A REPORT BY THE NEW YORK STATE OFFICE OF THE STATE COMPTROLLER

Alan G. Hevesi
COMPTROLLER

NEW YORK STATE OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE

NEW YORK STATE OFFICE FOR TECHNOLOGY

NEW YORK CITY HUMAN RESOURCES ADMINISTRATION

WELFARE MANAGEMENT SYSTEM: NEW YORK CITY GENERAL AND APPLICATION CONTROLS
2002-N-1

DIVISION OF STATE SERVICES

OSC Management Audit reports can be accessed via the OSC Web Page:

http://www.osc.state.ny.us

If you wish your name to be deleted from our mailing list or if your address has changed,

contact the Management Audit Group at (518) 474-3271

or at the

Office of the State Comptroller

110 State Street

11th Floor

Albany, NY 12236

Alan G. Hevesi
COMPTROLLER

Report 2002-N-1

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

Mr. Michael McCormack
Director
New York State Office for Technology
State Capital
Albany, NY 12224

Mr. Jason Turner
Commissioner
New York City Human Resources Administration
180 Water Street
New York, NY 10038

Dear Commissioner Wing, Director McCormack and Commissioner Turner:

The following is our report concerning the general and application controls of New York State's Welfare Management System, as it relates to New York City.

This audit was conducted pursuant to the State Comptroller's authority as set forth in Article V, Section 1, of the State Constitution; Article II, Section 8, of the State Finance Law; and Article III of the General Municipal Law. Major contributors to this report are listed in Appendix A.

Office of the State Comptroller
Division of State Services

September 26, 2003

EXECUTIVE SUMMARY

NEW YORK STATE OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE

NEW YORK STATE OFFICE OF TECHNOLOGY

NEW YORK CITY HUMAN RESOURCES ADMINISTRATION

WELFARE MANAGEMENT SYSTEM: NEW YORK CITY GENERAL AND APPLICATION CONTROLS

SCOPE OF AUDIT

The New York State Office of Temporary and Disability Assistance (OTDA), in accordance with Chapter 55, Section 21, of the Social Services Law of New York State (State), 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 the New York State Office for Technology (OFT) are responsible for supporting and maintaining the Welfare Management System (WMS). Established in 1997, OFT is charged with the coordination of the State's vast technology resources. It manages a consolidated New York State Data Center (Data Center) that supports WMS' data processing requirements, as well as those of 20 other agencies. However, the responsibility for managing local user access accounts and permissions is in the hands of local district coordinators. 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. The New York City Human Resources Administration (HRA) administers WMS through its Family Independence Administration (FIA). FIA operates local income support/job

centers in the five boroughs of New York City (City), where its staff process applications for public assistance, food stamps, and Medicaid.

WMS consists of two application subsystems: "Upstate," which is used to maintain the records of clients living in counties outside the City, and "New York City," which contains the data of clients who are City residents. We had previously conducted a general and application control audit of the upstate Welfare Management System and issued a report on our findings (Report 2001-S-35, *Office of Temporary and Disability Assistance, Welfare Management System: General and Application Controls*, issued March 14, 2003).

Our audit sought to answer the following question for the period January 1, 1999 through December 20, 2002:

- Have OTDA, OFT and HRA instituted general and application controls that provide reasonable assurance that the New York City WMS data is accurate and reliable, and protected from the risk of unauthorized physical and logical access?

AUDIT OBSERVATIONS AND CONCLUSIONS

We could not express an opinion on the accuracy and reliability of public assistance eligibility data because HRA could not provide us with case file records needed to verify 13 percent of our sampled WMS data elements. In addition, our tests showed that 8 of 44 cases we sampled, where we had sufficient budget-related supporting documentation, had incorrect benefit determinations because of data entry errors. (See pp. 7-8)

To verify the validity and reliability of WMS data, we selected a random statistical sample of 70 HRA cases, including 58 that were active. The actual number of data elements we tested varied by case, depending on the number of individuals involved. Our sample of active cases included 733 data elements, but we found that HRA's files did not contain the required supporting documentation for 94 of these. We found 39 errors and 23 variances in the remaining 639 data elements. A variance is an inconsistency between the WMS data and the source documentation; however, the clients' information was validated by the Social Security Administration. (See p. 8)

We also recalculated public assistance grants (grants) for the 58 cases and found that WMS had calculated the grants accurately based on information entered in WMS. However, we found that HRA employees had entered data incorrectly for eight cases, leading to the understatement of seven of the grants and the overstatement of one. (See pp. 8-9)

We found WMS security controls need improvement. For example, we found weaknesses in the granting and monitoring of user rights, and in the use of the security violation reports. We also found improvements can be made in training

users regarding security awareness. We made a total of 20 recommendations addressed to OTDA, OFT and/or HRA to enhance this area. (See pp. 11-24)

We found that OFT's disaster recovery plan lacks significant provisions. In addition, OTDA has not provided OFT with WMS recovery procedures, an application processing schedule, or a strategy for printing should a disaster occur. (See pp. 25-27)

Because some weaknesses we identified could be considered sensitive, we have not included the details relating to those weaknesses in this report. Instead, we have conveyed our findings to appropriate officials during the audit.

COMMENTS OF OTDA, OFT, AND HRA OFFICIALS

OTDA, OFT and HRA officials generally agreed or partially agreed with the report's findings and recommendations.

CONTENTS

INTRODUCTION

Background

The New York State Office of Temporary and Disability Assistance (OTDA), in accordance with Chapter 55, Section 21, of the Social Services Law of New York State (State), 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 the New York State Office for Technology (OFT) have responsibilities to support and maintain the Welfare Management System (WMS). Established in 1997, OFT is charged with the coordination of the State's vast technology resources. It manages a consolidated New York State Data Center (Data Center) that supports OTDA's data processing requirements, as well as those of 20 other agencies. For example, under the terms of a service-level agreement with OTDA, OFT is primarily responsible for the system's hardware-operating environment, including file management, disaster recovery, system backup, and computer center maintenance and support for WMS. The responsibility for managing local user access and permissions for WMS is in the hands of local district coordinators. OTDA is primarily responsible for administering WMS and maintaining WMS computer application.

Through its Family Independence Administration (FIA), the New York City Human Resources Administration (HRA) administers the public assistance (Temporary Assistance for Needy Families, or TANF), food stamps, and Medicaid programs in New York City (City). FIA operates local income support/job centers in the City's five boroughs, where staff process applications for the programs it administers. For the month of

December 2002, HRA provided services to more then 421,000 public assistance recipients and administered gross public assistance expenditures of more than $96 million.

WMS consists of two application subsystems: “Upstate,” which is used to maintain the records of clients living in counties outside the City, and “New York City,” which contains the data of clients who are City residents. In a network, various computer resources such as desktop computers, printers, file servers, and computer applications (e.g., word processing applications, data base applications, and specialized applications) are linked together and shared by different individual users. To access a computer application in this type of data processing environment, users must first obtain access to their network.

WMS collects, stores, validates, and processes basic demographic and eligibility data that it receives from districts over dedicated communication channels. It is designed to minimize the number of duplicate payments made to eligible clients and to help eliminate mismanagement and fraud. It is also designed to serve the client by maintaining accurate eligibility data at the same time it protects the client’s privacy. Edit checks are built into the system to help district staff verify the appropriateness, accuracy, and completeness of data entered in WMS. These checks are intended to assure management that program standards are being applied uniformly by enforcing and validating categorical and financial policies and regulations.

On July 29, 1999, New York State initiated a plan to upgrade its human services agencies’ ability to support network-based information technology. Part of this project includes the implementation of a single Statewide WMS database, known as WMS Redesign, to replace the two existing subsystems. The plan calls for the existing WMS to continue performing its primary eligibility-processing functions at the same time it uses new automation tools to create an integrated case management system. Ultimately, the planned system will facilitate a “shared front-end” environment among human services agencies that will enable them to meet clients’ needs more effectively.

In June 2001, district employees began using application software on their personal computers to access WMS and to access the network maintained for their own district applications. Access to WMS in this manner was accomplished

through the Human Service Network (HSN). HSN is a combination of hardware, software, transmission media and telecommunications that makes it possible for certain computers used by several State agencies to be interconnected. In such a network, various computer resources, including desktop computers, printers, file servers, and computer applications (e.g., word processing and data base applications as well as specialized applications such as WMS) are shared by various users in several locations. These users may be either district workers or employees of income maintenance offices, child welfare units, or voluntary agencies.

Both the upstate WMS and New York City WMS are accessible on the HSN located in the State's Data Center. We had previously conducted a general and application control audit of the upstate Welfare Management System and issued a report on our findings (Report 2001-S-35, *Office of Temporary and Disability Assistance, Welfare Management System: General and Application Controls*, issued March 14, 2003).

Audit Scope, Objective, and Methodology

During our audit, which covered the period January 1, 1999 through December 20, 2002, we examined the OTDA's general and application controls, including selected aspects of network controls, over the processing of electronic data for the New York City WMS. Our objective for this performance audit was to determine whether OTDA, OFT, and HRA have instituted general and application controls that provide reasonable assurance that New York City WMS data is accurate and reliable, and protected from the risk of unauthorized physical or logical access.

