

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

**Alan G. Hevesi
COMPTROLLER**



***OFFICE OF TEMPORARY AND DISABILITY
ASSISTANCE***

***WELFARE MANAGEMENT SYSTEM
GENERAL AND APPLICATION CONTROLS***

2001-S-35

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 2001-S-35

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

Dear Mr. Wing:

The following is our report concerning the general and application controls of the State's Welfare Management System.

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

Office of the State Comptroller
Division of State Services

March 14, 2003

EXECUTIVE SUMMARY

OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE

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

To help improve the administration and control of public assistance programs and related services provided by the State's 58 local social services districts (districts), both OTDA and the 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 New York State's vast technology resources. It manages a consolidated New York State Data Center that supports WMS' data processing requirements, as well as those of 20 other agencies. However, the responsibility for managing local user access accounts and permissions is in the hands of local district administrators. OTDA is primarily responsible for the applications and administration of WMS; OFT is primarily responsible for the system's hardware-operating environment, including file management, disaster recovery, system backup, and computer center maintenance and support.

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

Our audit sought to answer the following question:

- Have OTDA and OFT instituted general and application controls that provide reasonable assurance that data maintained in "Upstate" WMS is

reasonably accurate and reliable, and that controls minimize the risk of unauthorized physical and logical access?

AUDIT OBSERVATIONS AND CONCLUSIONS

While we found that the public assistance eligibility data, for the districts we reviewed, is reasonably accurate, our audit of general and application controls as developed and implemented within OTDA, OFT, and the local districts, found departures from recommended practices. To protect the integrity of computerized information systems and the confidentiality of electronic data, OTDA must institute appropriate controls. Our report contains 32 recommendations to assist OTDA officials in this regard.

Specifically, we found that neither OTDA nor OFT has adequately addressed physical and personnel security over WMS at the local district level. Nor has either agency clearly communicated comprehensive procedures to local administrators about their roles and responsibilities or the steps they would take in an emergency or other situations when WMS service availability has been affected. Also, OTDA and OFT do not monitor district compliance with security procedures and a disaster recovery plan for WMS has not been developed. In addition, we found opportunities for OTDA and OFT to strengthen their telecommunication, and physical security controls. (See pp. 7-19)

We identified a need to improve user ID and password controls. We also found that none of the four districts we visited (Monroe, Onondoga, Schoharie, and Ulster) conduct security awareness training. (See pp. 21-35)

To verify the validity and reliability of WMS data, we tested 1,235 data elements at the four districts. We found 59 errors, a 4.8 percent exception rate, meaning the data on the system was either different or incomplete when compared to the data in the source documents. As this error rate is within the Federal government's acceptable rate, we conclude the overall eligibility data at the four districts is reasonably accurate. (See pp. 37-42)

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 OTDA and OFT officials during the audit.

COMMENTS OF OTDA OFFICIALS

OTDA officials generally disagreed with our recommendations. OTDA officials are of the opinion that taking a more prescriptive role in the supervision of local district operations would exceed their legislative authority. While OTDA

officials acknowledge that they, and the local districts, are obligated to keep social services data confidential, they believe that they have no higher duty regarding WMS data, and no legislative authority to impose requirements on local district practices involving security and confidentiality as it pertains to WMS data. Our report does not say that OTDA's duty is greater with respect to WMS than with local district operations in general. While we continue to believe that OTDA does have the authority to mandate certain local district actions with respect to WMS, at a minimum, OTDA could, pursuant to the Social Services Law, render guidance to local districts in areas such as controls over system access, in an advisory manner.

CONTENTS

Introduction

Background	1
Audit Scope, Objective and Methodology	3
Response of OTDA Officials to Audit	4

Controls Over the Network

Security Management	8
Recommendations	11
Network Monitoring	12
Recommendations	12
Disaster Recovery Plan	13
Recommendation	15
Security Control Settings	15
Recommendation	17
Telecommunications	17
Recommendation	18
Physical Hardware Security	18
Recommendation	18
Removal of Information from OFT Disposed of or Transferred Equipment	18
Recommendation	19

Computer Security

User IDs and Passwords	22
Recommendation	24
Updating User Access	24
Recommendations	25
Assigning Application Functions to Users	26
Recommendations	29
Monitoring Access	30
Recommendations	33
Communication and Training	33
Recommendations	35

Data Integrity

Data Element Testing	37
Recommendations	39
Monitoring Personal Identifiers	39
Recommendations	42

Appendix A

Major Contributors to This Report

Appendix B

Response of OTDA Officials to Audit

Appendix C

State Comptroller's Notes

INTRODUCTION

Background

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

To help improve the administration and control of public assistance programs and related services provided by the State's 58 local social services districts (districts), both OTDA and the 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 New York State's vast technology resources. It manages a consolidated New York State Data Center that supports WMS' data processing requirements, as well as those of 20 other agencies. However, the responsibility for managing local user access accounts and permissions is in the hands of local district administrators. OTDA is primarily responsible for the applications and administration of WMS. 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.

