ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

May 10, 2004

Mr. Robert L. King
Chancellor
State University of New York
University Plaza
Albany, New York 12246

Re: Selected General Controls over Computer Network Security at Downstate Medical Center
Report 2003-S-43

Dear Chancellor King:

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 the Downstate Medical Center protects its computer systems and data. In addition, we audited the Downstate Medical Center's controls for providing continuous processing of critical data after a disaster or other mishap. Our audit covered the period January 1, 2003 to October 31, 2003.

A. Background

The State University of New York Health Sciences Center at Brooklyn, also known as the SUNY Downstate Medical Center (Center), was founded in 1860. As an academic medical center, it is comprised of a College of Medicine, College of Health Related Professions, College of Nursing, School of Graduate Studies, and a University Hospital. Although its primary mission is education, the Center also conducts research and provides patient care in its approximately 350 bed hospital.

The Center maintains an Ethernet based computer network with approximately 2,000 personal computer workstations to assist in fulfilling its missions. Its data center contains two IBM mainframe computers; one serves the hospital, while the other is used for scientific and academic purposes. There are also numerous servers. The Center's computer systems run applications that perform such critical functions as billing services and the maintenance of medical information.

B. Audit Scope, Objectives, and Methodology

Our audit, which covered the period of January 1, 2003 to October 31, 2003, examined selected aspects of the general controls over the Center's computerized processes. The objectives of our performance audit were to determine whether the Center's management had established organizational, physical, logical, and monitoring controls to reasonably ensure the confidentiality, integrity, and availability of computer systems and data; and whether wireless access points had been approved, configured, and encrypted properly so that they could provide reasonable assurance that data and systems are protected from unauthorized access.

To accomplish our objectives, we interviewed Center staff, reviewed Center policies and procedures, and performed walk-throughs of Center processes. We used New York State Office for Technology standards and the United States General Accounting Office's Federal Information System Controls Audit Manual as criteria. We also examined the report detailing the results of an independent security review of the Center's computer system that was completed in October 2002. To assess the effectiveness of computer system access controls, we compared samples of authorized users with the Center's employees listed on the New York State payroll system. Finally, to assess the adequacy of wireless network security, we toured the Center's campus using detection software; but we did not try to infiltrate any 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 those operations of the Center that are included in our audit scope. Further, these standards require that we understand the Center's internal control structure and its compliance with those laws, rules and regulations that are relevant to Center operations included in our audit scope. An audit includes examining, on a test basis, the 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, judgments and decisions made by management. We believe that our audit provides a reasonable basis for our findings, conclusions and recommendations.

In addition to being the State Auditor, the Comptroller performs certain other constitutionally and statutorily mandated duties as the chief fiscal officer of New York State, several of which are performed by the Division of State Services. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions and public authorities, some of whom have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under Generally Accepted Government Auditing Standards. In our opinion, these management functions do not affect our ability to conduct independent audits of program performance.

C. Results of Audit

Our audit identified findings and made recommendations for corrective actions on matters pertaining to securing computer systems and disaster preparedness at the Center. These findings and recommendations were presented in detail to Center officials throughout the audit. To further assure security of the Center's data processing operations, these findings and recommendations are not

included in this report. Subsequent follow-up reviews will be made on the detailed findings and recommendations to help insure improvement in the Center's operations.

Recommendation

Implement the recommendations detailed to Center officials during the audit for strengthening computer systems security and disaster preparedness.

Center officials generally agreed with our recommendations and state they are well on their way to implementing the recommendations. Their comments have been considered in preparing this report and are included in Appendix A.

Within 90 days after the final release of this report, as required by Section 170 of the Executive Law, the Chancellor of SUNY 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, if the recommendation was not implemented, the reasons therefor.

Major contributors to this report were Brian Reilly, Abe Fish, Keith Dickter, John Serrone, and Marticia Madory.

We wish to thank the management and staff of the Downstate Medical Center for the courtesies and cooperation extended to our auditors during the audit.

Very truly yours,

Steven E. Sossei
Audit Director

cc: Robert Barnes, DOB

SUNY DOWNSTATE Medical Center

University Hospital of Brooklyn
College of Medicine
School of Graduate Studies
College of Nursing
College of Health Related Professions

Executive Vice President and Chief Operating Officer

March 26, 2004

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

Dear Mr. Sossei:

Thank you for the opportunity to respond to your recent audit of information technology security matters at Downstate Medical Center. In general, we agree with your findings and are well on the way to implementing the recommendations made by your report and further strengthening our controls in this area.

Thank you for your cooperation.

Sincerely,

Ivan M. Lisnitzer
Executive Vice President
and Chief Operating Officer

Cc: John C. LaRosa,M.D.
Fred Hammond
Renee Poncet

State University of New York Downstate Medical Center
450 Clarkson Avenue, Box 106, Brooklyn, NY 11203-2098 • Phone 718 270-1234 Fax 718 270-4092
E-mail ILisnitzer@downstate.edu

Appendix A