To accomplish our objective, we interviewed OTDA, OFT, and HRA officials and reviewed pertinent policies and procedures relating to the overall computer operations of the Data Center. Our review covered controls over organization and management, system software and hardware, and security. We judgmentally selected a job center from each of the five boroughs that comprise New York City. The job centers selected, based on relative caseloads, were Dekalb Job Center in Brooklyn, Dyckman Job Center in Manhattan, Jamaica Job Center in Queens, Melrose Job Center in Bronx, and Richmond Job Center in Staten Island. To gain an understanding of terminal security control procedures being used in HRA's job

centers, we evaluated the Transaction Terminal Security System (TTSS) and its implementation at the job centers.

In addition, we reviewed TTSS guidance documents; interviewed local TTSS security coordinators; and reviewed the procedures for adding and deleting users, assigning rights to applications, and monitoring usage. We interviewed staff at all five job centers and observed the practices they follow. We randomly-selected TANF cases administered by FIA and compared selected WMS data elements with case file source documents. Because some of the weaknesses we identified could be considered sensitive, we have not included the details relating to these weaknesses in this report. Instead, we have conveyed those findings to appropriate officials during the audit.

As is our practice, we notify agency officials at the start of each audit that we will be requesting a representation letter in which agency management provides assurance, to the best of their knowledge, concerning the relevance, accuracy, and competence of the evidence provided to the auditors during the course of the audit. The representation letter is intended to confirm oral representations made to the auditors and to reduce the likelihood of misunderstandings. In the representation letter, agency officials assert that, to the best of their knowledge, all relevant financial and programmatic records and related data have been provided to the auditors. Agency officials further affirm either that the agency has complied with all laws, rules and regulations applicable to its operations that would have a significant effect on the operating practices being audited, or that any exceptions have been disclosed to the auditors.

However, officials at the New York City Mayor's Office of Operations have informed us that, as a matter of policy, Mayoral agency officials will not provide representation letters in connection with our audits. As a result, we lack assurances from HRA officials that all relevant information was provided to us during the audit. We consider this refusal to provide a representation letter to be a scope limitation on the findings and conclusions presented in this report.

Except as noted above, 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 OTDA, OFT, and HRA that are included within our audit scope. Further, these

standards require that we understand the internal control structure of OTDA, OFT, and HRA and the extent to which they comply with those laws, rules and regulations that are relevant to them, which 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 considered 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.

We use a risk-based approach when selecting activities to be audited. This approach focuses our audit efforts on those operations that have been identified through a preliminary survey as having the greatest probability for needing improvement. Consequently, by design, finite audit resources are used to identify where and how improvements can be made. Thus, little audit effort is devoted to reviewing operations that may be relatively efficient or effective. As a result, our audit reports are prepared on an "exception basis." This report, therefore, highlights those areas needing improvement and does not address in detail activities that may be functioning properly.

Response of OTDA, OFT, and HRA Officials to Audit

A draft copy of this report was provided to OTDA, OFT, and HRA officials for their review and comment. Their comments, as appropriate, have been considered in preparing this report, and are included as Appendix B. In addition, the State Comptroller's Notes to the responses are included as Appendix C.

OTDA, OFT and HRA officials generally agreed or partially agreed with the report's findings and recommendations.

Within 90 days after the final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the Office of Temporary and Disability Assistance, and the Director of the Office for Technology, shall report to the Governor, the State Comptroller, and 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 reason therefor.

In addition, we request that the Commissioner of HRA report to the State Comptroller, advising what steps were taken to implement the recommendations contained in this report, and where recommendations were not implemented, the reasons therefor.

DATA INTEGRITY

Controls over the validity and reliability of data include policies and procedures that help assure management that system data accurately represent information contained in source documentation. If public assistance payments are to be accurate, HRA employees must enter data accurately.

Data Element Testing

HRA is responsible for the entry of client demographic and financial data in the WMS. The accuracy of this data should be assured through system edits and supervisory case review.

WMS offers more than 900 system edits that can verify the integrity of specific data elements. For example, edits attest that data has been entered in the proper format and that they are compatible with other data elements. If an edit identifies a data error, WMS requires that the data errors be corrected before the WMS files are updated. When we observed data entry of WMS case information, we noted that the edits operated as designed.

However, edits cannot guarantee that the data entered represent the data in the source documents. For example, a user might transpose digits when entering a number, but as long as the entered number was the correct length, the error would pass the edit. In this situation, if an HRA supervisor followed a review procedure comparing the data entered with the data on the source documents, the error would be detected.

When data updates have cleared system edits, an authorization form is printed. Although supervisors are required to review and sign this form as an approval and an attestation of accuracy of the data processed in WMS, we found that HRA management has not developed written procedures that instruct supervisors about what they should do when they conduct these reviews (i.e., compare system data with source documentation). We believe HRA should develop procedures that explain a supervisor's role and responsibilities during supervisory reviews.

To determine the integrity of WMS data, we randomly selected 70 of the 90,785 TANF cases administered by FIA and included on WMS. We tested 58 of these (12 had closed between the time we generated our sample and the time we conducted our tests) by printing their WMS case comprehensive and latest budget data as of July 2002 and tracing selected elements of this data to source documents kept as hardcopy file or as electronically-scanned images. During this process, we noted that some scanned documents were not legible, making them useless for substantiating system data. We believe staff and supervisors should ensure that scanned documents are legible.

We selected eight demographic and budgetary data elements for testing: names of the individuals who are active on the case, date of birth for active individuals, Social Security Numbers (SSNs) for active individuals, actual monthly shelter cost, shelter type, fuel type, gross wages, and calculated net income. Although OTDA officials told us they consider all WMS data to be important, we selected these eight data elements for audit purposes because they are relevant to eligibility determination.

Although we sampled 58 cases, the actual number of data elements we tested varied, depending on the number of individuals in each case. In total, our sample included 733 data elements. However, because 94 (or 13 percent) of these elements lacked required supporting documentation, we could not test them. As a result, we tested 639 of the original 733 data elements and found 39 errors. We also noted 23 instances in which the Social Security Administration had validated the individual's SSN even though there was a variance between the WMS data and the individual's source documents. OTDA and HRA should make sure that job centers are obtaining the required supporting documentation and that job centers correct the errors and variances we noted during this audit.

From the same case sample, we manually recalculated the case's budget to determine whether WMS had calculated the benefits properly. The system had calculated the benefits correctly in every case, based on the data input. However, for 44 of the cases where we had sufficient budget-related supporting documentation, we found eight instances in which data entry errors had affected the public assistance grant. Seven of the eight budgeting errors were understatements of the client's grant; the remaining one had resulted in an overstatement. The seven public assistance recipients received

less money than the amount to which they were entitled. The errors generally occurred because staff had entered a shelter cost that was not consistent with the client's supporting documentation. We encourage HRA to review these cases and to modify the grants accordingly.

HRA should make every effort to verify that employees are entering accurate and complete data in WMS. Inaccurate personal identifiers can impair data matches and result in the inappropriate denial or issuance of benefits; and, as our tests indicate, inaccurate budget information can result in the issuance of inaccurate public assistance grants.

As previously stated, supervisors are required to perform supervisory reviews, verifying that the WMS data is accurate. We found that system edits have been developed for completeness, compatibility, and entry format. However, edits alone cannot guarantee that the WMS data is accurate. The information on source documents must be reviewed to help ensure that data on the system is accurate. Furthermore, our budget recalculations indicated the system is calculating public assistance payments accurately. Finally, because HRA did not provide supporting documentation for approximately 13 percent of the elements included in our sample, we were unable to determine whether the data is reasonably accurate. Thus, OJDA and HRA management lack assurances in these instances that WMS public assistance eligibility data is accurate and reliable.

HRA officials agreed with our data integrity findings and recommendations. They also told us they have developed a corrective action plan to improve case file integrity.

Recommendations

To HRA:

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

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

Recommendations (Cont'd)

To OTDA and HRA:

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

To OTDA:

4. Verify that HRA implements the data integrity recommendations in this report.

COMPUTER SECURITY

To provide reasonable assurance that computer resources are being protected against unauthorized modification, disclosure, loss, or impairment, agencies should develop and implement a security system that can prevent and detect unauthorized access. Such a system limits user access to both applications and data by allowing users only the access they need to perform their duties, preventing them from performing incompatible duties, and narrowly assigning access to sensitive applications (including the security system). Inadequate access controls can diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data.

The New York State Department of Family Assistance developed the Transaction Terminal Security System (TTSS) as a mandatory requirement of WMS and it is the security system that OTDA and the local social services districts currently use for WMS. TTSS consists of logical controls that can be used to add, delete, and identify users; assign rights to specific program applications; and track activity. TTSS is maintained by the OFT and implemented at the district level through designated local Terminal Security Coordinators.

TTSS was designed to accommodate varying degrees of terminal security control so that districts, which vary widely in size, caseload, and operating procedures, could provide the security controls best suited to their needs. HRA's Office of Data Security Management (ODSM) is responsible for granting access rights using the logical framework provided by TTSS. At each job center, a location coordinator is required to observe and monitor terminal reconfigurations, perform periodic reviews of processor logs, and assess operational and personnel changes that affect either a terminal's access or a user's functions. It is also the location coordinator's responsibility to report the latter changes to ODSM, to receive and distribute user ID/password envelopes to staff, and to promote information protection awareness among staff.