WMS consists of two application subsystems: "Upstate," which is used to maintain the records of clients living in counties outside New York City, and "New York City," which contains the data of clients who are residents of New York City. In 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 obtain access to 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 service 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 service agencies that will enable them to meet clients' needs more effectively.

In June 2001, districts began using applications software on the personal computers that employees use to access WMS through the Human Services Network (HSN) and to access the network maintained for their own district. HSN is a combination of hardware, software, and transmission media that comprise a system of interconnected computers used by several State agencies and the communications used to link them. In such a network, various computer resources, including desktop computers, printers, file servers, and computer applications (e.g., word processing applications, data base applications, and specialized applications such as WMS) are linked together and shared by different individual users in several locations. These users may be either district workers or employees of income maintenance offices, child welfare units, or voluntary agencies. According to OTDA records, software had been installed as of April 2002 in approximately 8,000 personal computers in the

offices of upstate districts that would allow district employees to access WMS. These computers are linked to HSN and/or a district's own internal networks.

AUDIT SCOPE, OBJECTIVE AND METHODOLOGY

During our audit, which covered the period of January 1, 1999 through April 30, 2002, we examined the OTDA's general and application controls over the processing of electronic data and selected aspects of the network controls in place over the Upstate subsystem of WMS. Our objective for this performance audit was to determine whether OTDA and OFT have instituted general and application controls that can provide reasonable assurance of the validity and reliability of data maintained in WMS and minimize the risk of unauthorized physical or logical access. The scope of our audit did not include a vulnerability assessment of HSN. We are currently conducting a separate audit of the New York City subsystem of WMS.

To accomplish our objective, we interviewed OTDA officials and reviewed pertinent OTDA policy and procedures relating to the overall computer operations of the OTDA data center. Our review covered controls over organization and management, system software and hardware, and security. We judgmentally selected the four local social services districts we audited (Monroe, Onondaga, Schoharie, and Ulster), based on relative caseloads and their case review methodology. We interviewed staff at all four districts and observed the practices they follow. The scope of the audit did not include a vulnerability assessment of HSN with a commercial vulnerability assessment product; nor did we test security by attempting to hack in and infiltrate the network. 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 OTDA and OFT officials during the audit.

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 that are included within our audit scope. Further, these standards require that we understand OTDA's internal control structure and its compliance with those laws, rules and regulations that are relevant to OTDA 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 Officials to Audit

A draft copy of this report was provided to OTDA officials for their review and comment. Their comments were considered in preparing this report, and are included in Appendix B. In addition, the State Comptroller’s Notes to OTDA’s response are included as Appendix C.

OTDA officials generally disagreed with our recommendations. OTDA officials are of the opinion that taking a more prescriptive role in the supervision of local district operations would exceed their legislative authority. While OTDA officials acknowledge that they, and the local districts, are obligated to keep social services data confidential, they believe that they have no higher duty regarding WMS data, and no legislative authority to impose requirements on local district practices involving security and confidentiality as it pertains to WMS data. Our report does not say that OTDA’s duty is greater with respect to WMS than with local district operations in general. While we continue to believe that OTDA does have the authority to mandate certain local district actions with respect to WMS, at a minimum, OTDA could, pursuant to the Social Services Law, render guidance to

local districts in areas such as controls over system access, in an advisory manner.

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 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.

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, and processed and reported completely and accurately.

As of January 2002, WMS maintained information on more than 656,000 recipients. WMS is the central registry of all welfare case client data in the State. 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 "...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.

We found that neither OTDA nor OFT has adequately addressed physical and personnel security over WMS at the local district level. Nor has either agency clearly communicated comprehensive procedures to local administrators about their roles and responsibilities or the steps they would take in an emergency or other situations when WMS service availability has been affected. OFT has developed an HSN LAN Administrator's Guide to provide information and assistance to local support staff. This guide explains the basic structure of the HSN and how to use it. In addition, OFT has also developed a Transaction Terminal Security System (TTSS) user reference manual. This manual has three purposes: to serve as a source of information for working with TTSS, to be a training aid for learning about TTSS, and to assist users with the operation of TTSS. However, neither of these manuals discusses steps to; protect computer equipment, monitor problem and password violation logs, or how to resolve problems identified by these logs. In addition, we found that OTDA and OFT has not developed a formal written document that defines OFT's overall responsibilities relating to the HSN network; and OFT itself has

no clear, documented job roles and responsibilities for WMS. In addition, we identified weaknesses in a number of operating system security features that are intended to prevent or detect unauthorized access to a computer network. We reported the details of these weaknesses to OTDA and OFT officials during our audit, but did not include them in this report.

