ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

August 16, 2004

Antonia C. Novello, M.D., M.P.H., Dr. P.H.
Commissioner
Department of Health
Corning Tower
Empire State Plaza
Albany, NY 12237

Re: Healthcom Network Security Controls
Report 2002-S-34

Dear Dr. Novello:

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 audited selected aspects of the security controls over the Department of Health's internal computer network, Healthcom. Our audit covered the period June 23, 2003 through December 3, 2003.

A. Background

The mission of the Department of Health (Department) is to promote and protect the health of New Yorkers through prevention, science and assurance of quality health care delivery. In fulfilling this mission and in implementing its various programs, the Department collects and maintains a wide variety of health-related information, such as information about births and deaths, and information about the disciplinary actions taken against medical professionals. The Department maintains this sensitive and confidential data on various computer systems, many of which are operated on or connected to an internal Department computer network called Healthcom.

Healthcom has logical connections to other computer networks, including the NYeNET (a statewide network used by State and local government agencies), the statewide data center maintained by the Office for Technology, outside consultant networks, and individual networks run by two Department units. Healthcom is equipped with a series of firewalls that are intended to protect the network against unauthorized access and create secure areas for sensitive information.

B. Audit Scope, Objective and Methodology

We audited selected aspects of the security controls in place over the Healthcom network. Our audit covered the period June 23, 2003 through December 3, 2003. The objective of our performance audit was to determine whether the Department has instituted appropriate controls for minimizing the risk of unauthorized physical or logical access to the Healthcom network.

To accomplish our objective, we reviewed Department policies and procedures relating to computer networks, equipment, and applications. In addition, we interviewed Department officials responsible for administering network security and operations. We also reviewed relevant laws, rules and regulations, and examined records and reports pertinent to our audit scope. Further, we provided Department officials with a questionnaire addressing the Department's security controls and general and application controls, and verified certain aspects of the responses provided by the officials. We also provided a similar questionnaire to users of the Healthcom network, and verified certain aspects of their responses. Healthcom users include the Department's data center and various Department units, whose servers and desktop computers reside on Healthcom.

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 Department operations that are included within the audit scope. Further, these standards require that we understand the Department's internal control structure and compliance with those laws, rules and regulations that are relevant to the operations that are 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, 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

Detailed results of our audit were provided to Department officials during the conduct of our audit. The details of our findings and recommendations are not included here due to the sensitivity of the information and the potential risk associated with the release of such information. As part of our audit, we identified certain areas in which security policies and controls needed to be improved. We presented this information to Department officials, and they stated that they would make improvements in these areas.

Recommendation

Implement the specific recommendations for strengthening Healthcom's security that were provided to the Department during the audit.

A draft copy of this report was provided to Department officials for their review and comments. Their comments have been considered in preparing this report, and are included as Appendix A. Department officials generally agreed with our comments and recommendations.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the Department of Health 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 therefor.

Major contributors to this report were Brian Reilly, Walter Irving, Nadine Morrell, Mark Ren, Michael Reilly, Kevin Sadvari and Jeff Yanni.

We wish to express our appreciation to the management and staff of the Department for the courtesies and cooperation extended to our auditors during this audit.

Very truly yours,

William P. Challice
Audit Director

cc: Robert Barnes, DOB

STATE OF NEW YORK
DEPARTMENT OF HEALTH

Corning Tower The Governor Nelson A. Rockefeller Empire State Plaza Albany, New York 12237

Antonia C. Novello, M.D., M.P.H., Dr.P.H.
Commissioner

Dennis P. Whalen
Executive Deputy Commissioner

July 14, 2004

William P. Challice
Audit Director
Office of the State Comptroller
110 State Street
Albany, New York 12236

Dear Mr. Challice:

The Department generally agrees with the comments on the Office of the State Comptroller's (OSC) draft audit report (2002-S-34) entitled "Healthcom Network Security Controls." The Department is taking the appropriate actions to address these recommendations.

Thank you for the opportunity to comment.

Sincerely,

Dennis P. Whalen
Executive Deputy Commissioner

Appendix A

cc: Ms. Carmack
Mr. Howe
Mr. Reed
Mr. Scott
Mr. Van Slyke