ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

September 28, 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 Stony Brook University Hospital and Health Sciences Center
Report 2004-S-2

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 Stony Brook University Hospital and Health Sciences Center protects its computer systems and data. Our audit covered the period January 1, 2004 to May 11, 2004.

A. Background

The Stony Brook University Hospital and Health Sciences Center (Center), a component of the State University of New York, is comprised of a hospital and an academic health sciences center. The Center's 504-bed hospital serves as a regional center for advanced patient care, education, research, and community service. It provides care for more than 25,000 inpatients, 43,600 emergency room patients, 475,000 physician and ambulatory care patients, and 6,000 dental patients each year. The Center's schools educate students to become physicians, dentists, nurses, social workers, and other health professionals.

The Center maintains complex computer and telecommunications networks. The computer systems run applications that perform critical functions such as billing and the maintenance of medical information.

B. Audit Scope, Objectives, and Methodology

Our audit, which covered the period of January 1, 2004 to May 11, 2004, 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 appreciate the State Comptroller's recognition of their ongoing efforts to evaluate and address risk, to improve security over their systems and to protect data against loss and unauthorized use. They generally agree with our recommendations and will continue their efforts to strengthen operations. 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 the State University of New York 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 reason why.

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

We wish to thank the management and staff of the Stony Brook University Hospital and Health Sciences Center for the courtesies and cooperation extended to our auditors during the audit.

Very truly yours,

Steven E. Sossei
Audit Director

cc: Robert Barnes, Division of the Budget

THE STATE UNIVERSITY *of* NEW YORK

September 16, 2004

Elizabeth D. Capaldi
Vice Chancellor and Chief of Staff

State University Plaza
Albany, New York
12246

518 443 5355
fax - 518 443 5360

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

Dear Mr. Sossei:

As permitted under Section 170 of the Executive Law, we are enclosing our comments to your draft audit report #2004-S-2 concerning the Selected General Controls over Computer Network Security.

Sincerely,

Elizabeth D. Capaldi

Enclosure

Appendix A

Stony Brook University Hospital and Health Sciences Center
Response to State Comptroller's Audit 2004-S-2
Selected General Controls Over Computer Network Security
September 8, 2004

RESPONSES TO RECOMMENDATIONS

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

We appreciate the State Comptroller's recognition of our ongoing efforts to evaluate and address risk, to improve security over our systems and to protect data against loss or unauthorized access. We generally agree with the recommendations and are continuing our efforts to implement them to further strengthen controls.