Security Management

According to Part 45, Section 95.621, of the Code of Federal Regulations, if a state agency is responsible for administering a program overseen by the U. S. Department of Health and Human Services, such as public assistance programs administered by OTDA, and it administers the program with an automated data processing (ADP) system such as WMS, the agency is responsible for the security of the data in the system. These regulations require OTDA and OFT to determine and implement appropriate ADP security requirements based on recognized industry standards, and to establish a security plan, policies, and procedures for maintaining the security of ADP data and other resources. They also require compliance certification of their ADP security program, for which they must designate an ADP security manager. Other areas of compliance that must be certified include the physical security of ADP resources and equipment, protecting it from theft and unauthorized use; software and data security; telecommunications and personnel security; emergency preparedness; and contingency plans for meeting critical processing needs generated by service interruptions.

Security Policy

To achieve the best possible safeguards for computer systems, networks, and electronic data, security policies and procedures must be established, documented, and followed. A security policy should address issues such as reviews of audit logs, security job descriptions and duties, and proper configuration of system settings that will achieve adequate security controls over information. Staff are more likely to take appropriate security measures when written policies and procedures relating to security are made available to them.

Although OFT has developed a general security policy, known as the State Data Center Security Policy, we found that it covers only physical and personnel security at the OFT data center

sites; it does not address software, data security, or telecommunications security. Neither OTDA nor OFT has addressed physical and personnel security over WMS at the local district level. Officials of both OTDA and OFT stated that the State Data Center Security Policy was not intended to address security in districts.

We also found that procedures have not been communicated to local administrators about their roles and responsibilities or the steps they should take in an emergency or unexpected situation that affects the availability of WMS service. Officials expressed the belief that district personnel understand they should use the State's help desk for emergencies. In fact, OTDA and OFT officials have stated that they are not responsible for district security -- and should not be -- because the public assistance delivery structure is State-supervised but locally-administered, with districts responsible for making sure that prudent security practices and internal controls are in place.

Without adequate written management directives regarding security procedures and their justification, and without clear definitions of system management job roles, lax security practices may be tolerated; and security exceptions might not be detected. In the absence of complete and comprehensive written procedures addressing the security of WMS, the information in the system is less likely to be adequately protected against unauthorized access. OTDA and OFT have a responsibility to develop security policies that comply with Federal regulations. Such compliance would require both agencies to ensure that districts have adequate security controls. We believe this cannot be achieved unless security policies and procedures are developed that encompass all aspects of a computer system. In addition, if the State is to handle emergencies effectively, it should develop and convey emergency procedures to affected parties, considering the end users, and enforcing district compliance. Officials stated that in January 2002, OTDA developed an Information Security Advisory Workgroup to review and update the agency's policies and procedures.

Roles and Responsibilities Not Formally Defined

An entity-wide program for security planning and management should establish a framework and a continuing cycle of activity that can be used to assess risk, develop and implement

effective security procedures, and monitor the effectiveness of those procedures.

In November 2001, OTDA established an Information Security Office (ISO) within its Division of Legal Affairs. The purpose and intent of the ISO is to ensure that issues related to agency information security (accessibility, integrity, confidentiality, and privacy) are assessed, monitored, managed, and coordinated properly and in a comprehensive manner. However, we found that the ISO's mission applies only to users within OTDA; it does not include users at other agencies or the districts. OTDA officials informed us that they might communicate best security practices to the districts as suggestions, and that their web site makes security information available to anyone who can access the site at the district level.

To achieve a well-designed security control structure, agency management must formally delegate responsibility for all information security matters. Multiple individuals across organizational lines may be involved as long as there is a clear separation of duties and responsibilities that provides effective checks, balances, and accountability. In addition, lines of communication and responsibility for agency information security must be established, maintained, and clearly defined. Communication must work in both directions for the reporting upward of information security problems and the reporting downward of problems, security alerts, and potential virus threats.

We found that OFT has no clear, documented definitions of job roles and responsibilities for HSN network management employees, and no documented method for ensuring proper segregation of duties. In fact, no formal written document exists that defines OFT's overall responsibilities relating to the HSN network or WMS. Although officials stated that they were working on a service-level agreement between the agencies for respective agency roles and responsibilities related to control over the WMS network, they would not share a copy of the draft agreement with the audit team.

