CITY OF NEW YORK
OFFICE OF THE COMPTROLLER

John C. Liu
Comptroller

BUREAU OF FINANCIAL AUDIT

H. Tina Kim
Deputy Comptroller for Audit

Audit Report on
Department for the Aging Controls over Personally Identifiable Information

7A10-092

June 30, 2010

http://comptroller.nyc.gov

THE CITY OF NEW YORK
OFFICE OF THE COMPTROLLER
1 CENTRE STREET
NEW YORK, N.Y. 10007-2341

John C. Liu
COMPTROLLER

June 30, 2010

To the Residents of the City of New York

My office has audited the Department for the Aging (DFTA) to determine whether the agency has adequate controls over personally identifiable information collected and stored, is properly securing personal information from unauthorized personnel and has followed the Department of Information Technology and Telecommunications' (DoITT) policies to ensure that personally identifiable information is being protected throughout its information-processing systems. We audit entities such as DFTA as a means of ensuring systems and technological resources of City agencies are cost-effective, efficient, secure, and operate in the best interest of the public.

DFTA generally has controls over the storage of personal identifiable information it has collected. However, DFTA does not adequately follow the DoITT polices concerning personal information protection through its information processing system. Specially, DFTA does not have a data classification policy requiring the classification of data into public, sensitive, private, and confidential categories, as specified by the DoITT Data Classification Policy. Also, DFTA lacks an adequate user access-control and password policy which poses a threat to the security of personally identifiable information (PII) by unauthorized personnel access. DFTA does not follow the DoITT information security policy to perform annual assessments of the electronic data collected and stored at contactor sites to identify patterns of security violations and to ensure that proper controls are instituted to prevent unauthorized access to PII. Finally, while DFTA has a disaster recovery plan, the agency did not conduct any disaster recovery tests as specified in the plan.

This audit contains six recommendations that if implemented should increase controls over personally identifiable information and minimize unintended disclosure.

The results of the audit have been discussed with DFTA officials, and their comments have been considered in preparing this report. Their complete written response is attached to this report.

If you have any questions concerning this report, please e-mail my audit bureau at audit@Comptroller.nyc.gov.

Sincerely,

John C. Liu

Table of Contents

AUDIT REPORT IN BRIEF 1

Audit Findings and Conclusions 1
Audit Recommendations 2

INTRODUCTION 3

Background 3
Objectives 4
Scope and Methodology 5
Discussion of Audit Results 7

FINDINGS AND RECOMMENDATIONS 8

Classification of Data Has Not Been Established 8
Identity Management Control Weaknesses 9
Lack of Central Access Controls 9
DIsaster Recovery Test Not Performed 10

APPENDIX List of DoITT Policies and Directives Used and DFTA Compliance

ADDENDUM Department for the Aging Response

The City of New York
Office of the Comptroller
Bureau of Financial Audit
IT Division

Audit Report on Department for the Aging Controls Over Personally Identifiable Information

7A10-092

AUDIT REPORT IN BRIEF

The New York City Department for the Aging (DFTA) promotes the independence, health, and well-being of older New Yorkers through advocacy, education, and the coordination and delivery of services. DFTA contracts with more than 400 local contractors to provide services to help older persons maintain or enhance their quality of life in the community. These contractors may collect personally identifiable information (PII) to provide Long Term Care Case Management program referrals or services at senior community centers.

In carrying out its mission, DFTA collects, processes, stores, and transmits many types of information about its clients. This data contains PII that is confidential or sensitive in nature, such as an individual's name, social security number, medical history and prescriptions, income, and any reports involving abuse. This data must be safeguarded to prevent theft, misuse, or disclosure to unauthorized persons that may result in criminal activities such as identity theft or other inappropriate uses of the information.

Audit Findings and Conclusions

DFTA generally has controls over the storage of personal identifiable information it has collected. It's "Computer Use and Electronic Processing Policy" defines personnel responsibilities to protect personal information on its systems. In addition, DFTA has case management standards for its contractors that require all case managers to be trained on the rights and privacy of clients. DFTA places records in a securely locked area, which includes locked file cabinets and storage rooms. Finally, DFTA's program officers conduct annual assessments to evaluate performance at the long-term care contractor sites.

