THOMAS P. DiNAPOLI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

June 9, 2011

Mr. Greg Olsen
Acting Director
New York State Office for the Aging
2 Empire State Plaza
Albany, New York 12223-1251

Re: Audit Report 2010-S-23

Dear Mr. Olsen:

According 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 New York State Office for the Aging's computer network (Network). Our audit covered the period May 5, 2010 through December 15, 2010.

A. Background

The New York State Office for the Aging (Office) administers various Federal and State-funded programs which serve the elderly. The majority of programs and services are administered through the 59 local offices for the aging.

The Office has a Chief Information Officer who leads two units: the Application, Database, and Website Unit and the Computer Infrastructure Unit. The Office has a part-time Information Security Officer that also works in the Computer Infrastructure Unit performing duties to manage and administer the Office network. This unit's supervisor oversees the work of the Information Security Officer and together they are responsible for security, technical, and program related duties for the Office.

The Office must comply with the Office of Cyber Security's Cyber Security Policy (Security Policy), which defines a minimum set of security standards state entities must meet. One of these standards is managing the risk of security exposure or compromise within the entity's system.

B. Audit Scope, Objective and Methodology

We did our performance audit according to generally accepted government auditing standards. We audited selected aspects of the security controls in place over the Network for the period May 5, 2010 through December 15, 2010. The objective of our audit was to determine whether network security at

the Office is sufficient to minimize the various risks associated with unauthorized access to systems and data.

We reviewed Office policies and procedures we deemed important to the control and maintenance of Network security. We interviewed agency technical staff responsible for Network security and operations. We also examined records and reports pertinent to our audit scope. We tested security controls by determining whether there is a risk someone could gain unauthorized access to the Network. These tests were performed on some, but not all, devices on the external and internal Network. In performing these assessments, we used various tools and techniques to identify Network weaknesses and to determine how these weaknesses could be exploited. Our testing included scanning for weaknesses on; specific servers, workstations, and web applications, and more in-depth testing of select servers and applications where we deemed it appropriate.

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. 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 functions do not affect our ability to conduct independent audits of program performance.

C. Results of Audit

Numerous critical weaknesses are on the Office's Network which need to be corrected. The Office's data and resources are at risk of unauthorized access to and disclosure of sensitive data and denial of service. Office management has not taken fundamental steps to secure their Network such as completing a risk assessment. Operations are emphasized over security at the Office and they have neglected serious security threats to Office operations. Staff responsible for protecting the Office's network and data are not provided with sufficient training or guidance to carry out their job duties. Further, there is a lack of support from upper management for the security of the Office's network.

Detailed results of our audit were provided to Office officials during 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. Office officials stated they have begun to make improvements.

Recommendation

Implement the specific recommendations for strengthening the Office's network security that were provided to Office officials during the audit.

We provided a draft copy of this report to Office officials for their review and comment. Their comments were considered in preparing this report, and are included as Appendix A. Office officials agreed with our audit recommendations and have already taken positive steps to address our findings.

Within 90 days after final release of this report, as required by Section 170 of the Executive Law, the Acting Director of Office for the Aging 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 why.

Major contributors to this report include Nadine Morrell, Claudia Christodoulou, Jennifer Van Tassel, Corey Harrell, and Randy Rose.

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

Yours truly,

Brian Reilly
Audit Manager

cc: Tom Lukacs, Division of the Budget

Andrew M. Cuomo
Governor

Greg Olsen
Acting Director

New York State OFFICE for the AGING

Two Empire State Plaza
Albany, New York
12223-1251

www.aging.ny.gov

May 3, 2011

Mr. Brian Reilly, Audit Manager
Office of the State Comptroller
Division of State and Local Government Accountability
110 State Street, 11th floor
Albany, NY 12236

Dear Mr. Reilly:

The New York State Office for the Aging (NYSOFA) has read the OSC Network Security Control Report # 2010-S-23 and agrees with the findings.

The findings contained in the report are consistent with the comments discussed with the auditors at the exit conference. Overall, the audit was a fair assessment of NYSOFA's Information Technology security practices that identifies certain areas for improvement and NYSOFA has already taken positive steps to address the more significant concerns. The remaining issues identified in the audit are being addressed by NYSOFA's Management, Information Security Officer, Chief Information Officer and IT staff and will be completed in the coming months.

NYSOFA appreciates OSC's assistance to help us ensure the confidentiality, integrity and protection of our data and information technology systems.

Sincerely,

Greg Olsen

cc: Tom Lukacs, Division of the Budget
Nicole Treacy, NYSOFA ISO

Appendix A