Unless network roles and responsibilities are clearly-defined and communicated to responsible employees, security controls may be inadequate; responsibilities may be unclear, misunderstood, or implemented improperly; problems or errors may go undetected and unreported; and controls may be

applied inconsistently. Such conditions may lead to the insufficient protection of sensitive or critical resources and disproportionately-high expenditures for controls over low-risk resources.

OTDA and OFT officials also told us that TTSS administrators and the appropriate district personnel are responsible for making sure that proper security and network controls are in place at the districts. During our site visits, we found that districts had not received adequate guidance from OFT and OTDA on how to implement adequate security procedures over WMS. While OTDA stated they will work with OFT to consider enhancements to the TTSS manual, they claimed that they are not required to or capable of developing and enforcing policies at districts. However, we believe the Law requires these agencies to supervise all forms of work related to public welfare programs for which the State is responsible, including districts' use of WMS to support decisions related to public assistance eligibility. In response to our request, the Counsel of the Office of the State Comptroller provided the opinion that OTDA is responsible for monitoring and supervising the districts' administration of WMS; and that, as part of its oversight function, OTDA is also responsible for guarding the confidentiality of the data collected.

Recommendations

1. Modify and convey a security policy that includes local social service districts and clearly defines administrator roles and responsibilities and encompasses all of the local social services districts.
2. Extend the ISO mission to include local social services districts.
3. In conjunction with OFT, define and document the roles and responsibilities of OFT, HSN network management staff for WMS, and verify that their duties have been segregated properly.
4. In conjunction with OFT, establish a formal written document defining OFT's network and WMS responsibilities.

Network Monitoring

An important element of risk management is verifying that policies and controls intended to reduce risk are effective. Over time, policies and procedures may become inadequate because of changes in operations or deterioration in the degree of compliance. Periodic assessments and ongoing monitoring are important means of identifying areas of noncompliance, reminding employees of their responsibilities and demonstrating management's commitment to the security plan. To assure themselves that their network security program is effective, OFT and OTDA management should monitor the program.

We found that OFT and OTDA staff do not monitor the districts' adherence to security procedures regarding WMS. For example:

- Staff do not oversee the work of district TTSS administrators, and could not identify unusual occurrences at the district level – e.g., excessive attempts to gain access to the system – because no one from the central office looks at violation logs by district or compares violation activities that occur in various districts.
- Staff do not confirm that district workers have not installed unauthorized software on personal computers that would permit access to WMS.

Recommendations

5. Provide local social services districts with guidance on how to implement adequate security procedures for WMS.
6. Monitor local social services districts to verify that they are following proper security practices, including:
 - reviews of violation logs or trending violations,
 - verification that districts have installed only software that has been authorized, and

Recommendations (Cont'd)

- periodic assessments of the appropriateness of district employee access rights.

Disaster Recovery Plan

Using the capacity to process, retrieve, and protect information maintained electronically can have a significant effect on an organization's ability to accomplish its mission. For this reason, an agency should have established procedures for protecting information resources and minimizing the risk of unplanned interruptions, as well as a plan to recover 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 the 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 reestablishing operations at a remote location. They may also include errors, such as writing over a file. If controls are not adequate, then even relatively 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 to share computer resources residing at the New York State Data Center (Center). This five-year agreement, which was effective on October 26, 2000, requires OFT to develop a Plan that can ensure the Center's ability to back up to a designated disaster recovery facility, and to maintain a Disaster Recovery Site (DR Site) in a prescribed offsite location where all Center workflow can be processed for an extended period. It also requires testing and updating the Plan at prescribed time intervals to assure management of its viability and the accuracy of the data.

Even though OFT and OTDA established a work group in October 2001 to develop a formal Plan, none has been developed. Both agencies should prepare and test a

comprehensive Plan that includes the identification and ranking of functions, as well as steps for restoring critical applications. It is important that such plans be documented clearly, communicated to affected staff, and updated to reflect current operations. Staff and other users of the system need to understand their responsibilities in case of emergencies.

The Plan should clearly identify the order in which processing should be restored, the individuals who will be responsible, and the supporting equipment or other resources that will be needed. Data files, computer programs, and critical documents should be routinely duplicated or backed up at an off-site storage facility to prevent or minimize damage to automated operations. 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 an unequipped site that will take some time to prepare for operations, 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 events.

Although OFT routinely performs system backups and has installed environmental controls at the Center, we found that OFT’s backup facility does not have adequate environmental controls. Agency officials told us that, although they have a system for monitoring smoke and water conditions, the cost of a fire suppression system and uninterrupted power system was not justified at the time the site was provisioned. In addition, the backup facility is equipped with system components that originally operated in the main Center; however, when the components were upgraded and/or were no longer needed at the Center, the equipment was transferred to the DR Site. To make sure that the facility is able to function adequately, OFT should equip it with proper environmental controls; and verify that existing equipment is sufficient to meet the processing needs of OTDA.