The U. S. General Accounting Office (GAO) has developed extensive guidelines regarding access to computer and security

systems. These guidelines are intended to assist auditors in dealing with issues that should generally be considered in any review of computer-related controls over the integrity, confidentiality, and availability of computerized data. To gain an understanding of terminal security control procedures being used in HRA's job centers, we evaluated TTSS and its implementation at the Dekalb, Dyckman, Jamacia, Melrose, and Richmond locations.

In addition, we reviewed TTSS guidance documents; interviewed local TTSS security coordinators; and reviewed the procedures for adding and deleting users, assigning rights to applications, and monitoring usage. We found that TTSS provides a logical framework that limits access to authorized users, allows the assignment of specific applications to matched duties, and limits the ability to make security changes to designated coordinators. It also tracks user activity, thereby allowing usage monitoring and security investigations.

During our audit, we found weaknesses in the TTSS logical access controls. We also found that ODSM and location coordinators are not using available security reports to monitor WMS access and usage in the job centers. TTSS coordinators, in accordance with their TTSS Coordinator Handbook, are required to ensure that ODSM receives timely notice of personnel changes; however, they do not always notify ODSM of these changes. It is important to notify security managers immediately when an employee terminates or otherwise no longer requires the access provided by the user ID, and to verify that users are given only the access they have been authorized to exercise.

We also found that location coordinators are not monitoring compliance with access policy by comparing authorization requirements with the actual access granted, and that there are opportunities for location coordinators to foster greater security awareness among system users.

Password Security

Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user identification numbers (user IDs), passwords, or other identifiers that are linked to predetermined access privileges. Logical access controls should be designed

to restrict legitimate users to the specific systems, programs, and files they need, and to prevent others from entering the system at all.

Logical security controls also enable an organization to identify individual users or computers that are authorized to have access to computer networks, data, and resources; restrict access to specific sets of data or resources; produce and analyze audit trails of system and user activity; and take defensive measures against intrusion.

Through the identification process, a computer system distinguishes one user from all others, usually with user IDs. User IDs are important because they are the means by which specific access privileges are assigned and recognized by the computer.

The most widely-used means of authentication is password protection. However, passwords are not conclusive identifiers of specific individuals, since they may be guessed, copied, overheard, or recorded and played back. Typical controls for protecting passwords include: having the assigned users create their own passwords; requiring passwords to be changed periodically (about every 30 to 90 days); not displaying passwords when they are entered; requiring passwords to be a minimum of 6 characters; prohibiting the use of names, words, or old passwords within 6 generations, while encouraging the use of alphanumeric passwords; and uniquely identifying users rather then having users within a group share the same ID or password.

To help prevent an unauthorized person from logging on to the system by guessing a password, users should be limited in the number of unsuccessful attempts they can make to log on to the system. Potential users are typically allowed three or four attempts to log on. Using this restriction in conjunction with the use of alphanumeric passwords reduces the risk that an unauthorized user can gain access.

We identified some password security weaknesses and reported them to OTDA and OFT officials. We have not included these details in this report.

Recommendation

To OTDA and OFT:

5. Implement the password security recommendations made during the course of our audit.

Monitoring Security Violations

According to the GAO, access control software should be used to maintain an audit trail of security accesses that will reveal how, when, and by whom specific actions have been taken. Typically, audit trails may include user ID, resources accessed, date, time, terminal location, and specific data modified. Such information is critical in monitoring both compliance with security policies and actual violations of security.

The TTSS captures all activity, including sign-on, sign-off, and associated edits, as well as attempts to perform unauthorized transactions and terminal timeouts. This information is available upon inquiry to site logs, which OFT Security uses to generate a weekly Terminal Security Violations Report (Report) that details, by site and date, various types of security violations, including failed sign-on attempts, incorrect passwords, time-outs, and disallowed transactions. Local security coordinators are responsible for reviewing the Report to determine whether there are patterns of violations they should address.

The Report lists violations by terminal and by user, in aggregate, by day (the total number of each type of violation, by the user, at the reported terminal). Transmitted electronically to each district on a weekly basis, it does not display each individual violation. For example, if a user "timed-out" at 9:30 a.m., 10:30 a.m., and 11:45 a.m., the report would show only that the time-out violation occurred three times that day for that user at that terminal. Although specific violation details such as time of day are not displayed, the Report does allow security coordinators to monitor usage by identifying the terminals or users related to the violations. In addition, by making local TTSS inquiries, the security coordinator could obtain the details of activity at specific terminals in real time for the current business week, as well as detailed transaction data. As of July

2002, HRA was administratively responsible for more than 13,000 WMS users.

When we obtained the Reports OFT provided to HRA for the week that ended on July 6, 2002, we found numerous violations at each job center, the most common being terminal timeouts. According to the WMS System Reference Manual (Manual), the purpose of the timeout is to limit the length of time a terminal is available, thereby reducing the possibility of access by unauthorized persons to unattended signed-on terminals.

The Report shows the users who had six or more daily timeouts. Terminal timeouts may indicate that a user left a terminal signed-on and unattended, leaving the system and system data vulnerable to exploitation. WMS users should always sign off on their terminals when they must leave it. Under no circumstances should a user leave a terminal unattended with data displayed.

The HRA official who receives the Reports from OFT expressed the belief that timeout violations do not require follow-up action. However, terminal timeouts may be an indicator of poor user security practices and follow-up action is required to determine the cause. Because it is not practical to follow up on every terminal timeout, coordinators should identify any users with an unusual number of violations and discuss the situation with them to identify the causes. Through this process, coordinators can identify poor security practices and take corrective action.

The effectiveness of the Report as a monitoring tool depends both on the usefulness of the information conveyed and the report recipient's actual use of the data. HRA officials told us they have not used the Report in more than a decade because the State has not conveyed its importance or specified ways in which it should be used for monitoring purposes. They said each Report they receive is retained for six months and then destroyed.

When we reviewed the Reports, we noted several discrepancies. For example, we found that they did not include all location codes (logical codes that identify the physical address to which a user is assigned) for which HRA is administratively responsible. In addition, the Report reflected violations for days outside the weekly reporting period, contained system violations for users administered by the Office

of Children and Family Services, and contained duplicate Reports for multiple location codes. We believe these discrepancies would have been discovered earlier if HRA had used the Reports as intended.

OTDA and OFT officials are modifying the report format to distinguish OTDA employees from persons employed by other agencies. Further, OFT officials explained that they may have inadvertently sent duplicate reports to HRA during the transition from paper to electronic reporting. OFT expressed an interest in determining why the discrepancies had occurred, so we provided them with copies for their review.

Recommendations

To HRA:

6. 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).

To OFT:

7. Verify that the Terminal Security Violation Reports OFT provides to HRA are complete and accurate.

8. Meet with HRA officials and explain the important uses of the Report.

To OTDA:

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

Updating User Access

Management or its representatives should use standardized access forms to approve the addition, removal, and/or modification of user rights. It is important to notify security managers when an employee leaves or otherwise no longer requires the access provided, and policies should be in place to clearly assign these responsibilities. To ensure compliance with access authorizations, management should require periodic comparisons of such authorizations to actual access activity and user rights.

In the five job centers we visited, we found that location coordinators complete special forms to request, terminate, and/or modify user or terminal access rights. Once the location coordinator completes these forms, they are forwarded to ODSM, along with a transmittal form for processing.

We found that ODSM has defined the location coordinators' role and the procedures they must follow in its TTSS Coordinator Handbook (handbook). However, the handbook is outdated and was last revised in March 1988. We found that the handbook does not reflect the forms currently used by location coordinators; it is missing definitions for more then 40 percent of the WMS functions the location coordinator must assign; and it contains numerous incorrect addresses, phone numbers, and items of personnel information. To assure management that location coordinators are carrying out their responsibilities correctly, HRA must see that the procedures they are required to follow are communicated clearly. We encourage ODSM to update the handbook and distribute the revised version to all location coordinators.

We also found that location coordinators do not retain a copy of the original forms; nor does ODSM return copies to them. In addition, location coordinators do not review user access/terminal rights to determine whether ODSM has assigned them as authorized. ODSM files the original TTSS forms, by date processed, in a secure room. To substantiate authorizations and provide accountability, authorization forms should be readily accessible. Under ODSM's current filing method, it is almost impossible to obtain and review these forms. Location coordinators also do not periodically review user and terminal access rights to verify that they are still appropriate. We believe HRA's controls would be stronger if it

required location coordinators to see that ODSM processed the forms properly by comparing the functions assigned to the functions authorized. Although users are likely to notify their location coordinator if insufficient rights are assigned, they are unlikely to be aware that they have been awarded greater rights than required or authorized − and even less likely to point it out to their location coordinator. Location coordinators who regularly review authorization assignments would be in a better position to identify such situations.

TTSS can provide ODSM and location coordinators with an authorized functions report that lists, for each job center, all active user IDs as well as the assigned user's name, job title, identification number, and assigned functions. A similar authorized function report identifies each job center terminal and the functions assigned to it. Both of these reports are available upon request, and location coordinators can use them periodically to determine the appropriateness of function assignments for either users or terminals. However, when we asked ODSM and location coordinators whether they obtain and use such reports, they told us they did not know they existed. We encourage HRA to enhance its control structure by using these reports as tools in periodic reviews to verify that the assignment of user and terminal rights has been appropriate. Location coordinators who review user and terminal rights might identify some that should have been terminated but were not, some that are inconsistent with the user's job responsibilities, or others that were assigned improperly.