However, DFTA does not adequately follow the DoITT polices concerning personal information protection through its information processing system. Specially, DFTA does not have a data classification policy requiring the classification of data into public, sensitive, private, and confidential categories, as specified by the DoITT Data Classification Policy. Also, DFTA

lacks an adequate user access-control and password policy which poses a threat to the security of PII by unauthorized personnel access. DFTA does not follow the DoITT information security policy to perform annual assessments of the electronic data collected and stored at contactor sites to identify patterns of security violations and to ensure that proper controls are instituted to prevent unauthorized access to PII. Finally, while DFTA has a disaster recovery plan, the agency did not conduct any disaster recovery tests as specified in the plan.

Audit Recommendations

To address these issues, we make 6 recommendations that DFTA should:

- Establish a data classification policy as specified by DoITT's policy which requires all information collected concerning the City's general business be classified into four categories: public, sensitive, private, or confidential.

- Comply with DoITT's password policy to create a lockout feature that is activated within 15 minutes of unattended inactivity by users.

- Revise password policy and require passwords to contain at least eight characters at contractor sites.

- Require all users to change their passwords at least every 90 days.

- Perform annual assessments of electronic data collected and stored at the contractor sites.

- Comply with its disaster recovery plan and perform the required disaster recovery test twice per year.

INTRODUCTION

Background

DFTA promotes the independence, health, and well-being of older New Yorkers through advocacy, education, and the coordination and delivery of services. In carrying out its mission, DFTA collects, processes, stores, and transmits many types of information about its clients. This data contains PII that is confidential or sensitive in nature, such as an individual's name, social security number, medical history and prescriptions, income, and any reports involving abuse. This data must be safeguarded to prevent theft, misuse, or disclosure to unauthorized persons that may result in criminal activities such as identity theft or other inappropriate uses of the information.

DFTA contracts with more than 400 local contractors to provide services to help older persons maintain or enhance their quality of life in the community. These contractors may collect PII to provide Long Term Care Case Management (LTC) program referrals or services at senior community centers (BSC). The LTC program includes conducting in-home assessments of homebound elderly clients and connecting them with available community-based services and benefits for which they are eligible. Case managers working for the LTC contractors conduct the in-home assessments and collect PII for each client, noting it on hard-copy documents. Later, they enter the client information in the DFTA Provider Data System (PDS). PDS is a client and service tracking application that offers an alternative to the process of maintaining manual client records and provides electronic data storage. Senior community centers maintain PII to provide services such as congregate meals or nutrition counseling. They use another system called the Senior Participant Profiles (SPP) system, which is also under DFTA's oversight.

The unintended disclosure of PII can be the result of the loss of backup computer tapes on Universal Serial Bus drives or laptop computers; exposure through Web-site attacks; unsecured or inappropriate e-mail exchanges or other electronic communications; or data storage exposures. Disclosure can also occur through the inappropriate disposal of paper files. There have been some high profile reports of PII being lost as a result of the poor stewardship of personal data by organizations entrusted with its care.

Several government and private organizations have been tracking data breaches to determine the risks and trends associated with those violations of personal information security. The nonprofit consumer information and advocacy organization Privacy Rights Clearing House (PRCH) started tracking PII incidents and found that over a four-year period (January 2005–June 2009) a total of more than 200 million records containing sensitive personal information involving U.S. companies and government agencies were at risk.

Widespread use of computerized recordkeeping and the growth in the use of the Internet to collect and share information has resulted in public concern about the privacy of PII collected by the government. These concerns include those related to the government's ability to ensure the accuracy and confidentiality of information about individuals and prevent misuse of personal information. The City of New York takes responsibility for the protection of PII that it collects while providing municipal services to the public. All employees and contractors with access to City information-processing systems are required to read and acknowledge the Department of

Information Technology and Telecommunications (DoITT) policy concerning the responsibilities of systems users prior to their being allowed access to City information systems.

In 1981, Mayoral Directive 81-2 charged the Department of Investigation (DOI) with the responsibility to establish citywide standards for information technology (IT) security and to ensure that programs, data files, data communications, and City computer systems comply with the standards. To that end, in 1998 DOI created the Citywide Information Security, Architecture, Formulation and Enforcement Unit (CISAFE). CISAFE was responsible for the creation, development, and enforcement of consistent and cost-effective security procedures, standards, and controls to ensure the confidentiality, integrity, and controlled accessibility of all electronic information that is processed through the City of New York. Later, in a Memo of Understanding dated August 8, 2006, between DoITT and DOI, DoITT became responsible for the formulation of security policies and the publication of Citywide information security policies and standards that all agencies and employees, and all contractors and vendors doing business with the City must follow.