We also found that the DR Site is located less than one half-mile from the Center, which is not far enough. A single event, such as an extended power or communications outage, would likely impact both locations. Officials told us their choice of location was based on history, cost, and continuity. They said

they had incurred no significant costs to install electrical service, a raised floor, or a cooling system because the site was formerly used by another agency as a data center. They pointed out that the proximity of the DR Site allows for disk mirroring, significantly reducing recovery time, as well as efficient re-deployment of critical staff. We believe OFT should reevaluate this location in light of the possibility that an interruption of power and/or communication lines could affect both the Center and the DR Site. Action should be taken that could prevent a single event from threatening the operations of both locations.

To determine whether the plans will function as designed in an emergency, OFT should conduct periodic disaster-simulation exercises. Through such testing, OFT can identify important weaknesses and take corrective action.

Recommendation

7. Enforce the requirements of the service-level agreement by requiring OFT to:
 - develop a comprehensive Disaster Recovery Plan that considers the detailed aspects delineated in this report, including the conduct of a disaster-simulation exercise to confirm its viability;
 - verify that the Disaster Recovery Site has been equipped with proper environmental controls, including a fire suppression system and an uninterrupted power supply;
 - verify that the Disaster Recovery Site equipment can meet the agency's emergency needs; and
 - evaluate the locations of the Disaster Recovery Site and the New York State Data Center in terms of vulnerability to the effects of a single event (e.g., loss of power and/or communication lines).

Security Control Settings

Network security features should be set to levels that will protect against unauthorized access to network resources, unless settings that provide a lower level of security can be

justified. We reviewed selected security settings on the network's operating system, and then compared them with the settings recommended in a technical reference manual. Because certain weaknesses that we identified could be considered sensitive, we have not included the details relating to these weaknesses in this report. Instead, we have conveyed our findings to OTDA and OFT officials during the audit.

A system of the magnitude of HSN creates unique security challenges; every piece of hardware and software that is introduced into the environment increases the possibility of a security risk. Security is the responsibility of the system administrators, who are responsible for configuring the security settings. An administrator should first research the network security settings recommended by the vendor and then configure the settings for optimal security based on the system's unique needs. If properly configured, the operating system is capable of being very secure; but if it has not been configured correctly, the system can be exploited. The hardware and software alone do not guarantee a secure environment. Just as important as the security settings of the operating system are the organization's policies and procedures, which should be developed and implemented with the cooperation of all the departments of an organization. To create a comprehensive security culture, all of the entity's components should work together.

WMS resides on HSN, which is the collection of hardware, software, and communications involved in connecting and coordinating multiple computers and their resources. OFT services the network and provides network support for several State agencies, including OTDA. WMS and CONNECTIONS (New York's statewide automated child welfare information system) reside on the same network.

During a recent audit, (*Security of the CONNECTIONS System Supporting Child Welfare Services*, Report 2000-S-51, issued March 6, 2002), we found a number of weaknesses in the HSN operating system. OFT officials told us during this audit that they have not yet addressed those weaknesses. As a result, we believe attempts by unauthorized users to gain access to WMS on PCs capable of connecting to HSN are more likely to be successful than they would be if the security features had been set to adequate levels.

During the CONNECTIONS audit, we met with OFT officials to review selected network security settings, and provided them with a listing of weaknesses. In response to that audit, OFT officials indicated that variances between actual and recommended security settings were justified given the transition to a new environment. In addition, they indicated they would adopt settings that are more consistent with the recommended settings after they migrate HSN to a new operating system; however, they predicted that this migration would not take place for three to four years. Meanwhile, OFT expects to continue using the current operating system for HSN for two or three more years, with no immediate plans to change any of the security settings. Consequently the risks we have identified will continue to be present for the near future.

Recommendation

8. Work with OFT to adjust the security settings for the network operating system to the recommended levels unless adequate justification can be given for settings that provide a lower level of security.

Telecommunications

Adequate controls should be established to prevent users from employing their own computers to access WMS, regardless of their location. According to the State's "Preferred Standards and Procedures for Information Security," (Standards) extended authentication procedures are needed to control remote external access to an agency network that contains confidential information. These standards indicate that procedures for remote access should be more stringent than procedures required for on-site logon access. Possible additional protection mechanisms include dial-back systems, in-place procedures that require all connections to be made through a central access point, and devices that prevent desktop modems from being left in the auto-answer mode.