Although location coordinators are required to notify ODSM of personnel changes, not all coordinators comply. ODSM officials told us they try to perform a quarterly payroll match as a compensating control to identify users who may no longer need system access, but work demands occasionally prevent them from doing so. We noted that they had performed such a match twice in 2002. During this process, WMS users are compared with names in HRA's employment database. All exceptions (users not active in HRA's payroll system) are noted on an exception report that is distributed to job center directors. Such directors are responsible for verifying that the need for WMS access still exists and that the name and SSN of each exception is accurate. When we reviewed six exception logs, we found that the directors generally did not complete the logs in accordance with ODSM's instruction. For example, one directed some users to sign their names next to their user IDs

but left most of the form incomplete. Another crossed off some names and provided explanations for other names, and submitted a form with one signature that ran vertically along the side of the page. If the report is not completed properly, the individual who processes it cannot determine what action to take.

Making sure that user rights are terminated in a timely manner is critical to guaranteeing the integrity of a system and its data. We encourage ODSM to perform the payroll match on a quarterly basis, as intended, and to see that directors complete the exception reports as instructed.

Recommendations

To HRA:

10. Update the TTSS Coordinator Handbook and distribute copies of the revised version to all location coordinators.

11. Establish an accountability system for approved authorization forms that allows them to be retrieved.

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

13. 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.

14. Require directors to complete the payroll exception report properly and have ODSM perform the payroll match on a quarterly basis.

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

Recommendations (Cont'd)

To OTDA:

16. Verify that HRA implements the recommendations in this report regarding the updating of user access.

Assigning Application Functions to Users

To restrict users from performing incompatible functions or functions beyond their level of responsibility, agencies using computer resources should identify the specific user or class of users authorized to obtain direct access to each resource for which they are responsible. This process can be simplified by developing standard profiles (matrices) that describe access needs for groups of users. According to GAO, users' specific application needs should be approved by appropriate senior management and communicated in writing to individuals performing the security function. GAO further points out that failure to assign responsibility for granting application access can leave the decision-making in the hands of personnel who can not make an informed decision about a user's needs. This can lead to the assignment of overly-broad access, circumventing control objectives and providing opportunities for fraud, sabotage, and inappropriate disclosures.

TTSS limits application access by assigning WMS functions to both users and terminals. Employees are allowed to access specific WMS transactions only if the relevant TTSS function has been assigned to them and the terminal. Access control objectives should be structured in such a way that users have only the access needed to perform their duties, and employees should be prevented from performing incompatible functions. We found that coordinators use Job Functionality Matrices to help them assign functions to users. The matrices identify appropriate functions for various job titles and work units, and the system can track the function assignments through a Terminal Operators Function Report.

To determine whether assigned user functions were consistent with established job functionality matrices, we statistically sampled 50 of the 839 users at the job centers we visited (Dyckman, Melrose, Jamaica, Dekalb, and Richmond). We obtained Terminal Operator Functions Report from OTDA that

contained all the authorized functions for each terminal and user at each of the five job centers. We compared the rights granted to each user with HRA's job functionality matrices, and found several variances. We cannot conclude that these variances are errors, because the matrices are used as a guide and coordinators may assign greater rights then defined in the matrices. However, the variances do indicate that the rights assigned to these users fall outside their typical functional assignments based on their job titles and work units. Specifically, we found variances for 23 of the 50 individuals sampled. We found that more functions had been assigned to ten of the users than had been defined in the matrices; the job titles of six users were not reflected in the matrices; three users had functions that did not match their titles; and one user had been assigned fewer functions than the number defined by the matrices. These variances might represent situations in which more-expansive rights have been assigned than authorized. Since coordinators use these matrices as a guide, HRA should update them to ensure that coordinators who are responsible for functional assignments have access to complete and reliable guidance documents. These matrices should be incorporated into the TTSS Coordinator Handbook. We also noted that three job units were not reflected in the matrices.

ODSM officials told us that the job functionality matrices have not been updated, even though job titles have changed. They expressed the belief that it is OTDA's responsibility to update them. However, the State TTSS coordinator for HRA at OTDA informed us that their office did not develop the matrices, and is not responsible for their updating. But we believe that, since the State developed TTSS to give counties the latitude they need to assign functions in accordance with their individual needs, HRA should handle the updating and then distribute revised copies to the location coordinators.

We also reviewed HRA's TTSS Coordinator Handbook to determine whether it provided location coordinators with sufficient guidance on how the matrices are to be used and which TTSS functions should be segregated. We found the Handbook indicates that the functionality matrices are "currently under development," even though these matrices are outdated. It does not provide guidance on what functions should be segregated.

Recommendations

To HRA:

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

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

To OTDA:

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

Communication and Training

To enhance the overall effectiveness of a security system, GAO offers the following guidelines:

- Inform users of the importance of the information they are handling and the legal and business reasons for maintaining its integrity and confidentiality.

- Distribute documentation describing security policies, procedures, and individual responsibilities, including expected behavior.

- Require users to periodically sign a statement that acknowledges their acceptance of responsibility for security and their awareness of the consequences of security violations, and recognizes their obligation to follow all organizational policies, including the maintenance of confidentiality of passwords and physical security over their assigned areas.

- Require comprehensive security orientation training and periodic refresher programs that communicate such security guidelines to both new and existing employees.

When location coordinators assume their coordinating roles, HRA provides them with security awareness training that includes important security-related information. For example, they receive a handbook, entitled *Information Protection and You,* that introduces HRA's Information Protection Program, outlines the reader's responsibility for following established protection measures, and provides guidance in how to carry out their responsibilities. ODSM also provides location coordinators with a handout that offers suggestions on how to protect one's password. Location coordinators are encouraged to share this material and other related security information with the staff who work at their site; however, HRA has no assurance that they actually do so. We believe HRA should require ODSM to distribute the Handbook and the password guidance to each user at the time the user ID/password is authorized.

An HRA official told us that trainers discuss security awareness in an 8-week training course for new employees, even though it is not a required topic. We reviewed the course agenda HRA officials gave us, but we could not find references to security awareness in the materials. Nor could the officials provide us with the syllabus used by their instructors for the security-related portion of the course. We also noted on our visits to job centers that users seldom received information on the importance of security or data integrity. The TTSS Coordinator Handbook requires location coordinators to promote information-protection awareness among staff, and we believe HRA should verify that coordinators do so.

The Transaction Terminal Security System Manual (TTSS Manual) is a comprehensive guide designed to assist users in TTSS operations and to serve as a training aid. However, we found the TTSS Manual offers no specific guidance on implementing controls. For example, the section on user status changes is silent about the reasons for changing the status of terminated employees. While the Manual provides detailed instruction for assigning functions to users and terminals, it provides no guidance on segregating duties between critical activities, for example, application intake and benefit authorization. Similarly, while the Manual describes various reports and inquiry functions, it is silent on their use for monitoring access and does not provide guidance on security awareness procedures.

GAO recommends that employers provide security awareness training periodically to all users, educating users about possible

risks and conditioning them to be less likely to compromise sensitive information and resources. We believe HRA should incorporate security awareness into its agenda for the eight-week new-employee course. In addition, the Manual should be revised to provide guidance on the implementation of controls. OTDA officials have told us that they will work with OFT on enhancing the Manual by incorporating control objectives into the content.

Recommendations

To HRA:

20. 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.

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

22. 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.

To OTDA and OFT:

23. 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.

To OTDA:

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

CONTROLS OVER THE NETWORK

General controls comprise the structure, methods, and procedures that apply to the overall computer operation of OTDA. They include organization and management controls, security controls, and system software and hardware controls. Application controls, which are related directly to individual computerized applications, help ensure that transactions are valid, properly-authorized, processed, and reported completely and accurately.

As the central registry for all welfare case client data in the State, WMS maintained information about more than 656,000 recipients as of January 2002. In this individual-oriented environment, the issues of security and privacy assume particular importance. Public Law 93-579, also referred to as the Federal Privacy Act of 1974, states that "...the right to privacy is a personal and fundamental right protected by the constitution of the United States..." As such, the State has an obligation to protect the personal information stored in WMS, and to maintain adequate control of access to that data.

Disaster Recovery

Losing the capacity to process, retrieve, and protect information maintained electronically can have a significant effect on HRA's ability to accomplish its mission. For this reason, an agency should establish procedures for protecting information resources and for minimizing the risk of unplanned interruptions, as well as a plan for recovering critical operations should interruptions occur. These plans should consider the activities performed at general support facilities, such as data processing centers and telecommunications facilities, as well as those activities performed by users of specific applications.

Generally called a Disaster Recovery Plan (Plan), these controls should secure service continuity by addressing the entire range of potential disruptions. These may include relatively-minor interruptions, such as temporary power failures, as well as major disasters such as fires or natural disasters that would

require re-establishing operations at a remote location. They may also include errors, such as writing over a file; if controls are inadequate, even minor interruptions can result in lost or incorrectly-processed data, expensive recovery efforts, and inaccurate or incomplete information.

OTDA has entered into a service-level agreement with OFT, effective on October 26, 2000, to share computer resources residing at the New York State Data Center (Center). This five-year agreement requires OFT to develop a plan for securing the Center's ability to provide back up computer processing. In this regard, OFT must maintain a Disaster Recovery Site (DR Site) in a prescribed offsite location where all Center workflow can be processed for an extended period. OFT must test and update the Plan at prescribed time intervals to assure management of its viability.

