ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

January 13, 2004

Dr. Matthew Goldstein
Chancellor
City University of New York
535 East 80th Street
New York, New York 10021

Re: General Controls at the Data Center and Selected Colleges
Report 2003-S-10

Dear Chancellor Goldstein:

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 manner in which CUNY Computer and Information Services protects its computer systems and the colleges' data, and ensures the continuous processing of critical data after a disaster or other mishap. Our audit covered the period January 1, 2002 to July 28, 2003.

A. Background

The City University of New York (CUNY) is the largest urban university, and the third-largest public university system in the nation. It consists of ten senior colleges, six community colleges, a technical college, a graduate center, a law school, and a school of biomedical education. Governed by a 17-member Board of Trustees, CUNY employs about 5,600 full-time faculty members, and has approximately 208,000 students enrolled in degree programs.

In 1972, CUNY consolidated its data processing operations. Major computer application data processing is now done centrally by Computing and Information Services (CIS). CIS maintains the major administrative, financial, human resources, and library applications. However, each of the colleges also maintains its own data processing installation.

CIS has entered into a standard service level agreement (SLA) with each college. The SLAs stipulate that CIS will provide the colleges with computer time and access; central support of college-managed software; data storage, back-up and recovery services; CIS staff to coordinate CIS-college interaction; problem resolution services, including tracking, escalation procedures, and reporting on usage of resources; and documentation and training. The colleges

are responsible for writing, updating, and ensuring the accuracy of the data they maintain at CIS; and for maintaining and modifying any individual applications that they purchase or design. They also have primary responsibility for authorizing the access rights to their data.

B. Audit Scope, Objectives, and Methodology

Our audit examined the general information technology (IT) controls at the CIS Center and five judgmentally selected CUNY colleges for the period of January 1, 2002, to July 28, 2003. The sampling methodology was designed to obtain a mixture of small and large colleges (based on enrollment), a representation of boroughs, and a variety of college types. The objectives of our performance audit were to determine whether CIS and the colleges had an adequate IT organizational and planning structure; whether CUNY management had established physical, logical, and monitoring controls that would ensure the confidentiality, integrity, and availability of computer systems and data; and whether wireless access points at CIS and the colleges had been approved, configured, and encrypted properly so they could provide reasonable assurance that data and systems are protected from unauthorized access.

To accomplish these objectives, we interviewed CIS and college officials and reviewed available system and network documentation, policies, and procedures. We also reviewed other relevant documents and records, toured the data centers at each location, observed control practices, and tested the effectiveness of selected controls, primarily using the United States General Accounting Office Federal Information Systems Controls Audit Manual as criteria. To assess the security controls, we used tools designed to detect wireless access points; but we did not attempt to infiltrate any system. Since our audit was designed to examine general IT controls, we did not focus on the controls pertaining to individual applications.

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 those CUNY operations included in our audit scope. Further, these standards require that we understand the CUNY's CIS 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 supporting transactions recorded in the accounting and operating records and applying such other auditing procedures, as we consider necessary in the circumstances. An audit also includes assessing the estimates, judgment and decisions made by agency management. We believe our audit provides a reasonable basis for our findings, conclusion 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 efforts to reviewing operations that may be relatively efficient or effective. As a result, our audit reports are prepared on an "exception basis." This report, therefore, highlights those areas needing improvement and does not address in detail activities that may be functioning properly.

C. Results of Audit

Our audit identified findings and made recommendations for corrective actions pertaining to securing computer systems and disaster preparedness at the Data Center and the colleges. These findings and recommendations were presented in detail to CUNY throughout the audit. To further assure security of CUNY's data processing operations, these detailed findings and recommendations are not included in this report. CUNY officials indicate that they share our concerns about improving IT security safeguards and are taking steps to address the concerns within existing funding limitations and fiscal constraints. Their comments have been considered in the preparation of this report and are included as Appendix A.

Recommendation

Implement the recommendations detailed to CUNY during the audit for strengthening computer systems security and disaster readiness.

Within 90 days of the final release of this report, as required by Section 170 of the Executive Law, the Chancellor of CUNY 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 recommendation contained herein and where the recommendation was not implemented, the reasons therefor.

Major contributors to this report were Brian Reilly, Abe Fish, Keith Dickter, Alexander Marshall, Bebe Belkin, Mike Reilly, Russell Budnick, and Matricia Madory.