We reviewed the controls in place for remote access to WMS system and found some weaknesses. Because they could be considered sensitive, we have not included the details relating to these weaknesses in this report. Instead, we have conveyed those findings to OTDA and OFT officials during the audit.

Recommendation

9. Develop a remote access policy that will address the weaknesses identified by this audit, including adequate controls over remote dial-up access.

Physical Hardware Security

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 that are used to access a computer; microcomputers; computer file storage areas; and telecommunications equipment and lines, including wiring closets.

We found that OFT limits and monitors access to the Center that houses the host system. However, we did identify some physical security weaknesses. Because they could be considered sensitive, we have not included the details relating to these weaknesses in this report. Instead, we have conveyed these findings to OTDA and OFT officials during the audit.

In response to our preliminary findings, OTDA and OFT officials stated that they are currently reviewing their physical hardware security system.

Recommendation

10. In conjunction with OFT, improve physical security controls over information systems by addressing the weaknesses identified during this audit.

Removal of Information from OFT Disposed of or Transferred Equipment

Part of a control structure to prevent unauthorized access should include procedures for clearing sensitive information and software from computers, disks, and other equipment or media when they are disposed of or transferred to another use. If sensitive information is not fully cleared, it may be recovered and used inappropriately or disclosed by unauthorized

individuals who gain access to the discarded or transferred equipment and media.

The responsibility for clearing information should be clearly assigned. In addition, standard forms or logs should be used to document that all discarded or transferred items are examined for sensitive information and that this information is cleared before the items are released.

Although we found that OFT's practice is to clear data from equipment that is transferred and or disposed of, procedures have not been developed for clearing sensitive information and software. OFT also does not use standard forms or a log to document that all discarded or transferred items have been examined for sensitive information. In response to our findings, OFT officials stated that their practices support the removal of information from media when practical.

Recommendation

11. In conjunction with OFT, develop and implement written procedures for clearing sensitive information and software from equipment and media taken out of service or otherwise transferred.

COMPUTER SECURITY

To verify that computer resources are being protected against unauthorized modification, disclosure, loss, or impairment, agencies should develop and implement a security system that will prevent and detect unauthorized access. Such a system limits 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). According to the U. S. General Accounting Office (GAO), inadequate access controls diminish the reliability of computerized data and increase the risk of destruction or inappropriate disclosure of data.

GAO has developed extensive criteria for access security systems. Using that criteria, we evaluated the TTSS and its implementation at the four local districts (Monroe, Onondaga, Schoharie, and Ulster) in which we conducted our audit fieldwork. We selected these districts to gain an understanding of procedures in districts with small, moderate, and large caseloads. To evaluate the implementation of security controls, we reviewed TTSS guidance documents; interviewed local coordinators; and reviewed local procedures for adding and deleting users, assigning rights to applications, and monitoring usage. We also compared user reports with personnel records, made functional inquiries for terminals and users, and reviewed usage of a security violations report.

We found that TTSS provides a logical framework that limits access to authorized users, allows assignment of specific application rights, and limits the ability to make security changes to designated coordinators. The system tracks user activity, thereby allowing for usage monitoring and security investigations.

All information, regardless of the medium in which it is maintained or communicated, is subject to pertinent State and Federal laws governing access, the protection of privacy, and prohibitions against unauthorized disclosure. Since some of the information in the WMS system is confidential, care must be taken to make sure that only authorized individuals have access

to the system. However, we found that some aspects of TTSS impair its use as a system of security control. We conveyed these weaknesses to OTDA and OFT but omitted them from this report because the details were considered sensitive.

User IDs and Passwords

User identification numbers (IDs) and passwords are logical access controls that identify users and isolate access to system applications. Logical access controls involve the use of computer hardware and software to prevent or detect unauthorized access by requiring users to input user IDs, passwords, or other identifiers that are linked to predetermined access privileges. Logical access controls should be capable of restricting legitimate users to the specific systems, programs, and files they need, and at the same time prevent others from entering the system at all. Logical security controls also enable an organization to identify individual users or computers that have authorized 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.

Access to WMS is controlled through various security features such as passwords. The level of security provided by each feature can be adjusted through the security settings available on the WMS operating system. We reviewed certain of these settings and found that a number of security features were set to provide a lower level of security than is recommended. We reported the details of these weaknesses to OFT officials during the audit, but did not include them in this report.

Security for WMS is maintained and implemented in a highly-distributed control environment that includes OTDA, OFT, and the local social services districts. Through its Network Security TTSS Operations Unit (OFT Security), OFT is responsible for maintaining and operating the TTSS, a mandatory component of WMS that consists of logical controls to add, delete, and identify users of the system; assign rights to specific program applications; and track user and terminal data base activity. OTDA and the districts are responsible for using the TTSS, and for developing security procedures for the assignment of access rights to WMS users and monitoring their usage.