The Plan should clearly identify the order in which processing will be restored, the individuals who will be responsible, and the supporting equipment or other resources that will be needed. A remote backup operations facility should also be identified and prepared for use in the event that the one normally used is rendered inoperable despite the installation of environmental controls such as fire-suppression systems or backup power supplies. Alternative facilities can range from an equipped site ready for immediate backup service, referred to as a "hot site," to one that is not equipped and will take some time to prepare, referred to as a "cold site." Any such DR Site should be located far enough away that it is not likely to be subject to impairment from the same event.

We found that OFT had drafted an interim disaster recovery plan on December 11, 2002, but when we reviewed it, we found that it lacked significant provisions. For example, the plan does not identify system criticality and restoration priorities, individual roles and responsibilities and time-related tasks, procedures for actually testing the adequacy of the plan, and the entire process OFT would follow to make the DR Site operational after a disaster or mishap.

In the event of an outage, loss of system data, or disaster, the interim plan also requires Data Center staff to follow recovery procedures that have been prescribed by the individual customer agency for restoring processing. However, OTDA has not provided recovery procedures for WMS; nor has it provided

an applications-processing schedule for disaster recovery or a strategy for printing under disaster conditions.

OTDA officials told us that their Division of Information Technology has developed business continuity and recovery strategies for critical mainframe systems. They also since told us they have identified issues that will need to be incorporated into the agency's Business Continuity Plan, pointing out that OTDA has entered into a contract to undertake a Disaster Recovery and Business Continuity Study. It is expected that the study will help officials assess disaster recovery needs for selected critical systems/applications in such areas as recoverability, mitigation steps to reduce exposure, business impact, and current enterprise disaster recovery readiness.

Recommendations

To OFT:

25. 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 Site operational after a disaster.

To OTDA:

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

27. Develop recovery procedures for WMS and deliver them to OFT.

28. Verify that OFT implements the Disaster Recover Plan recommendation made in this report.

Physical Access

Physical security controls restrict physical access to computer resources and protect them from intentional or unintentional loss or impairment. Computer resources to be protected include primary computer facilities; cooling system facilities; terminals used to access a computer; micro computers; computer file

storage areas; and telecommunications equipment and lines, including wiring closets.

Access to a data center and its resources should be limited to personnel who have a legitimate need for access so they can perform their duties. Management should regularly review and approve a list of persons authorized to have physical access to sensitive facilities. On occasion, access to sensitive areas or facilities may be granted to persons other than regularly-authorized personnel, such as employees from another facility, maintenance personnel, contractors, and the infrequent or unexpected visitor. All of these visitors should be controlled and not granted unrestricted access. Controls should include preplanned appointments, identification checks, control of the reception area, and procedures for logging in and escorting visitors.

HRA limits and monitors access to its data center. It also requires visitors to show proper identification, sign a visitor's logbook, and wear a visitor pass. In addition, management has authorized selected staff to escort visitors. However, HRA has not developed a written access policy that identifies the individuals authorized to grant access, and those who may receive access. Nor has it developed written procedures for issuing or obtaining access to the Data Center, such as an identification badge.

HRA also does not require the periodic review of access lists to verify that access privileges granted to individuals remain appropriate. Although the data center's existing computerized access system has been operating for only a year, and management reviewed individual access rights when the system was developed, HRA should ensure that the list remains current by developing a formal policy that requires periodic reviews.

When we visited the Brooklyn, DeKalb, Jamaica, Melrose, and Richmond job centers, we checked the security of each job center's telecommunication closet that contains WMS communication lines. We found that not all of these closets had been secured properly.

Staff at the job centers understood the need to secure WMS telecommunication equipment, but HRA has not developed procedures for addressing physical security at those sites. We believe that HRA should develop and convey such procedures,

emphasizing its policy that all job centers are to safeguard WMS equipment.

Recommendations

To HRA:

29. 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.

30. 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.

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

32. 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.

To OTDA:

33. 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.

PROGRAM CHANGES

Strong controls for authorizing, developing, testing, and implementing WMS program changes will provide HRA with greater assurance of the integrity of WMS and the data it contains. This can be accomplished through the institution of policies, procedures, and techniques that require: the authorization and approval of management, adequately testing changes and monitoring changes to ensure compliance. Without proper controls, there is a risk that an individual could inadvertently or deliberately omit or "turn off" security features or even introduce processing irregularities or malicious codes.

Program Change Procedures

Authorization is the first step in implementing system changes. The process for obtaining, documenting, and communicating authorization should be defined in a system development life cycle (SDLC) that details the procedures staff are to follow when applications are being designed and developed, as well as when they are subsequently modified. The SDLC should provide a structured approach for identifying and documenting needed changes to computerized operations and for designing, developing, testing, and approving system modifications. If staff are to apply the methodology properly, management should document it well enough that it provides clear and consistent guidance. The use of standardized change request forms helps ensure that requests are communicated clearly and that approvals are documented.

A disciplined process for testing and approving new and modified programs before their implementation is essential to reassure management that programs will operate as intended and that no unauthorized changes will be introduced. The extent of testing varies, depending on the type of modification. For major system enhancements, testing should be extensive, generally progressing through a series of test stages that include the testing of individual program modules (unit testing), of groups of modules that must work together (integration testing), and of an entire system (system testing). Minor modifications may require less-extensive testing; however,

management should carefully control and approve changes, since minor program code changes, if done incorrectly, can have a significant impact on overall data integrity.

We found that OTDA has not updated its SDLC in more then 15 years, and that it does not reflect OTDA's current system change methodologies. OTDA now uses a Workload Management (WLM) process for identifying, scheduling, and implementing program area requests from all human services agencies. All change requests must be submitted through the WLM process by persons OTDA has authorized. The testing process is a joint effort accomplished in several steps by user developers and program area staff, and successful user acceptance testing is required before OTDA releases a program change. The WLM does not include the components of a SDLC. For example, its requirements for the development of detailed test plans for each modification do not define the levels and types of test to be performed. Nor do they define the responsibilities of each person involved in testing and approving software; or require the development of related changes to system documentation, including hardware documentation, operating procedures and user procedures, supervisory review, or documented approvals by appropriate personnel.

We selected one program change for review, and sought to determine whether its test plan and test plan results had been documented adequately. When we obtained and reviewed the user test plan and test results, we found that the individual(s) responsible for conducting the test had not fully documented the test results. In fact, we found that matching the user test plan to the test plan results was extremely difficult and time-consuming. For the sampled program change, the 17-page test plan had approximately 150 documented test page results. However, the user test plan was not marked to indicate that the tester had completed each test or that the program had achieved the appropriate test results. The only document that summarizes the test results indicates that the software version is working according to specification, and that the pilot sites may begin to use the modified program. We believe management should review and approve these test plans, and that testers should be required to document their test results thoroughly. OTDA should update its SDLC, which should clearly convey the requirements for conducting and documenting test plans.

During the audit, we found a "glitch" that could be attributed to incomplete system testing. We found that, when a client has a sanction for noncompliance with the City's Office of Child Support Enforcement policies, they impose a 25-percent grant reduction; when this happens the system's console display does not accurately display an individual's "other" grant line item. Even though the system displays an incorrect "other" grant amount, the actual grant paid to the client is correct. It is possible that defined testing standards in OTDA's SDLC might have enabled programmers and/or system testers to find the glitch during their tests. We shared our finding with OTDA officials, who indicated that they were taking steps to correct this system error.

WMS documentation is also outdated. For example, OTDA designed the WMS System Reference Manual for staff to use as a WMS reference tool. We reviewed the Manual, which describes the system as designed for use by the New York City HRA, and found that OTDA had not revised it since March 1997. Because the Manual is intended to serve as a reference tool for staff, OTDA should ensure that it is updated on an ongoing basis, with each programming change.

An organization should also segregate work responsibilities so that one individual can not control all critical stages of a process. For example, an individual should not be authorized to write, test, and approve program changes. Dividing duties among two or more individuals or groups diminishes the likelihood that errors and wrongful acts will go undetected; the activities of one group or individual will serve as a check on the activities of the other. Inadequately-segregated duties increase the risk that erroneous or fraudulent transactions can be processed, that improper program changes can be implemented, and that computer resources can be damaged or destroyed.

The extent to which duties are segregated depends on the size of the organization and the risk associated with its facilities and activities. A large organization will have more flexibility in separating key duties than a small organization that must depend on a few individuals to perform its operations. Smaller organizations may rely more extensively on supervisory review to control activities.

We selected a WMS program change for review and sought to determine whether the change had been authorized, documented, tested, and implemented properly. When we reviewed the documentation that supported the program change, we found that the individual responsible for developing the change specifications had also developed the test plan, tested the program changes, and authorized the program changes to be rolled out to pilot sites. OTDA officials stated that when the WLM process is used, job duties are segregated (performed by requestors, developers, and testers). However, we found that a requester had also tested the changes we reviewed, and had authorized the rollout as well.

To protect approved software programs from unauthorized changes or impairment and prevent different versions from being misidentified, organizations must maintain carefully-controlled libraries. Inadequately-controlled software libraries increase the risk that unauthorized changes could be made either inadvertently or deliberately for fraudulent or malicious purposes. Access to software libraries should be protected by the use of access control software or operating system features and physical access controls. The OFT operates the State's Data Center, as well as OTDA's software libraries, maintaining logs for identifying the deposit and distribution of tapes and cartridges to and from the library. During our audit, we found a weakness in the controls over the tape libraries and reported it to management. The details of this weakness and related recommendations have not been included in this report.

