ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

August 23, 2005

Mr. Gino Menchini
Commissioner
New York City Department of Information
Technology and Telecommunications
75 Park Place
New York, New York 10007

Ms. Rose Gill Hearn
Commissioner
New York City Department of Investigation
80 Maiden Lane
New York, New York 10038

Re: Selected General Controls
Over Data Center Security
Report 2004-N-1

Dear Mr. Menchini and Ms. Gill Hearn:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1, of the State Constitution; and Article III of the General Municipal Law, we have audited the manner in which the New York City Department of Information Technology and Telecommunications and the New York City Department of Investigation protects New York City's computer systems and data. Our audit covered the period July 1, 2003 through December 31, 2004.

A. Background

The Department of Information Technology and Telecommunications (DoITT) deploys, operates, and maintains the technology infrastructure to support critical functions for City agencies and other government entities. DoITT also provides services that involve mainframe processing and communications and internet applications. For fiscal year 2003, DoITT reported $8.4 million in personal service (PS) and $23.5 million in other-than-personal service (OTPS) expenses for its data centers; the totals rose in fiscal 2004 to $9.4 million and $27.1 million, respectively.

The Department of Investigation (DOI) is responsible for the design and implementation of a system of information security policies for the City and its constituent agencies. To accomplish this task, DOI created the Citywide Information Security, Architecture, Formulation and Enforcement Unit (CISAFE). Among other responsibilities, this unit creates, develops, and enforces consistent and cost-effective information security policies, directives, and standards intended to ensure the

confidentiality, integrity, and controlled accessibility of all electronic information processed through the City's computer systems. CISAFE reported PS expenditures of $708,870, for nine employees, in fiscal 2003; the PS expenditures for fiscal 2004 totaled $496,445 for seven employees.

B. Audit Scope, Objectives, and Methodology

Our audit, which covered the period of July 1, 2003 through December 31, 2004, examined selected aspects of the general security controls and oversight at City data centers. The objectives of our performance audit were to determine whether physical access to DoITT's data centers is limited to individuals who have a job-related need for such access, whether inventory controls over DoITT's backup data storage are sufficient to reasonably ensure the continuous processing of critical data after a disaster or other mishap, and to determine whether DOI and DoITT guidance, oversight, and enforcement of the City's policies on agency data center security are adequate.

To accomplish our objectives, we interviewed DoITT and DOI staff, reviewed DoITT and DOI policies and procedures, and performed walk-throughs of data centers at DoITT and five selected agencies. As criteria, we used DOI policies, standards, and guidelines, as well as the New York City Comptroller's Directives 1 and 18. To assess the effectiveness of controls over data center access, we compared samples of authorized user names with the names of DoITT employees listed on the New York City payroll system. To assess the adequacy of controls over remotely-stored backup cartridges, we toured the City's remote storage facility, attempted to physically locate a sample of cartridges, and compared DoITT and storage facility inventory records. We also submitted questionnaires to, and conducted follow-up interviews with officials of, the five agencies to review the controls in place at their data centers.

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 DoITT and DOI that are included in our audit scope. These standards also require that we understand the internal control structure of DoITT and DOI and their compliance with those laws, rules, and regulations that are relevant to the DoITT and DOI operations included in our audit scope. An audit includes examining, on a test basis, the evidence supporting transactions that were recorded in the accounting and operating records, and applying other auditing procedures that we consider necessary under 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 City computer system and disaster preparedness at the City's data centers, and DOI and DoITT's oversight of the City's policies on agency data center security. These findings and recommendations were presented in detail to DoITT and DOI officials throughout the audit. To further assure security of the City's data processing operations, these findings and recommendations are not included in this report. Subsequent follow-up audits will be made on the detailed findings and recommendations. DoITT and DOI officials' comments have been considered in preparing this final report. DoITT and DOI officials agreed with our recommendations and indicated they will take action to implement them. The response of DOI and DoITT officials are included as Appendices A and B respectively.

Recommendation

DoITT and DOI should implement the recommendations detailed during the audit for strengthening City computer systems security, improving disaster preparedness, and enhancing oversight and monitoring activities.

Within 90 days after final release of this report, we request that the Commissioners of the New York City Department of Information Technology and Telecommunications and the New York City Department of Investigation report to the State Comptroller 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, Abe Fish, Keith Dickter, Alina Mattie, Michael D'Amico, and Matricia Madory.

We wish to thank the management and staffs of the Department of Information Technology and Telecommunications and the Department of Investigation for the courtesies extended to our auditors during this audit.

Very truly yours,

Carmen Maldonado
Audit Director

cc: S. Kupferman, Mayor's Office of Operations

The City of New York
Department of Investigation

ROSE GILL HEARN
COMMISSIONER

80 MAIDEN LANE
NEW YORK, NY 10038
212-825-5900

June 9, 2005

Ms. Carmen Maldonado
Director
Office of the State Comptroller
Division State Services
123 William Street – 21st Floor
New York, New York 10038

Dear Ms. Maldonado:

In response to your draft audit report (2004-N-1), I would like to thank you for your efforts in assessing the manner in which the Department of Investigation ("DOI") protects New York City's systems and data. DOI's specific responses to your draft audit report are included herewith.

*

DOI certainly agrees in principle that any contingency planning process, including our own, can be improved and requires continual attention and testing to ensure its viability; and DOI agrees that any lapse in procedure or protocol must be addressed and corrected, regardless of its severity or implied threat level.

Sincerely,

Rose Gill Hearn
Commissioner

* DOI's specific responses are not included due to their security sensitivity.

Appendix A

The City of New York

DEPARTMENT OF INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

75 Park Place, 9th Floor
New York, NY 10007
(212) 788-6633
Fax: (212) 788-8130
E-Mail: gmenchini@doitt.nyc.gov

GINO P. MENCHINI
Commissioner
Chief Information Officer

June 6, 2005

Carmen Maldonado
Director
Office of the State Comptroller
Division State Services
123 William Street – 21st Floor
New York, NY 10038

Dear Ms. Maldonado

In response to your draft audit report (2004-N-1), I would like to thank you for your efforts in assessing the manner in which the Department of Information Technology and Telecommunications (DoITT) protects New York City's computer systems and data.

DoITT certainly agrees with the importance of a sound contingency planning process, and will continue to seek out and institute measures, which further enhance the Department's business continuity strategy.

Sincerely,

Gino P. Menchini

Appendix B