ALAN G. HEVESI
COMPTROLLER

110 STATE STREET
ALBANY, NEW YORK 12236

STATE OF NEW YORK
OFFICE OF THE STATE COMPTROLLER

February 12, 2006

Mr. Robert Doar
Commissioner
New York State Office of Temporary and Disability Assistance
40 North Pearl Street
Albany, NY 12243

Ms. Meg Levine
Acting Director
New York State Office for Technology
State Capitol
Albany, NY 12243

Ms. Verna Eggleston
Commissioner/Administrator
New York City Human Resources Administration
180 Water Street
New York, NY 10038

Re: 2005-F-22

Dear Mr. Doar, Ms. Levine and Ms. Eggleston:

Pursuant to the State Comptroller's authority as set forth in Article V, Section 1 of the State Constitution, Article III of the General Municipal Law and Article II, Section 8 of the State Finance Law, we have reviewed the actions taken by officials of the Office of Temporary and Disability Assistance (OTDA), the New York State Office for Technology (OFT), and the New York City Human Resources Administration (HRA) to implement the recommendations contained in our audit report, *Welfare Management System: New York City General and Application Controls* (Report 2002-N-1).

Background, Scope and Objective

OTDA, in accordance with Chapter 55, Section 21, of New York State Social Services Law (Law), is required to design, implement, and maintain a welfare management system. This system must be capable of receiving, maintaining, and processing information relating to persons who have applied for, or have been determined eligible for, benefits under any program for which OTDA has supervisory responsibility. OTDA must consider this information confidential.

To help improve the administration and control of public assistance programs and related services provided by the State's 58 local social services districts (districts), both OTDA and OFT have responsibilities to support and maintain the Welfare Management System (WMS). Established in 1997, OFT is charged with the coordination of New York State's vast technology resources. It manages a consolidated New York State Data Center that supports WMS' data processing requirements, as well as those of 24 other agencies. However, the responsibility for managing local user access accounts and permissions is in the hands of local district administrators. OTDA is primarily responsible for the applications and administration of WMS; OFT is primarily responsible for the system's hardware-operating environment, including file management, disaster recovery, system backup, and computer center maintenance and support.

WMS consists of two application subsystems: "Upstate," which is used to maintain the records of clients living in counties outside New York City, and "New York City," which contains the data of clients who are residents of New York City. In New York City, HRA administers WMS.

Our initial audit report, which was issued on September 26, 2003, determined whether OTDA, OFT, and HRA had instituted general and application controls that provide reasonable assurance of the validity and reliability of data maintained in WMS and minimize the risk of unauthorized physical or logical access. We could not express an opinion on the accuracy and reliability of public assistance eligibility data and we found departures in the general and application controls, as developed and implemented within OTDA, OFT, and HRA, from recommended practices. Specifically, we found that physical and personnel security over WMS had not been adequately addressed and comprehensive emergency procedures had not been adequately established. The objective of our follow-up, which was conducted in accordance with generally accepted government auditing standards, was to assess the extent of implementation, as of November 30, 2005, of the 37 recommendations included in our initial report.

Because some of the weaknesses we identified could be considered sensitive, we did not include the details relating to those weaknesses in our initial report. Instead, we conveyed those findings to officials during the audit. We followed this same process for our follow-up audit.

Summary Conclusions and Status of Audit Recommendations

We found that OTDA, OFT and HRA have made progress in correcting the problems we identified. However, additional improvements are needed. Of the 37 audit recommendations, 16 recommendations have been implemented, 8 recommendations have been partially implemented, and 13 recommendations have not been implemented.

Follow-up Observations

Recommendation 1

HRA: *Develop written supervisory case review procedures that explain a supervisor's role and responsibilities. Include matching selected data with appropriate source documentation.*

Status - ImplementedAgency Action - HRA officials developed a written supervisory case review policy that explains a supervisor's role and responsibilities. We reviewed this policy and found it requires supervisors to confirm WMS data agrees with supporting documentation.

Recommendation 2

HRA: Require job centers to make sure that scanned source documents are legible.

Status - Implemented

Agency Action - We reviewed HRA's written policy and found it requires supervisory staff to confirm that all scanned documents are legible.