Recommendations

To OTDA:

34. Update the SDLC 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.

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

Recommendations (Cont'd)

36. Update the WMS System Reference Manual as the system is modified.

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

MAJOR CONTRIBUTORS TO THIS REPORT

William Challice

Richard Sturm

Donald Geary

Nadine Morrell

Randy Partridge

Carole LeMieux

Hector Mercedes

Marticia Madory

Appendix A

George E. Pataki
Governor

NEW YORK STATE
OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE
40 NORTH PEARL STREET
ALBANY, NEW YORK 12243-0001
(518) 474-4152
(518) 486-6255 - Fax

Brian J. Wing
Commissioner

August 6, 2003

Re: Draft Audit Report: Welfare Management System: New York City General and Application Controls – 2002-N-1

Dear Mr. Challice:

The following is the New York State Office of Temporary and Disability Assistance (OTDA) response, written in conjunction with the Office for Technology, to the Office of State Comptroller (OSC) recommendations offered in the draft report entitled "New York State Office of Temporary and Disability Assistance, New York State Office for Technology, New York City Human Resources Administration, Welfare Management System: New York City General and Application Controls."

Our specific responses to individual findings and recommendations are as follows:

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

   Response: HRA will respond to this item separately.

2. **Recommendation:** ***Require job centers to make sure that scanned source documents are legible.***

   Response: HRA will respond to this item separately.

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

   Response: OTDA will obtain a list of the cases where errors were identified and verify that HRA has made the corrections.

4. **Recommendation:** ***Verify that HRA implements the data integrity recommendation in this report.***

   Response: OTDA will continue to monitor the accuracy of system data in various ways.

5. **Recommendation:** ***Implement the password security recommendations made during the course of our audit.***

   Response: These recommendations will be considered during the WMS redesign.

6. **Recommendation:** ***Use the Termination 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).***

   Response: HRA will respond to this item separately.

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

Response: OFT will continue to monitor the process for distributing reports to HRA and work with OTDA to resolve any problems HRA may communicate along these lines. To this point, the problem cited in the audit appears to have been a single occurrence.

8. **Recommendation:** ***Meet with HRA officials and explain the important uses of the report.***

Response: OFT will include HRA in any correspondence and/or training materials developed regarding proper use of TTSS reports.

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

Response: OTDA will consider self-assessment for completion by the HRA Security Coordinator(s). Where there appear to be inadequate or incomplete responses, OTDA's Information Security Officer (ISO) can request auditors to do an on-site review as priorities permit.

10. **Recommendation:** ***Update the TTSS Coordinator Handbook and distribute copies of the revised version to all location coordinators.***

Response: HRA will respond to this item separately.

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

Response: HRA will respond to this item separately.

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

Response: HRA will respond to this item separately.

13. **Recommendation:** ***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.***

Response: HRA will respond to this item separately.

14. **Recommendation:** ***Require directors to complete the payroll exception report properly and have ODSM perform the payroll match on a quarterly basis.***

Response: HRA will respond to this item separately.

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

Response: HRA will respond to this item separately.

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

Response: While OTDA agrees that HRA should establish clear procedures, it is our opinion that we do not have the legislative authority to control or require such procedures. OTDA and OFT will continue as they have in the past, to provide guidance.

* ***Note 2***

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

Response: HRA will respond to this item separately.

18. **Recommendation:** ***Include in the updated TTSS Coordinator Handbook how location coordinators should use the job functionality matrices and indicates which TTSS functions should be segregated.***

Response: HRA will respond to this item separately.

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

Response: See response to recommendation #16.

* Note 2

20. **Recommendation:** ***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.***

Response: HRA will respond to this item separately.

21. **Recommendation:** ***Verify that location coordinators are promoting information security awareness among staff.***

Response: HRA will respond to this item separately.

22. **Recommendation:** ***Incorporation 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.***

Response: HRA will respond to this item separately.

23. **Recommendation:** ***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.***

Response: This guidance has been provided in the past. OTDA and OFT will assess the need to update the information and consider this along with other priorities.

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

Response: OTDA has provided recent materials and guidance on information security awareness. Since HRA is responsible for security in their operations, OTDA concludes that assuming a more prescriptive posture would exceed the agency's legislative authority.

* Note 2

25. **Recommendation:** ***Finalize the Data Center Disaster Recovery Plan and ensure that it provides for system critically 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 Site operational after a disaster.***

Response: An extract of the OTDA Business Continuity Plan was provided to substantiate the fact that a data center/mainframe disaster recovery plan exists. OTDA and OFT are working together to determine final requirements.

26. **Recommendation:** ***Provide OFT with a disaster application-processing schedule and printing strategies.***

Response: A priority disaster application list has been provided to OFT Data Center staff. OTDA will discuss printing strategies with OFT.

27. **Recommendation:** ***Develop recovery procedures for WMS and deliver them to OFT.***

Response: Recovery procedures for WMS have been in place and successfully accomplished for years, as needed.

* Note 3

28. **Recommendation:** ***Verify that OFT implements the Disaster Recovery Plan recommendation made in this report.***

Response: OTDA will continue to work with OFT on finalizing and implementing the Disaster Recovery Plan.

29. **Recommendation:** ***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.***

Response: HRA will respond to this item separately.

30. **Recommendation:** ***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.***

Response: HRA will respond to this item separately.

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

Response: HRA will respond to this item separately.

32. **Recommendation:** ***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.***

Response: HRA will respond to this item separately.

33. **Recommendation:** ***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.***

Response: See response to recommendation #16 and #24.

* Note 2

34. **Recommendation:** ***Update the SDLC 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.***

Response: Presently, OTDA is using the Workload Management (WLM) process to identify, schedule and implement program area requests from all Human Services agencies (OTDA/DOH/OCFS). The only avenue to submit requests is through the WLM process from authorized individuals and they are therefore approved. Testing is a joint effort accomplished in several steps that includes user developers and program area staffs. Program migration requires successful user acceptance testing.

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

Response: OCSE/CSMS Management has already initiated corrective action related to this recommendation.

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

Response: OTDA maintains a number of user manuals other than the WMS System Reference Manual which are updated regularly with each new software change and do provide information concerning WMS system requirements. Page replacements are sent to HRA for each new version of software.

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

Response: Individuals and organizations within OTDA do have segregated job duties when using the WLM process: requestors, developers and testers.

Thank you for sharing the report with us and we trust that our comments will be considered and the appropriate changes made to the report prior to its final release.

Sincerely,

Brian J. Wing

Mr. William P. Challice
NYS Office of the State Comptroller
Division State Services
State Audit Bureau
123 William Street – 21st Floor
New York, New York 10038

W-2-184A
Rev. 6/03

HUMAN RESOURCES ADMINISTRATION
OFFICE OF AUDIT SERVICES
180 WATER STREET
NEW YORK, NEW YORK 10038
(212) 331-3978 Fax: (212) 331-5474
E-mail: lehmand@hra.nyc.gov

VERNA EGGLESTON
Administrator/Commissioner

DAN LEHMAN
Executive Deputy Commissioner

August 1, 2003

Mr. William Challice
Audit Director
Office of the State Comptroller
Division State Services
State Audit Bureau
123 William Street – 21st Floor
New York, New York 10038

Re: Welfare Management System: New York City General and Applications Controls 2002-N-1

Dear Mr. Challice:

Thank you for the opportunity to respond to the draft report on the above referenced audit. The report has assisted us in our ongoing efforts to improve the operations of our Agency.

Following are our specific responses to the audit findings and recommendations:

DATA INTEGRITY

Data Element Testing

Auditors' Finding:
HRA management has not developed written procedures that instruct supervisors about what they should do when they conduct these reviews (i.e., compare system data with source documentation).

Agency's Response:
We agree with the finding and have developed, as of April 24, 2003, Policy Directive #03-63 SYS Case Record Consistency with Welfare Management System (WMS), to instruct supervisors on what they should do when they conduct reviews.

Auditors' Finding:
HRA should develop procedures that explain a supervisor's role and responsibilities during supervisory reviews.

Agency's Response:
We agree with the finding and have developed, as of April 24, 2003, Policy Directive #03-63 SYS Case Record Consistency with WMS, which explains the supervisor's role and responsibilities during supervisory reviews.

Auditors' Finding:
Although we sampled 58 cases, the actual number of data elements we tested varied, depending on the number of individuals in each case. In total, our sample included 733 data elements. However, because 94 (or 13 percent) of these elements lacked required supporting documentation, we could not test them. As a result, we tested 639 of the original 733 data elements and found 39 errors. We also noted 23 instances in which the Social Security Administration had validated the individual's Social Security Number (SSN) even though there was a variance between the WMS data and the individual's source documents.

Agency's Response:
We agree with the finding and, as of April 30, 2003, have developed Policy Directive #03-24-ELI, Necessity of Accurate Social Security Numbers in WMS. In addition, we have corrected the errors in the cases disclosed in the report.

Auditors' Finding:
For 44 of the cases where we had sufficient budget-related supporting documentation, we found eight instances in which data entry errors had affected the public assistance grant. Seven of the eight budgeting errors were understatements of the client's grant; the remaining one had resulted in an overstatement.

