New York State Office of the State Comptroller
110 State Street
Albany, New York 12236

Re: General Controls at the Consolidated State Data Centers, Report 2002-S-46

Dear Mr. Sossei:

In accordance with Section 170 of the Executive Law, the Office for Technology (OFT) responds to the September 2003 draft of the above-referenced report as follows. OFT agrees with the overall recommendations identified by the Office of the State Comptroller (OSC) during the audit process, and has already undertaken actions consistent with many of these recommendations. OFT will continue to improve policies, procedures, and practices to address issues identified in the audit recommendations.

As stated during the audit process, OFT will meet regularly with your office to discuss and demonstrate actions taken in response to the findings and recommendations of the audit. OFT appreciates the positive steps the Office of the State Comptroller has taken in the course of the audit process in response to security concerns raised by OFT and looks forward to working together to further ensure the security of the State's critical information technology infrastructure.

Sincerely

Michael McCormack

Web Site: www.oft.state.ny.us
E-mail Address: nyoft@oft.state.ny.us

Appendix A