Recommendation 3

OTDA and HRA: *Enforce the requirement that job centers obtain supporting documentation and verify that they have corrected the errors and variances we noted during our audit.*

Status - Partially Implemented

Agency Action - We reviewed HRA's written policy bulletin that informs supervisors of the requirement to obtain sufficient documentation. OTDA officials also reported that the errors we noted had been corrected. However, when we reviewed 23 of the 39 errors noted during the audit, we found that only 4 had not been corrected.

Recommendation 4

OTDA: *Verify that HRA implements the data integrity recommendations in this report.*

Status - Not Implemented

Agency Action - OTDA officials reported that they will continue to monitor the accuracy of system data in various ways. However, OTDA officials believe that taking a more prescriptive role in the supervision of district operations would exceed their legislative authority.

Recommendation 5

OTDA and OFT: *Implement the password security recommendations made during the course of our audit.*

Status - Not Implemented

Agency Action - OTDA and OFT officials conveyed that improving TTSS (Transaction Terminal Security System) user identification (ID) and password controls would be difficult due to limitations in the current mainframe environment. They believe that the time, effort and costof attempting to do so would not be worthwhile or appropriate given the State's direction in modernizing/redesigning WMS.

Recommendation 6

HRA: *Use the Terminal Security Violations Reports to monitor compliance with security policies and to investigate potential system violations. Verify that the reports HRA receives are complete (e.g., contain all location codes).*

Status - Partially Implemented

Agency Action - We found that HRA worked with OFT to obtain in September 2005, Terminal Security Violations Reports that specifically identified the locations where potential violations occurred. These reports allowed HRA to readily distribute them to locations. HRA officials stated they will use the reports to monitor compliance with security policies and to investigate potential security violations. HRA staff conveyed they receive a report for each location code.

Recommendation 7

OFT: *Verify that the Terminal Security Violations Reports OFT provides to HRA are complete and accurate.*

Status - Implemented

Agency Action - OFT officials reported that they reviewed the program used to create the Terminal Security Violations reports and found it produces complete and accurate reports. We confirmed that location codes missing during the initial audit are now included in the reports.

Recommendation 8

OFT: *Meet with HRA officials and explain the important uses of the Report.*

Status - Implemented

Agency Action - In October 2005, OFT and HRA officials began modifying the Report to meet HRA's needs. We found OTDA and OFT developed a cover letter that OFT distributes with the Terminal Security Violations Reports. The cover letter details the violations and provides guidance on addressing them.

Recommendation 9

OTDA: *Verify that HRA and OFT implement the recommendations in this report regarding the use of the Terminal Security Violations Reports.*

Status - Partially Implemented

Agency Action - OTDA officials stated that taking a more prescriptive role in the supervision of district operations would exceed their legislative authority, therefore, they have not verified that HRA and OFT implemented the recommendations. However, OTDA did work in conjunction with OFT to develop a cover letter that OFT distributes with the Terminal

Security Violations Reports. The cover letter details the violations and provides guidance on addressing them.

Recommendation 10

HRA: Update the TTSS (Transaction Terminal Security System) Handbook and distribute copies of the revised version to all location coordinators.

Status - Partially Implemented

Agency Action - While HRA has updated portions of the TTSS Coordinator Handbook we noted that the revised Handbook does not provide guidance on segregation of user rights which we believe users could benefit from.

Recommendation 11

HRA: *Establish an accountability system for approved authorization forms that allows them to be retrieved.*

Status - Implemented

Agency Action - Our audit found that the WMS Request Intake and Tracking Procedure establishes an accountability system that allows approved authorization forms to be retrieved.

Recommendation 12

HRA: *Require location coordinators to verify the appropriateness of user/terminal rights by comparing assigned functions with authorizations before distributing user IDs/passwords.*

Status - Implemented

Agency Action - HRA, in an E-mail dated October 11, 2005, reminded TTSS Coordinators to compare assigned functions with authorizations before the user IDs and passwords are distributed.

Recommendation 13

HRA: *Review the Terminal Operator Authorized Functions reports at least annually to determine whether employees and terminals have been assigned proper access to WMS, and update access rights where appropriate.*

Status - Not Implemented

Agency Action - HRA officials report that they are working with OTDA to obtain a report that they can use to perform this review. The current report lacks sufficient detail for the report to be used effectively.