By 2008, DoITT addressed how City agencies should protect business information assets. It did so through the release of several policies that require City agencies and vendors to have an appropriate level of data and facility protection, an assessment to determine the value of the information being maintained and the appropriate security requirements to protect City data resources and ensure their integrity and compliance with laws and regulations. In addition, the Municipal Records Management Division of the City's Department of Records and Information Services (DORIS) is responsible for the secure maintenance of records having continuing administrative and legal value and the retirement or proper disposal of records no longer in current use.

There has never been a comprehensive review of efforts by City agencies to determine whether there are adequate controls in place to safeguard PII. Given the inherent risks of inadequately protecting personal information, we have initiated a series of audits of City agencies to review and evaluate the sufficiency of their security and other controls over the PII they maintain

Objectives

The objectives of this audit were to determine whether DFTA:

- Has adequate controls over personally identifiable information that is being collected and stored.
- Is properly securing personal information from unauthorized personnel.
- Has followed DoITT's policies to ensure that personally identifiable information is being protected throughout its information-processing systems.

Scope and Methodology

This performance audit was conducted in accordance with generally accepted government auditing standards. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. This audit was conducted in accordance with the audit responsibilities of the City Comptroller as set forth in Chapter 5, §93, of the New York City Charter.

Our fieldwork was conducted from October 2009 to April 2010. To achieve our audit objectives, we interviewed various DFTA officials to obtain knowledge on their PII protection processes and controls. We reviewed relevant DoITT policies and City laws regarding the collection and security controls over PII at DFTA, including statutory requirements when such information is breached. We met with DFTA bureau and division officials that collected relevant information. Of the bureaus interviewed, we evaluated those that included divisions collecting information from clients that could be considered sensitive.

We obtained information from interviews and walkthroughs to determine whether the overall security awareness of DFTA personnel and its affiliates included responsibilities for safeguarding the agency's personal information. We also used the information obtained from these interviews to determine whether DoITT's Citywide Information Security Directive and Policies were in place and being followed, and to determine the overall security awareness of DFTA personnel responsible for safeguarding the agency's PII (see Appendix). In addition, we:

- Reviewed and analyzed Help Desk logs and security procedures for filing, storing, and retrieving client information in electronic equipment and file cabinets.

- Reviewed and inspected security reports from security software (Websense and DFTA's Firewall logs) that are in place to monitor agency systems to ascertain whether there have been any security breaches.

- Observed processes related to the retention and disposal of DFTA documents and DFTA shredding procedures that included information for the destruction and disposal of PII to determine whether DFTA followed the necessary measures for storing and destroying physical and electronic data.

- Reviewed a list of active employees with access to system applications, and databases used to store personal client information and compared those employees to those on the Payroll Management System (PMS) to determine whether all employees were currently active.

- Reviewed DFTA policies on personal information including the "End User Backup and Restore Policy," the "Software/Hardware Policy," the "Code of Conduct," and the "Wide/Local Area Network Policy" and the "Incident Response Policy."

- Reviewed and analyzed DFTA's "Computer Use and Electronic Processing Policy" to determine whether it complied with DoITT's Citywide Information Security Directive and Policies concerning the security of personal data.

- Reviewed and examined DFTA contingency planning procedures *LAN-WAN Documentation and Disaster Mitigation Consideration Manual* to determine whether it complied with DoITT's disaster recovery standards.

- Determined whether DFTA password procedures and its respective Case Management Services Agreement comply with DoITT's Citywide Information Security Directive and Policies.

- Conducted a system walkthrough to review how PDS and SPP function. Attended a PDS training session to gain an understanding of user needs, information collected, information stored, and functions using PII submitted by contractors.

- Examined PDS and SPP user manuals to determine whether they included procedures for protecting PII.

- Reviewed and analyzed DORIS guidelines, policies, and procedures to determine DFTA compliance.

- Reviewed Comptroller's Directive #1 mandated DFTA Financial Integrity Statement Filings for 2008; specifically those sections referencing Management Information Systems (MIS), Internet Connectivity, Risk Assessment, Data Classification, Information Security and Incident Response.

Between January 27, 2010, and February 3, 2010, we conducted a total of five field observations of DFTA LTC contractors at each of the New York City boroughs to assess overall security awareness and to determine whether DFTA policies and procedures for information security are being followed. We observed, examined, and evaluated the following during our visits:

- The physical storage of personal information collected to determine whether the practices complied with DFTA's Case Management Standards.

- Inspected file cabinets and unattended rooms containing client information to determine whether contractors are following the necessary procedures.

- The contractors' disposal policies for physical and electronic information to determine whether they complied with DoITT's Information Security Directive for Disposal of Information Assets.

