OFFICE OF THE
STATE COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

January 17, 2007

Mr. John R. Ryan
Chancellor
State University of New York
State University Plaza
Albany, New York 12246

Re: Network Security Controls
Report 2006-S-25

Dear Chancellor Ryan:

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 in place over the State University of New York System Administration's (System Administration) computer network. Our audit covered the period April 11, 2006 through September 22, 2006.

A. Background

System Administration, which oversees SUNY operations, has created a computer network (Network) to help carry out its duties. SUNY employees use the Network to access the Internet and email, and shared files. System Administration's Office of Administrative Systems' Technical Services (Technical Services) maintains the Network. This includes supporting all servers, hardware, and software, setting up desktop computers, providing network connectivity for all business units, and managing network devices. As of June 2006, there were 1,228 authorized user accounts for the Network, and approximately 70 servers supporting the Network.

In 2002, System Administration initiated a five-year effort to transition system-wide administrative computer systems to more modern technology in support of campus business requirements. The project's objectives included standardization of business processes, data terminology, and technology; streamlining of business functions; transitioning applications to a more distributed environment by moving mainframe applications out to Network servers; greater reliance on electronic versus paper processes; greater functionality for user departments; improved reporting and access to information; enhanced security of systems and information; and less expensive and easier maintenance of systems. In 2002, System Administration "webified" its interface with campuses to systems in Albany. This included using special software that allowed campus users to securely access SUNY applications maintained by System Administration. Using this software, SUNY campus employees could log into SUNY applications over the Internet from an authorized IP address with their unique user IDs and passwords through an encrypted connection.

System Administration must comply with the Office of Cyber Security and Critical Infrastructure Coordination's Cyber Security Policy that defines a set of minimum information security requirements that all State entities must meet related to securing systems and data. In addition, the Security Policy requires that each State entity establish a framework to initiate and control the implementation of information security within the entity. The Security Policy further requires that each agency appoint an Information Security Officer. To determine the appropriate levels of protection for information, each agency must also establish a process based on best practices, State directives, and legal and regulatory requirements.

B. Audit Scope, Objective and Methodology

We audited selected aspects of the security controls in place over the Network. Our audit covered the period April 11, 2006 through September 22, 2006. The objective of our performance audit was to determine whether System Administration has established adequate security controls to minimize the risks of unauthorized access to its data resources. Our audit provided a snapshot of the Network's security controls at a particular point in time.

To accomplish our objective, we reviewed System Administration policies and procedures relating to computer networks, equipment and applications. We interviewed System Administration technical and facility staff responsible for administering Network security and operations. We also examined Department records and reports pertinent to our audit scope. In addition, in coordination with System Administration officials, we performed external and internal vulnerability assessments of the Network. In performing these assessments, we used various tools and techniques to proactively identify Network vulnerabilities and to determine how these vulnerabilities could be exploited.

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 System Administration operations that are included within the audit scope. Further, these standards require that we understand the System Administration'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 System Administration 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 the controls needed to be improved. We presented this information to System Administration officials, and they stated that they have begun to make improvements in these areas. Their comments are included as Appendix A. Subsequent follow-up reviews will be made on the detailed findings and recommendations to help ensure improvement in System Administration's operations.

Recommendation

Implement the specific recommendations for strengthening System Administration's Network security that were provided to System Administration officials during the audit.

Within 90 days of 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 recommendations contained herein, and where recommendations were not implemented, the reasons therefor.

Major contributors to this report include Brian Reilly, Nadine Morrell, Mark Ren, James Edge, Jennifer Van Tassel, and Sue Gold.

We wish to thank the management and staff of the State University of New York System Administration for the courtesy and cooperation extended to our auditors during this audit.

Very truly yours,

Steven E. Sossei
Audit Director

cc: Lisa Ng, Division of Budget

THE STATE UNIVERSITY *of* NEW YORK

December 13, 2006

Dr. Kimberly R. Cline
Vice Chancellor and
Chief Financial Officer

State University Plaza
Albany, New York
12246

518 443 5105
fax - 518 443 5321

kim.cline@suny.edu
www.suny.edu

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

Dear Mr. Sossei:

In accordance with Section 170 of the Executive Law, we are providing our comments to the draft audit report on SUNY System Administration Network Security Controls (2006-S-25). We are pleased that the State Comptroller found that the SUNY System Administration has taken many noteworthy steps to create a secure networking environment and respectfully request that you include a statement acknowledging that fact in the report. System Administration recognizes the importance of information security and strives to establish and maintain a secure information technology environment. We will use the report to further improve our controls. Our comment to the recommendation follows:

Recommendation – Implement the specific recommendations for strengthening System Administration's network security that were provided to System Administration officials during the audit.

Response – System Administration substantially agrees with the findings and recommendations that were provided during the audit, and has taken action to address most of the recommendations.

Thank you for the opportunity to respond to the audit report. If you have any questions, please contact Michael Abbott at 518-443-5533 or michael.abbott@suny.edu.

Sincerely,

Kimberly R Cline

Kimberly Cline

Copy: Chancellor Ryan

Appendix A