We wish to thank the management and staff of the City University of New York 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
LouisChiacchere

The City University of New York

OFFICE OF INTERNAL AUDIT AND MANAGEMENT SERVICES
535 East 80th Street, New York, NY 10021
Voice:(212) 997-5820 Fax:(212)997-2301
e-mail: ljcbh@cunyvm.cuny.edu

December 1, 2003

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

Dear Mr. Sossei:

I write in response to your request for comments regarding the less detailed draft audit report on security controls and business continuity plans over computer information systems and electronic data at the University Office of Computing and Information Services (CIS) and selected colleges. The University shares your concerns about improving IT security safeguards and is taking steps to address these concerns within existing fund limitations and fiscal constraints. My comments below address the University's efforts to assure continued progress in this area.

The creation of the IT Steering Committee in November 2001, and the subsequent establishment of the position of Chief Information Officer (CIO) reflected a University-wide collaborative approach to addressing the challenges of a rapidly evolving IT environment in higher education and in anticipating IT's transformative effects on teaching, research and administration currently underway at CUNY colleges. This collaborative effort is intended to facilitate the formulation of the University's IT strategies. Several years ago, a similar committee-type approach was successfully used as a catalyst, facilitator and coordinator in assisting CUNY colleges in achieving full compliance with system requirements for year 2000.

Of particular strategic importance to the University and its constituent colleges is the maintenance of critical IT systems at high availability. Efforts are made everyday to ensure that the IT infrastructure, telecommunications and applications meet current needs and to ensure that future needs will be met as well. Running, maintaining and continually improving the computer and IT systems for faculty, staff and students, and doing it cost efficiently, remains a primary mission of University IT operations.

In recent years, as documented by numerous articles and reports written by news reporters, journalists and consultants, and by incidents reported in the press, the increased reliance on the use of IT systems brings increased security risks. The passage of federal and state laws relating to privacy and information technology security is also affecting how colleges and universities deploy technology services. Federal legislation such as the Family Educational Rights and Privacy Act (FERPA), the

Health Insurance Portability and Accountability Act of 1996 (HIPAA) and the Gramm-Leach-Bliley Act (GLBA) require the protection of confidential personal information. In addition, New York State passed legislation limiting the use of social security numbers in colleges. As a result, maintaining the security of IT systems is now also vital to the mission of University IT operations.

Balancing the University's finite resources between these dual missions is an ongoing challenge generally resulting in progress being made on an incremental rather than on a large-scale basis. Advancing both the development of and security over IT systems is contingent on the availability of state funds and accordingly, budget considerations will always have us in a "catch up" mode. An exception to this funding dilemma was the imposition of a student technology fee last year to make up for state cuts in technology spending. The funds generated by the technology fee were earmarked to support the technology needs of students on each campus. The situation described in your audit report issued last year about the existence of outdated and limited student computer resources at CUNY senior colleges was reversed shortly thereafter with the purchase of new computers and expanded IT support services made possible by the funds generated from the imposition of the student technology fee.

Unfortunately, the University has learned to remain flexible in implementing technology initiatives and security enhancements over IT systems with respect to state funding. Despite these budgetary constraints the University is committed to deploying broad and emerging technologies throughout our campuses and formulating effective computer and network security and access controls in the management of our IT systems. KPMG, the University's External Auditor, in their management letter related to their FY2002 University audit reported a number of responsive steps taken by the University to address previous IT security concerns raised by KPMG (see **Attachment I**). The University takes seriously the importance of securing information, computers, networks, and systems and these reported steps reflect our ongoing commitment to maximizing our finite resources on an incremental basis.

* ***Note 1***

The University will continue to face an uphill battle in maintaining the security over our IT systems without sufficient funding support. As indicated in the articles contained in **Attachment II**, many other IT systems face a similar funding dilemma, as well as a need to continue ongoing efforts to improve IT security safeguards.

Sincerely,

Louis Chiacchere

c: Senior Vice Chancellor Allan Dobrin
Vice Chancellor Ernesto Malave
Brian Cohen, Chief Information Officer
Michael Ribaudo, Chief Technology Officer
Steven Yoman

IA#1523

Note 1: The attachments have not been included because of the sensitive IT-related material contained within the referred documents.