According to the TTSS Manual, TTSS was designed to accommodate varying degrees of security control so that the various districts, which differ widely in size, caseload, and operating procedures, can provide the security controls best suited to their needs. Therefore, each district is responsible for developing access controls using the logical framework TTSS provides. The local district security coordinators (coordinators) are responsible for adding, modifying, deleting, and monitoring access privileges for users and terminals within their districts. The TTSS provides identification and isolation controls through user IDs and passwords, which are required for all sign-ons to WMS. User IDs identify specific users and assign rights to specific applications, while passwords make it possible to authenticate access rights to the identified user. User IDs are assigned and not confidential, but passwords are designated by the individual user and are assumed to be confidential to that person. However, passwords provide access security only if controls have been established to ensure their confidentiality. If controls are not effective, an individual might impersonate an authorized user and gain inappropriate access to WMS applications.

To control the confidentiality and authorized use of passwords for system access, GAO recommends the assignment of uniquely-identified, individual users who are asked to create their own passwords with a minimum of six characters. It points out that passwords should be changed periodically (every 30-90 days) and not displayed upon entry. GAO guidelines discourage the use of names, words, or old passwords within six generations, but encourage the use of alphanumeric combinations. In addition, GAO notes that the effectiveness of passwords can be enhanced if limits are set on the number of entry attempts a person can make with a password that is invalid. Such limits prevent access through continuous sequential attempts, and helps guard against computer-assisted unauthorized penetration.

Although TTSS contains several control elements that enhance password security, we identified some weaknesses. Because they could be considered sensitive, we have not included the details relating to these weaknesses in this report. Instead, we have conveyed those findings to OTDA and OFT officials during the audit. The officials told us that the existing password policy was the result of a prior security audit and pointed out that any password modification would contradict that audit. However, we

note that the audit was conducted in the mid-1980s by an external audit organization. As technology changes, so should a system's security controls. In response to preliminary, officials stated that they would consider enhancements when they redesign WMS. We encourage OTDA and OFT to strengthen their system controls by implementing our recommendations.

Recommendation

12. Improve user ID and password controls by addressing the weaknesses identified during this audit.

Updating User Access

According to GAO, the addition of new users to a computer system should be approved by appropriate managers and communicated to security managers in writing with the use of standardized access forms. It is equally important for security managers to be notified immediately when an employee is no longer working in the authorized capacity and does not require access. Policies governing such notifications should make it clear who is responsible for handling them. Compliance with access authorizations should be monitored through periodic comparisons of authorizations with the actual level of access activity.

All four of the districts we visited depend on communications from supervisors for addition notifications. TTSS also allows coordinators to perform access inquiries and to generate routine reports on user IDs. However, once a user is on the system, districts do not consistently update personal identifiers, nor do they consistently update the system to terminate access for users who no longer hold authorized positions.

OFT Security provides an Authorized Functions Report that lists, for each district, all active user IDs along with the user's name, job title, identification number, and assigned functions. This report is sent to the districts in hard copy once a year, but is available on request throughout the year. At Monroe, Onondaga, and Ulster, we compared the names of individuals listed in the October 16, 2001, Authorized Functions Reports with names contained in district personnel lists and local lists of employee departures. There were 2,140 individuals with WMS access in Monroe, Onondaga, and Ulster. We judgmentally

sampled 365 users and found 28 instances where their name differed from the district's personnel listing. We were able to verify that these differences were the result of name changes that the personnel office had not communicated to the coordinator. Failure to communicate such changes impairs the usefulness of system reports as monitoring tools.

In Monroe, Onondaga, and Ulster, we found 11, 2, and 8 active user IDs and application functions, respectively, for individuals who no longer held authorized positions. Although the system will deactivate a user ID if it is not used for six months, the IDs for these former employees represent a vulnerability in the meantime until they are deactivated; if they are obtained and used inappropriately, they will not deactivate automatically.

The inappropriate user IDs remained active because the coordinators did not receive timely notice from management stating that the user no longer required WMS access. Some coordinators use local payroll or personnel reports as a compensating control alerting them of the need to make changes. However, authorized users do not always work for the district. For example, both Onondaga and Ulster have substantial numbers of users who work for other agencies. Four of the eight exceptions found in Ulster involved employees of other agencies. If the user is not employed by the district, the coordinator will know that a change is required only if the management at the user's agency communicates the need to make the change.