- A list of inventory on electronic equipment such as scanners, printers, laptops and computers owned by DFTA and compared it to physical inventory.

- DFTA’s assessment tool to determine if the *Program Assessment System (PAS)* evaluated the performance and security of personal identifiable security.

- Determine if user account policy at the contractor location compiled with DoITT’s Citywide Information Security Directives and Policies.

As criteria, we used the DoITT Citywide Information Security Directives and Policies, the National Institute of Standards and Technology (NIST) *Generally Accepted Principles and Practices for Securing Information Technology System,* the New York City Comptroller’s Internal Control and Accountability Directive #18, “Guidelines for the Management, Protection and Control of Agency Information and Information Processing Systems,” DORIS guidelines, policies and procedures, NYS Information Security Policy “Cyber Security Policy P03-002” (2005), DFTA’s *BSC Program Standards for Safeguarding Personal Information*, and the DFTA *Case Management Standards*.

Discussion of Audit Results

The matters covered in this report were discussed with DFTA officials during and at the conclusion of this audit. A preliminary draft report was sent to DFTA officials and was discussed at an exit conference held on May 28, 2010. On June 3, 2010, we submitted a draft report to DFTA officials with a request for comments. We received a written response from DFTA on June 15, 2010. In their response, DFTA officials generally agreed with the findings and recommendations of this audit.

The full text of the DFTA response is included as an addendum to this final report.

FINDINGS AND RECOMMENDATIONS

DFTA generally has controls over the storage of personal identifiable information it has collected. It's "Computer Use and Electronic Processing Policy" defines personnel responsibilities to protect personal information on its systems. In addition, DFTA has case management standards for its contractors that require all case managers to be trained on the rights and privacy of clients. DFTA places records in a securely locked area, which includes locked file cabinets and storage rooms. Finally, DFTA's program officers conduct annual assessments to evaluate performance at the long-term care contractor sites.

However, DFTA does not adequately follow the DoITT polices[1] concerning personal information protection through its information processing system. Specially, DFTA does not have a data classification policy requiring the classification of data into public, sensitive, private, and confidential categories, as specified by the DoITT Data Classification Policy. Also, DFTA lacks an adequate user access-control and password policy which poses a threat to the security of PII by unauthorized personnel access. DFTA does not follow the DoITT information security policy to perform annual assessments of the electronic data collected and stored at contactor sites to identify patterns of security violations and to ensure that proper controls are instituted to prevent unauthorized access to PII. Finally, while DFTA has a disaster recovery plan, the agency did not conduct any disaster recovery tests as specified in the plan.

Classification of Data Has Not Been Established

The data classification process is critical to protecting the personal information held by DFTA. DoITT's data classification policy states that agencies should "ensure that business information assets receive an appropriate level of protection, the value of the information must be assessed to determine the requirements for security protection." We found DFTA has not complied with DoITT's data classification policy requiring the classification of data into public, sensitive, private, and confidential categories. DFTA is in the process of working on such a policy for their programs. As a consequence, DFTA is currently unable to monitor the value of data subject to loss and therefore has inadequate controls over PII.

Recommendation

DFTA should:

1. Establish a data classification policy as specified by DoITT's policy which requires all information collected concerning the City's general business be classified into four categories: public, sensitive, private, or confidential.

DFTA Response: DFTA agreed with this recommendation.

[1] See Appendix.

Identity Management Control Weaknesses

Each agency is responsible for the management of its user identities. This includes identity validation and registration, authentication, authorization and management of identities. To ensure that City agency systems are safeguarded against unauthorized access and accidental or deliberate interference, agency administrators are instructed by DoITT to review the settings of the users on networks and applications. The DoITT password policy states, "All passwords and personal identification Numbers (PINs) used to protect City of New York Systems must be appropriately configured, periodical changed, and issued for individual use." However, DFTA does not have an adequate policy or procedures to ensure the security of personal information and does not comply with DoITT policies, thus posing a threat to the personal information it has collected and stored on its systems. DFTA does not require its users to change their passwords for the PDS and SPP systems, nor has DFTA complied with the following provisions of the DoITT password policy:

- "Screen lock must be activated within fifteen (15) minutes of unattended inactivity."
- "Passwords and/or PINs must have a minimum length of eight (8) characters."
- "Passwords and/or PINs must be changed at least every ninety (90) days."

Recommendations

DFTA should:

2. Comply with DoITT's password policy to create a lockout feature that is activated within 15 minutes of unattended inactivity by users.