Agency's Response:
We agree with this finding and have developed Policy Directive #03-63 SYS, Case Record Consistency with WMS to provide guidance in this area. In addition, we have taken steps to correct the errors in the case records noted in the report.

Auditors' Recommendation #1:
HRA should develop written supervisory case review procedures that explain a supervisor's role and responsibilities. Include matching selected data with appropriate source documentation.

Agency's Response:
We agree with this recommendation, and, as of April 24, 2003, have developed Policy Directive #03-63 SYS, Case Record Consistency with WMS, which defines the supervisor's role and responsibilities.

Auditors' Recommendation #2
Require job centers to make sure that scanned source documents are legible.

Agency's Response:
We agree with this recommendation and have developed Policy Directive #03-63 SYS dated April 24, 2003, entitled Case Record Consistency with WMS, which requires that scanned source documents be legible.

Auditors' Recommendation #3:
Enforce the requirement that job centers obtain supporting documentation and verify that they have corrected the errors and variances we noted during our audit.

Agency's Response:
We agree with this recommendation and have developed as of April 24, 2003, Policy Directive #03-63 SYS, entitled Case Record Consistency with WMS, which requires that job centers obtain supporting documentation. In addition, we will institute a review to ensure that the errors identified in this report have been corrected.

COMPUTER SECURITY

Password Security

Auditors' Finding:
Office of Data Security Management (ODSM) and location coordinators are not using available security reports to monitor Welfare Management System (WMS) access and usage in the job centers.

Agency's Response:
We agree with this finding and will take steps to correct the deficiency. ODSM will develop procedures on how to use these reports to increase security. These procedures will be used throughout the agency, including in the Job Centers, to monitor WMS access and usage. We anticipate that this procedure will be completed and implemented by December 31, 2003.

Auditors' Findings:
TTSS coordinators do not always notify ODSM of personnel changes.

Agency's Response:
We agree with this finding. It should be noted that as part of coordinator training site managers are routinely instructed to inform ODSM of changes to personnel. However, in future training sessions, we will reinforce the importance of and need for this action.

Auditors' Finding:
Location coordinators are not monitoring compliance with access policy by comparing authorization requirements with the actual access granted, and that there are opportunities for location coordinators to foster greater security awareness among system users.

Agency's Response:
We agree with this finding. FIA will incorporate the new ODSM procedure into the monthly Train-the–Trainer sessions. The trainers will in turn relate this information to all staff in our routine training sessions. We anticipate implementing this new procedure by December 2003.

MONITORING SECURITY VIOLATIONS

Auditors' Finding:
The Terminal Security Violations Report (Report) for week ending July 6, 2002, contained numerous violations at each job center, the most common being terminal timeouts.

Agency's Response:
We partially agree with this finding. Most *Security Violations* reported are Terminal Timeouts. This timeout function has been discussed as a security feature, not a violation. In the normal course of business, workers may do extensive off-line work in conjunction with on-line activity, so that a reasonable timeout time must be a compromise between security concerns and operational hindrance. Such a compromise might be an increase in WMS session timeouts paired with a shortened windows host screen locking feature that would prevent any but the logged on operator to resume an active WMS session. Users will be encouraged to log off at any time that a terminal session is unattended.

Auditors' Recommendation #4:
HRA should use the Terminal Security Violations Report 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).

Agency's Response:
We agree with this recommendation. However, we believe that the terminal timeout report noted above should be moved to a separate report for management review in terms of individual worker time management. ODSM will contact program management staff for selected reviews where warranted by excessive terminal timeouts and will review (as appropriate and resources permit) other areas of potential violations.

UPDATING USER ACCESS

Auditors' Finding:
TTSS Coordinator Handbook is outdated and was last revised in March 1988. The handbook does not reflect the forms currently used by location coordinators; it is missing definitions for more than 40 percent of the WMS functions the location coordinator must assign; and it contains numerous incorrect addresses, phone numbers, and items of personnel information.

Agency's Response:
We agree with this finding. The TTSS Coordinator Handbook will be reviewed and updated to include training material and forms definitions by March 2004.

Auditors' Finding:
Location coordinators do not retain copy of the original forms; nor does ODSM return copies to them. In addition, location coordinators do not review user access/terminal rights to determine whether ODSM has assigned them as authorized.

Agency's Response:
We partially agree with this finding. Location Coordinators do retain a copy of the WMS Access/Update TTSS-24, Form M499 before mailing to ODSM. While ODSM does not return the original form to the coordinators, they do return the password information based on the original request, by means of Form M499f, Verification of UserID/Password Distribution. The Location Coordinator and the employee, for whom the ID was secured, sign the M499f to verify receipt of the password and UserID. This form is then returned to ODSM.

Auditors' Finding:
Location coordinators do not use authorized functions report.

Agency's Response:
We agree with this finding. Currently, ODSM distributes the results of the quarterly match to program area staff, who verifies the presence and need for staff to have the accounts provided. In addition to the verification of staff assigned to these sites, beginning in August 30, 2003 program management will be asked to verify that the staff continue to need the functions as requested and assigned.

Auditors; Finding:
Job Center Directors generally do not complete the exception logs in accordance with ODSM's instruction. For example, one directed some users to sign their names next to their user IDs but left most of the form incomplete. Another crossed off some names and provided explanations for other names, and submitted a form with one signature that ran vertically along the side of the page.

Agency's Response:
We agree with this finding. It should be noted that ODSM returns to the center all forms that are not properly completed. In addition, ODSM incorporates electronic communication via e-mail and the Automated Paperless Access Request Transmission System (APART) to relay this information.

Auditors' Recommendation #5:
Update the TTSS Coordinator Handbook and distribute copies of the revised version to all location coordinators.

Agency's Response:
We agree with this recommendation. The TTSS Coordinator Handbook will be reviewed and updated to include training material and forms definitions by March 2004.

Auditors' Recommendation #6:
Establish an accountability system for approved authorization forms that allows them to be retrieved.

Agency's Response:
We agree with this recommendation and in April 2003, ODSM developed a new spreadsheet database, which allows retrieval by request date.

Auditors' Recommendation #7:
Require location coordinators to verify the appropriateness of user/terminal rights by comparing assigned functions with authorizations before distributing users IDs/passwords.

Agency's Response:
We agree with this recommendation and location coordinators will be advised immediately to review the assigned functionality by either comparing it with the original retained forms or by the performance of a desk audit.

Auditors' Recommendation #8:
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.

Agency's Response:
We agree with this recommendation. Proper access is determined by program management based on the need to perform specific tasks. Available staff resources often require management to assign tasks outside of the "matrix" to staff for the continuation of effort. ODSM will update access rights based on program management needs and in accordance with applicable oversight policy. The need for program management to advise ODSM of changes in job specifications will be reinforced.

Auditors' Recommendations #9:
Require directors to complete the payroll exception report properly and have ODSM perform the payroll match on a quarterly basis.

Agency's Response:
We partially agree with this recommendation. We will require all directors to complete the payroll exception report properly. However, it should be noted that ODSM does perform the payroll match currently, on a quarterly basis and submits the reports to program directors for review.

* Note 1

Auditors' Recommendation #10:
Verify that location coordinators are following policy that requires them to provide ODSM with timely notification of all personnel changes.

Agency's Response:
We agree with this recommendation and we will immediately reinforce the need for program management to advise ODSM of changes in job specifications.

ASSIGNING APPLICATION FUNCTIONS TO USERS

Auditors' Finding:
To determine whether assigned user functions were consistent with established job functionality matrices, we statistically sampled 50 of the 839 users at the job centers we visited (Dyckman, Melrose, Jamaica, Dekalb and Richmond). We obtained Terminal Operator Functions Report from OTDA that contained all the authorized functions for each terminal and user at each of the five job centers. We compared the rights granted to

* See State Comptroller's Notes, Appendix C

each user with HRA's job functionality matrices, and found several variances. We found variances for 23 of the 50 individuals sampled. We found that more functions had been assigned to ten of the users than had been defined in the matrices; the job titles of six users were not reflected in the matrices; three users had functions that did not match their titles; and one user had been assigned fewer functions than the number defined by the matrices.

Agency's Response:
We agree with this finding. Proper access is determined by program management based on the need to perform specific tasks. The available staff resources often require management to assign tasks outside of the "matrix" to staff for the continuation of effort. ODSM will update access rights based on program management requests and needs and in accordance with applicable oversight policy. ODSM has requested an updated functionality report from the program areas.

Auditors' Finding:
The HRA TTSS Coordinator Handbook indicates that the functionality matrices are "currently under development," even though these matrices are outdated. It does not provide guidance on what functions should be segregated.

Agency's Response:
We agree with this finding. An updated functionality matrix is now incorporated in an on-line system called APART (Automated Paperless Access Request Transmission). Interim hard copy documentation will be printed and distributed along with the updated TTSS Coordinator Handbook due for completion March 30, 2004.

Auditors' Recommendation #11:
Update the job functionality matrices and incorporate them into the appropriate section of the TTSS Coordinator Handbook.

Agency's Response:
We agree with this recommendation. ODSM has requested an updated functionality report from the program areas and will incorporate these functions into an updated matrix. These changes will be incorporated into the revised TTSS Coordinator Handbook scheduled for completion by March 30, 2004.