Recommendation 14

HRA: *Require directors to complete the payroll exception report properly and have ODSM [Office of Data Security Management] perform the payroll match on a quarterly basis.*

Status - Implemented

Agency Action - We reviewed a memorandum that HRA distributes with the payroll exception report requiring directors to complete the payroll exception report and instructing directors on how to do this.

Recommendation 15

HRA: *Verify that location coordinators are following policy that requires them to provide ODSM with timely notification of all personnel changes.*

Status - Not Implemented

Agency Action - HRA officials state they use a semi-annual payroll match to verify that location coordinators make timely notifications of all personnel changes to ODSM. The match is used to identify users that no longer are employed by HRA; and to confirm vendors who have WMS access continue to need such access. However, the match will not identify all personnel changes that affect user rights. Further, HRA officials did not provide documentation to support the semi-annual payroll match.

Recommendation 16

OTDA: *Verify that HRA implements the recommendations in this report regarding the updating of user access.*

Status - Not Implemented

Agency Action - OTDA officials did not verify that HRA implemented these recommendations. OTDA officials stated that taking a more prescriptive role in the supervision of district operations would exceed their legislative authority.

Recommendation 17

HRA: *Update the job functionality matrices and incorporate them into the appropriate section of the TTSS Coordinator Handbook.*

Status - Partially Implemented

Agency Action - We found that while HRA incorporated its functionality matrix into the TTSS Coordinator Handbook, HRA did not incorporate the profile matrix into the handbook. In addition, HRA reported they updated the profile matrix to include Job Opportunity Specialist, but did not report that they added the five additional job titles that were missing from the matrix when our initial audit was conducted.

Recommendation 18

HRA: Include in the updated TTSS Coordinator Handbook how location coordinators should use the job functionality matrices and indicate which TTSS functions should be segregated.

Status - Partially Implemented

Agency Action - We found HRA updated the TTSS Coordinator Handbook. While it explains how the matrices should be used, it does not indicate which TTSS functions should be segregated.

Recommendation 19

OTDA: *Verify that HRA implements the recommendations in this report that deal with the assignment of application functions to users.*

Status - Not Implemented

Agency Action - See Agency Action for Recommendation 16.

Recommendation 20

HRA: *Distribute a copy of the Information Protection and You handbook and other security-related information to users when they receive their user IDs and passwords.*

Status - Partially Implemented

Agency Action - HRA officials incorporated the Information Protection and You handbook into the revised TTSS Coordinator Handbook which was finalized and distributed to location coordinators on December 23, 2005. While officials stated location coordinators are instructed to distribute the handbook to users when they receive their user IDs and passwords, we cannot confirm this practice is in effect.

Recommendation 21

HRA: Verify that location coordinators are promoting information security awareness among staff.

Status - Implemented

Agency Action - We found that HRA has taken steps to confirm that location coordinators are promoting information security awareness. Such steps include contacting staff to confirm coordinators share this information.

Recommendation 22

HRA: Incorporate security awareness training and guidance into the eight-week training course new employees are required to complete. Such training could include maintaining the integrity of user IDs and passwords, maintaining security over terminal sessions, and handling confidential information and transactions.

Status - Implemented

Agency Action - HRA updated the eight-week training course for new employees and it now includes security awareness.

Recommendation 23

OTDA and OFT: *Revise the TTSS Manual to incorporate control objectives, such as guidance on implementing controls and the handling of available monitoring reports and their intended use.*

Status - Not Implemented

Agency Action - OTDA and OFT officials stated that they assessed the need to update the TTSS manual and found that no additional updates were necessary at this time. However, they were not able to provide documentation to support their review.

Recommendation 24

OTDA: Verify that HRA and OFT implement the communication and training recommendations contained in this report.

Status - Not Implemented

Agency Action - While OTDA shares security awareness information with local districts it does not verify that the communication and training recommendations contained in this report were implemented.

Recommendations 25, 26, and 27

OFT: *Finalize the Data Center Disaster Recovery Plan and ensure that it provides for system criticality and restoration priorities, individual roles and responsibilities and time-related tasks, procedures for testing the adequacy of the Plan, and the process OFT is to follow to make the DR [Disaster Recovery] Site operational after a disaster.*

OTDA: Provide OFT with a disaster application-processing schedule and printing strategies.