DFTA Response: DFTA agreed with this recommendation.

3. Revise password policy and require passwords to contain at least eight characters at contractor sites.

DFTA Response: DFTA agreed with this recommendation.

4. Require all users to change their passwords at least every 90 days.

DFTA Response: DFTA agreed with this recommendation.

Lack of Central Access Controls

The DoITT information security policy states, "Information Owners are responsible for ensuring that electronic data systems on which city information resides and is processed are periodically reviewed for compliance with the governing information security policy, directives, and standards."

DFTA provided a list of all LTC contractors in the five boroughs. Out of 23 sites, we selected five (one from each borough) when we performed our observations between Jan 27, 2010, and February 3, 2010. During our walkthroughs, three of the sites had their own IT personnel while others relied on calling DFTA for maintenance as needed. DFTA does not perform an annual assessment of the hardware and software at the sites. It also relies on all the individual sites to monitor its users. Such assessments would help DFTA to identify patterns of security violations and to ensure that proper controls are instituted to prevent unauthorized access to PDS. The DoITT database management systems directive states, "All vendor or third parties activities must be directly monitored by the database administer and database level auditing must be enabled on all vendor and third party user accounts."

Recommendation

DFTA should:

5. Perform annual assessments of electronic data collected and stored at the contractor sites.

DFTA Response: DFTA agreed with this recommendation.

<u>Disaster Recovery Test Not Performed</u>

According to DoITT's Citywide Information Security Directive and Policies, an agency must develop a disaster recovery plan to safeguard important data from damage. Furthermore, the plan must detail the procedures the City agency must follow to put its systems back in service after a disaster and must require that the agency conduct periodic tests of the plan.

DFTA provided us with its disaster recovery plan, *LAN-WAN Documentation and Disaster Mitigation Considerations Manual.* The DFTA plan was last updated in August 2009 and states, "to maintain the concurrence of this plan, twice yearly tests of the plan is required. Disaster Recovery plan test schedule is during the second week of March and September." We found that DFTA did not conduct disaster recovery tests as specified in its manual. If DFTA does not perform regular formal disaster recovery tests, it leaves itself vulnerable to the loss of mission-critical information in the event of a disaster.

Recommendation

DFTA should:

6. Comply with its disaster recovery plan and perform the required disaster recovery test twice per year.

DFTA Response: "DFTA would like to clarify the language of its disaster recovery plan. Although the plan does literally say that DFTA should perform disaster recovery tests twice per year, DFTA intended its disaster recovery plan to state that DFTA should test its disaster recovery plan for up-to-date vendor and staff information and network infrastructure/specs twice a year."

Auditor Comment: In its response, DFTA suggests that the disaster recovery plan does not correctly represent current information and practice. However, despite its stated practice of twice-yearly testing, DFTA has not performed a formal disaster recovery test since August 2009 and leaves itself vulnerable in the event of a disaster should aspects of the plan fail. DFTA should immediately revise its plan to reflect current information and practice, disseminate it throughout the agency, and conduct the tests accordingly.

Appendix

List of DoITT Policies and Directives Used and DFTA Compliance

DoITT Policies and Directives	DFTA Compliance	Reasons/Comments
Data Classification Policy	No	Does not classify data into public, sensitive, private, and confidential categories. DFTA stated “they are in the process”
Identity Management and Password Policy	No	1. Password and User controls weakness at contractor locations. 2. Password does not have a minimum length requirement of 8 characters on PDS. 3. Does not require users to change their passwords every 90 days. 4. No lockout feature that is activated within 15 minutes of unattended inactivity on all DFTA staff.
User Account Management Directive	No	Does not require users to change their passwords every 90 days
Database Management Systems Directive	No	Does not require users to change their passwords as defined in the policy and the passwords do not have a minimum length requirement of 8 characters on PDS and SPP.
Incident Response Policy	Yes	
Personnel Security Policy	Yes	
Portable Data Security Policy	Yes	
Security Accreditation Process*	N/A	DFTA has not developed a new system application
User Responsibility Policy	Yes	
Directory Services Directive	Yes	
Disposal of Information Assets Directive	Yes	
Incident Response Directive	Yes	
Risk Assessment Directive	Yes	

*Process applies only when new systems are developed

Department for
the Aging

LIlliam Barrlos-Paoli
Commissioner

2 Lafayette St.
New York, NY 10007

212 442 1100 tel
212 442 1095 fax

June 15, 2010

Ms. Tina Kim, Deputy Comptroller for Audits
Office of the Comptroller
One Centre Street, Room 1100
New York, NY 10007-2341

Re: Comptroller's Audit on Department for the Aging Controls
Over Personally Identifiable Information 7A10-092

Dear Deputy Comptroller Kim:

Thank you for the opportunity to respond to your June 2, 2010 audit of the Department for the Aging's (DFTA's) controls over personally identifiable information. We are pleased with the positive findings of the audit and appreciate the constructive recommendations for improving our internal controls. Please see below for detailed DFTA responses to the audit findings.