Auditors Recommendation #12:
Include in the updated TTSS Coordinator Handbook how location coordinators should use the job functionality matrices and indicate which TTSS functions should be segregated.

Agency's Response:
We agree with this recommendation. Please note that functionality matrices are provided as a baseline. Functions that enable a single individual to perform an action including initiation and authorization are segregated. This information will be included in the revised TTSS Handbook due for completion by March 30, 2004.

COMMUNICATION AND TRAINING

Auditors' Finding:
An HRA official told us that trainers discuss security awareness in an 8-week training course for new employees, even though it is not a required topic. We reviewed the course agenda HRA officials gave us, but we could not find references to security awareness in the materials. Nor could the official provide us with the syllabus used by their instructors for the security-related portion of the course. We also noted on our visit to job centers that users seldom received information on the importance of security or data integrity.

Agency's Response:
We agree with this finding. However, it should be noted that security awareness training is conducted as part of location coordinator training through a "Train-the-Trainer" approach. ODSM provides a booklet as an adjunct to this training. More formal training in security awareness is currently under development with interactive CBT and classroom instruction planned.

We are currently evaluating several different methods of training delivery from a number of vendor offerings as well as in-house developed products. In addition, we are in discussions to have this product made available on a citywide basis for all employees. Once we have decided on the option that will best serve the agency, we will proceed with the roll-out, which we anticipate will be in April 2004.

Auditors' Finding:
The TTSS Manual offers no specific guidance on implementing controls. For example, the section on user status changes is silent about the reasons for changing the status of terminated employees. It provides no guidance on segregating duties between critical activities, for example, application intake and benefit authorization. Similarly, while the Manual describes various reports and inquiry functions, it is silent on their use for monitoring access and does not provide guidance on security awareness procedures.

Agency's Response:
We agree with this finding. This information will be included in the revised TTSS Handbook due for completion by March 30, 2004.

Auditors' Recommendation #13:
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.

Agency's Response:
We agree with this recommendation. Coordinators are instructed to distribute this handbook. This practice will be reinforced.

Auditors' Recommendations #14
Verify that location coordinators are promoting information security awareness among staff.

Agency's Response:
We agree with this recommendation. ODSM will make a policy recommendation that each site performs and documents this function on a quarterly basis when they carry out the match activities described above.

Auditors' Recommendation #15:
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.

Agency's Response:
We agree with this recommendation. Once it is completed, FIA will incorporate the training instrument discussed above that ODSM is developing into the eight-week on-going new hires training program.

CONTROLS OVER THE NETWORK

Physical Access

Auditors' Finding:
HRA has not developed a written access policy that identifies the individuals authorized to grant access, and those who may receive access. Nor has it developed written procedures for issuing or obtaining access to the Data Center, such as an identification badge.

Agency's Response:
We agree with this finding. MIS Facilities personnel will develop a procedure for issuing identification badges and obtaining access to the Data Center. Please note that a phased move for MIS to Brooklyn has been planned. The first phase will be conducted in November 2003, and the last in February 2004. We anticipate that the written procedures will be completed by March 2004.

Auditors' Finding:
HRA also does not require the periodic review of access lists to verify that access privileges granted to individuals remain appropriate.

Agency's Response:
We disagree with this finding. The Deputy Commissioner of MIS periodically reviews the access list to ensure that it is updated. In addition, once ODSM is notified of staff status changes, that office modifies physical and logical access privileges to match the new situation.

* *Note 5*

Auditors' Finding:
When we visited the Brooklyn, DeKalb, Jamaica, Melrose and Richmond job centers, we checked the security of each job center's telecommunication closet that contains WMS communication lines; we found that not all of these closets had been secured properly.

* See State Comptroller's Notes, Appendix C

Agency's Response:
We agree with this finding. However, it should be noted that an inspection of the rooms in which the equipment is maintained by the MIS Office of Enterprise Networking (OEN) has revealed that they all have locking doors. We will stress to the sites, the importance of keeping them locked when not in use by authorized personnel.

Auditors' Finding:
HRA has not developed procedures for addressing physical security at those sites.

Agency's Response:
We disagree with this finding. The Office of Security Services (OSS), which is part of the Agency's General Support Services (GSS), has security procedures that are used by OSS personnel and contract guards who provide direct security services at our locations. These procedures are indicated in the "Security Guard Manual" (for contract guards) and the respective manuals for Senior Special Officers (in-house Sergeants who manage security at many locations) and Principal Special Officers (in-house Captains who oversee the Sergeants). The manuals cover various subjects relating to safeguarding of Agency premises, such as daily coverage of assigned security posts, controlling access to and within our premises, on-site patrols, maintenance of security logbooks and incident reports, timely response to security incidents, timely reporting of dangerous conditions/unusual situations, etc. Copies of these manuals are attached.

OSS also has security procedures that provide guidelines for the staff in general. One of these procedures, which is called "Theft of Agency or Personal Property or Illegal Entry into Agency Locations" (Procedure No. 96-6, dated June 10, 1996), covers all Agency locations and all Agency property. Aside from having been distributed previously in hard copy form on an Agency-wide basis (in 1996), this procedure is available for our personnel to access on-line on the Agency web site. It is now being updated by GSS, and it is anticipated that the updated policy will be issued in August 2003.

* *Note 4*

Other procedures currently in place (which were also distributed throughout the Agency previously) cover such topics as security incident reporting and emergency evacuation. In February 2003, the OSS field staff organization was expanded considerably, when the 45 Captains and Sergeants – who have peace officer status and the power to make arrests - were added to increase monitoring of contract guard personnel. As a result, the current procedures are under review, and it is expected that some updates will be required.

In addition to security procedures involving OSS personnel, Custodial Services area staff – who are part of the GSS Office of Facilities Operations (OFO) – perform certain daily activities that are security-related and designed to safeguard Agency premises/property. For example, as part of the standard procedure for opening and closing buildings (see attached protocol), building custodians are responsible for setting burglar alarms and locking up at night.

It should also be noted that in July 2003, the locks on computer rooms were changed, and only MIS and the center directors have the keys. As a long-term measure, a card access system tied to the servers and motion detectors will be installed at every computer room. The card access system will require authorized personnel to swipe an electronic locking device which will recognize authorized personnel and record those individuals on the server, thus providing a

* See State Comptroller's Notes, Appendix C

permanent record of all those gaining entry. The motion sensors will be tied to a keypad that would disarm the sensor. If an unauthorized person entered the space (and didn't know the code to disarm the sensor), then our central monitoring service would be notified, and security personnel would be dispatched to investigate. Given funding approval for this equipment, it would be in place by the last quarter of Calendar Year 2003. Furthermore, GSS will ensure monitoring of closed circuit television cameras, which are to be installed on the doors to computer rooms. We expect to begin work on these new measures immediately.

Auditors' Recommendation #16:
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.

Agency's Response:
We agree with this recommendation, and such procedures are being developed by the Office of Facilities Management, in conjunction with ODSM and OEN. We anticipate that they will be completed by April 30, 2004.

Auditors' Recommendation #17:
List in writing the procedures to be followed when issuing or obtaining identification badge that grants regular access to the New York City data center.

Agency's Response:
We agree with this recommendation, and, as stated above in our response to Recommendation #16, we are currently developing procedures for access to the Data Center. These procedures will be completed by April 30, 2004.

Auditors' Recommendation #18:
Require, at least annually, the review of the data centers' access lists to verify that access privileges granted to individuals are current and appropriate.

* Note 5

Agency's Response:
We agree with this recommendation, and will conduct such reviews annually.

Auditors' Recommendation #19:
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.

* Note 4

Agency's Response:
We disagree with this recommendation. As stated above, the Agency has extensive security procedures that have been in effect for some time. In addition, as of July 2003, we have changed the locks on computer rooms at the centers, so that only MIS and the center directors can access them.

The Agency appreciates the efforts and cooperation of the auditors and we trust that our comments presented in this response will be reflected in the final report. Should you require any

* See State Comptroller's Notes, Appendix C

additional information on this matter, please contact Hope Henderson, Director of the Bureau of Audit Coordination, at (212) 331-3522.

Sincerely,

Dan Lehman

c: Commissioner Verna Eggleston
Richard O'Halloran

State Comptroller's Notes

1. As stated on page 18 of our report, we found that the payroll matches were not performed on a quarterly basis, and ODSM officials acknowledged that, on occasion, work demands prevented them from performing the quarterly matches.

2. OTDA is responsible for monitoring and supervising the districts' administration of WMS; and as part of its oversight function, OTDA is also responsible for guarding the confidentiality of the data collected. While we believe that, as part of this responsibility, OTDA should monitor that local districts have implemented adequate controls to safeguard WMS and the data maintained on this system, at a minimum, OTDA could, in an advisory manner, provide guidance to local districts in this regard.

3. During the audit, OFT officials acknowledged that they were not provided with recovery procedures for WMS. We therefore encourage OTDA to provide them to OFT.

4. We acknowledge that HRA's Office of Security Services has developed a series of security procedures. However, these procedures do not address physical security of WMS equipment. Such procedures should address how to protect computer-related resources, such as the primary computer and cooling system facilities, microcomputers, terminals, computer file storage devices, and telecommunications equipment and lines.

5. While HRA officials disagreed with this finding, they, nevertheless, agreed to review access annually. (See Auditor Recommendation 18, page 11 of HRA's response.)