OTDA: Develop recovery procedures for WMS and deliver them to OFT.

Status – Implemented

Agency Action - We found that OTDA and OFT have finalized a comprehensive Disaster Recovery Plan that includes an application processing schedule, printing strategy and WMS recovery procedures. In addition, we noted that a Disaster Recovery Site has been established and equipped with proper environmental controls.

Recommendation 28

OTDA: *Verify that OFT implements the Disaster Recover Plan recommendation made in this report.*

Status - Partially Implemented

Agency Action - While OTDA and OFT have developed a comprehensive Disaster Recovery Plan, this Plan has not been tested to confirm its viability. Therefore, OTDA has no assurance that the Disaster Recovery Site can meet the agency's emergency needs.

Recommendation 29

HRA: *Develop a written access policy that identifies the individuals authorized to grant access to the New York City data center, as well as those who are allowed to receive access.*

Status - Implemented

Agency Action - We found HRA has developed a written access policy identifying individuals authorized to grant access to the New York City data center, and those allowed to receive access.

Recommendation 30

HRA: List in writing the procedures to be followed when issuing or obtaining an identification badge that grants regular access to the New York City data center.

Status - Implemented

Agency Action - Our audit found that HRA's written procedure details the process for issuing and obtaining an identification badge that grants regular access to the New York City data center.

Recommendation 31

HRA: Require, at least annually, the review of the data centers' access lists to verify that access privileges granted to individuals are current and appropriate.

Status – Implemented

Agency Action - Our audit found that HRA now requires an annual review of the data centers' access lists to verify that access privileges granted to individuals are current appropriate.

Recommendation 32

HRA: *Develop and convey procedures for addressing physical security of WMS equipment at the job centers and verify that they are taking appropriate measures to safeguard their equipment.*

Status - Not Implemented

Agency Action - HRA officials disagree with the need for this recommendation and conveyed that they have extensive security procedures that have been in effect for some time. However, we found during our initial audit, that some WMS equipment was not properly safeguarded and we attributed these security weaknesses to the lack of procedures addressing physical security of WMS equipment.

Recommendation 33

OTDA: *Verify that HRA implements the recommendations in this report regarding the development and implementation of a written access policies for the New York City data center and a physical security policy for WMS equipment at the job centers.*

Status - Not Implemented

Agency Action - See Agency Action for Recommendation 16.

Recommendation 34

OTDA: *Update the SDLC [System Development Life Cycle] to define management's current objectives and staff responsibilities, and provide appropriate staff with a copy. The SDLC should include the development of detailed test plans, definitions of responsibilities for each person involved in testing and approving changes, and the development of related system documentation.*

Status - Not Implemented

Agency Action - During our audit, OTDA officials told us they had not implemented this recommendation. However, officials stated on December 22, 2005, that they purchased a new application that will gradually replace the components of the current SDLC.

Recommendation 35

OTDA: *Correct the system display to reflect the appropriate "other" grant when a case has an Office of Child Support Enforcement sanction.*

Status - Implemented

Agency Action - Our audit found that OTDA corrected the system display to reflect reductions due to Office of Child Support Enforcement sanctions.

Recommendation 36

OTDA: *Update the WMS System Reference Manual as the system is modified.*

Status - Not Implemented

Agency Action - OTDA officials reported that they currently use several other documentation and notification vehicles to document software changes other than the WMS System Reference Manual.

Recommendation 37

OTDA: *Verify that when the WLM process is followed program change responsibilities are properly segregated to prevent a single individual from controlling more than one critical stage of the change process.*

Status - Not implemented

Agency Action - During our audit, OTDA officials told us that they had not implemented this recommendation. However, on December 22, 2005, OTDA officials stated that they purchased a new SDLC tool that will replace the WLM process.

Major contributors to this report were Richard Sturm, Donald Geary, Randy Partridge and Theresa Lawrence.

We would appreciate your response to this report within 30 days, indicating any actions planned or taken to address any unresolved matters discussed in this report. We also thank the management and staff of OTDA, OFT and HRA for the courtesies and cooperation extended to our auditors during this process.

Very truly yours,

William P. Challice
Audit Director

cc: Robert Barnes, Division of the Budget
Christine Unson, OTDA Audit Liaison