Comptroller's Recommendation 1: DFTA should establish a data classification policy as specified by DOITT's policy which requires all information collected concerning the City's general business be classified into four categories: public, sensitive, private or confidential.

DFTA Response: DFTA's Information Technology Department was transferred to the Human Resources Administration (HRA) in FY10. This organizational change delayed DFTA's work on establishing a data classification system. We agree with your recommendation and are working towards establishing a data classification system and assigning a data steward with HRA.

Comptroller's Recommendation 2: DFTA should comply with DoITT's password to create a lockout feature that is activated within fifteen minutes of unattended inactivity by (PDS and SPP) users.

DFTA Response: The network for DFTA's Senior Participant Profiles (SPP) system does time out the user when the system remains inactive after fifteen minutes.

We agree with your recommendation regarding DFTA's Provider Data System (PDS) database. PDS is an antiquated database application created twenty years ago, and the system has no timed lockout feature as part of the application. DFTA will be directing case management agencies using PDS to implement a timeout feature in their network operating system to lock out users after fifteen minutes of inactivity.

Comptroller's Recommendation 3: DFTA should revise its password policy and require passwords to contain at least eight characters at contractor sites.

DFTA Response: We agree with your recommendation. The eight character minimum has been implemented in SPP. PDS runs locally, and many of the system security protocols are controlled by the case management programs' own IT departments. In these situations, the Department will direct and require programs to implement the minimum eight character password control in their network operating system for computers using PDS.

Comptroller's Recommendation 4: DFTA should require all (PDS and SPP) users to change their passwords at least every 90 days.

DFTA Response: We agree with your recommendation. We have started adjusting SPP to require contracted programs to change the SPP password after 90 days. The Department will direct case management programs using PDS to set up this security feature of changing the password every 90 days on their network operating system for computers using PDS.

Comptroller's Recommendation 5: DFTA should perform annual assessments of electronic data collected and stored at the contractor sites.

DFTA Response: We agree with your recommendation. DFTA will draft and implement security standards and a security checklist for contracted case management programs using DFTA's PDS database. HRA MIS field staff will use this checklist when they do annual site visits to assess whether security controls are maintained at the sites. The results of this assessment will be shared with DFTA's Long-term Care program bureau for additional joint follow-up and monitoring.

Comptroller's Recommendation 6: DFTA should comply with its disaster recovery plan and perform the required disaster recovery tests twice per year.

DFTA Response: DFTA would like to clarify the language of its disaster recovery plan. Although the plan does literally say that DFTA should perform disaster recovery tests twice per year, DFTA intended its disaster recovery plan to state that DFTA should test its disaster recovery plan for up-to-date vendor and staff information and network infrastructure/specs twice a year.

DFTA is a small City Agency, and its resources and data needs do not support an off-site location for its IT systems that can support actual mock disasters twice a year. DFTA's e-mail and internet systems are hosted by other City agencies. DFTA's data is backed up daily and stored up to three weeks at an off-site location. This back-up ability is constantly "tested" on a regular basis from users requesting data to be pulled from these back-up tapes. DFTA will revise its current disaster recovery plan to clarify this ambiguity.

In closing, we appreciate the opportunity to respond to the draft audit. If you have any questions about this written response, please contact John Jones at (212) 442-1156 or by e-mail at jjones@aging.nyc.gov.

Sincerely,

Lilliam Barrios-Paoli
Commissioner

cc: Sally Renfro, First Deputy Commissioner (DFTA)
Maureen Murphy, General Counsel (DFTA)
Karen Shaffer, Assistant Commissioner (LTC)
Jane Fiffer, Deputy Assistant Commissioner (LTC)
Frank Guglielmo, Director of IT (HRA)
Sal Rullan, Deputy Director of IT (HRA)
Richard Siemer, Deputy Commissioner, MIS (HRA)
Faigi Hornung, Director of Financial Audits (Comptroller's Office)
Vincent Liquori, Assistant Director for IT/Support Services (Comptroller's Office)