ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

June 29, 2005

Mr. Daniel D. Hogan
Commissioner
New York State Office of General Services
Governor Nelson A. Rockefeller Empire State Plaza
Albany, NY 12242

Re: Office of General Services
Network Security Controls
Report 2004-S-65

Dear Mr. Hogan:

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 Office of General Services' computer network. Our audit covered the period September 16, 2004 through December 24, 2004.

A. Background

The Office of General Services (OGS) provides various support services to State agencies, public authorities, municipalities and other political subdivisions of New York State. For example, OGS provides design and construction services, centralized contracting and procurement services, and surplus property services. OGS also administers New York State's fixed-asset accounting system.

In carrying out its responsibilities, OGS makes considerable use of its Internet web site and other interconnected electronic data processing systems. For example, OGS uses its web site to make information available to its customers and to provide customers with access to certain services, such as its vendor registration system. OGS also maintains and updates the statewide fixed-asset accounting system, and provides several agencies with administrative support systems such as payroll, human resources, purchasing and accounts payable. In addition, OGS provides Internet access and email capability to its employees.

OGS uses a computer network (Network) to facilitate its electronic data processing activities. The Network is maintained and overseen by two units in OGS: the Information Resource Management Unit and the Information Security Office. The Information Resource Management Unit is responsible for maintaining the computing resources, while the Information Security Office is responsible for protecting the resources and electronic information. The Information Security

Office is headed by an Information Security Officer. Both units are overseen by a Chief Information Officer, who has overall responsibility for the security and protection of OGS information assets.

New York State agencies are expected to comply with the requirements of the State's Cyber Security Policy, which was developed by the Office of Cyber Security and Critical Infrastructure Coordination. Each agency is expected to meet the specific security requirements described in the Policy, and to establish a framework for initiating and controlling the implementation of information security within the agency.

B. Audit Scope, Objective and Methodology

We audited selected aspects of the security controls in place over the Network. Our audit covered the period September 16, 2004 through December 24, 2004. The objective of our performance audit was to determine whether OGS instituted controls and security measures that minimized the risk of unauthorized access to Network data and computer resources. Our audit provided a snapshot of the Network's security controls at a particular point in time.

To accomplish our objective, we reviewed OGS policies and procedures relating to computer networks, equipment and applications. We interviewed OGS officials responsible for administering Network security and operations, and provided a questionnaire addressing security controls to the officials. We also examined OGS records and reports pertinent to our audit scope. In addition, we performed tests of remote access into the Network and, in coordination with OGS 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 OGS operations that are included within the audit scope. Further, these standards require that we understand OGS' 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 OGS 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. OGS officials generally agreed with our recommendations and are taking action to address them. They considered this audit to be a useful and constructive service. Their comments are included as Appendix A.

Recommendation

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

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the Office of General Services shall report to the Governor, the State Comptroller, and the leaders of the Legislature and fiscal committees, advising what steps were taken to implement our audit recommendation, and if the recommendation was not implemented, the reasons why.

Major contributors to this report were Brian Reilly, Walter Irving, Nadine Morrell, Michael Reilly, Kevin Sadvari, and James Edge.

We wish to thank the management and staff of the Office of General Services for the courtesy and cooperation extended to our auditors during this audit.

Very truly yours,

Frank J. Houston
Audit Director

cc: Robert Barnes, Division of Budget

DANIEL D. HOGAN
COMMISSIONER

STATE OF NEW YORK
EXECUTIVE DEPARTMENT
OFFICE OF GENERAL SERVICES
MAYOR ERASTUS CORNING 2ND TOWER
THE GOVERNOR NELSON A. ROCKEFELLER EMPIRE STATE PLAZA
ALBANY, NEW YORK 12242

ROBERT J. FLEURY
FIRST DEPUTY COMMISSIONER

June 15, 2005

Mr. Frank J. Houston
Director, State Audit Bureau
Office of the State Comptroller
Division of State Services
110 State Street – 11th Floor
Albany, NY 12236

Dear Mr. Houston:

The Office of General Services (OGS) acknowledges receipt of the Office of the State Comptroller's (OSC) draft audit report (2004-S-65) entitled "Network Security Controls". We generally agree with the recommendations provided in the report and are taking the appropriate actions to address them.

We regard this audit as a useful and constructive service provided by OSC and are pleased that the results validate the measures we have already taken or have in progress to foster a robust information security and assurance program at OGS.

We appreciate the work and the courtesy provided by your team.

Sincerely,

Robert J. Fleury

recycled paper

Appendix A