OFT Security sends out a cover letter to the districts suggesting that they use the Authorized Functions Report to verify access. We believe that local control over users would improve if the districts obtained and reviewed these reports at periodic intervals.

Recommendations

13. Require local social services districts to establish clear procedures for communicating personnel changes (e.g., adds, deletes, title/responsibility changes, and name changes) to the security coordinators.

Recommendations (Cont'd)

14. Require local social services districts to distribute periodic memos to supervisors of all WMS users reminding them of their responsibility to provide timely notice to the security coordinators for employment changes.
15. Provide local social services districts with Authorized Functions Reports more frequently than annually (e.g., every six months). Require security coordinators to review the reports to verify the appropriateness of the individuals and functions listed.

Assigning Application Functions to Users

To provide assurance that users are restricted 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. According to GAO, a user's specific application needs should be approved by appropriate senior management and communicated in writing to the security function. A formal process for assigning application access can reduce the risks associated with mishandling, altering, or misunderstanding the authorization. GAO further states that failure to take responsibility for assigning application access can leave the decision-making in the hands of personnel who are not in the best position to determine a user's needs. This can lead to the assignment of overly-broad access, the circumvention of control objectives, and the introduction of 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 their terminal.

Although TTSS allows a logical functional segregation control for the various WMS applications, its effectiveness is diminished because of insufficient guidance, inconsistent implementation practices in the districts, and the inability of the transactions

allowed by the applications to match the job responsibilities of some users.

When users and their supervisors request access to a particular application, they are requesting a specific coded transaction on the WMS system. Although several hundred transaction steps are described throughout the WMS System Reference Manual, the manual contains no index that references a specific transaction code to the detailed description of the transaction. Without a ready reference to the activities allowed under the transaction code, supervisors who request functions and coordinators who assign them must rely either on experience or reference to the functions held by users with similar responsibilities. This can lead to situations in which users have greater access rights than they need.

Coordinators who assign functions must first determine which TTSS menu choice is required to allow the user (and terminal) access to the requested transaction. Although the TTSS manual provides clear guidance on how to assign applications to users, it offers none on determining which functions are appropriate for job responsibilities. According to GAO, the process of determining application rights can be simplified by developing standard profiles that describe access needs for groups of users. Of the four districts we audited, only Monroe has developed such a standard profile for assigning applications. As a result, Monroe supervisors and coordinators know which functions to request and assign, based on a standard pattern. In the other three districts we audited, the supervisor may have a clear understanding only of the WMS transaction. This limitation is reflected in the forms used in Onondaga, Schoharie, and Ulster to authorize access for a user. Onondaga's form has no area devoted to functions, and Ulster confines the designation of functions needed to a brief comments section. Schoharie's form contains a checklist of TTSS functions, and this device can be circumvented by providing the name and job title of an existing user with similar responsibilities.

Because supervisors do not know which applications they should use to perform the assigned functions, their signatures on the user authorization form cannot serve as a control to ensure that applications assigned to a user have been approved by management.

The same report that allows monitoring of user ID access rights can be used to monitor the functions assigned to the user. In addition, TTSS coordinators may make functional inquiries about users and terminals at any time. Using these reports and inquiries, we performed limited testing of functions assigned to users and terminals in Onondaga and Ulster, which had substantial numbers of users employed by other agencies. In both, we found that users had been assigned functions that were not needed in their work areas. For example, in Onondaga, 4 of the 15 sampled employees placed by an outside employment agency had been given the ability to make non-services data entries even though they had no data entry responsibilities.

We also reviewed functions assigned to remote terminals in these two districts. Terminal functions are usually assigned to match those of the expected user(s). However, the terminal reportedly located at Ulster County Mental Health had functions that were not needed by the user at the site. According to the Terminal Authorized Functions Report, the five terminals sampled in Onondaga also had all functions that were not needed by the users at the site. These remote sites offer opportunities for anyone with the function assigned to his or her user ID to manipulate data on WMS.

Every year, OFT Security sends a Terminal Operator Authorized Functions Report to each district. Included with this report was a cover letter suggesting that the district use the information it contains to monitor users and functions assigned. Such a report was distributed to the districts in Onondaga and Ulster in August 2001, two months before our site visits. Despite the ready availability of this information, management has not reviewed the activities of its users or terminals.

We reviewed those functions related to input, edit, and inquiry of data related to Temporary Assistance for Needy Families (TANF). However, these functions, as they exist on TTSS, do not fully allow the matching of application rights to job responsibilities. For example, some transactions overlap functions. Prior to conversion, non-budget TANF data was entered by clerks in a data entry unit. Direct data entry allows examiners to enter case data as well as budget data, and most case data is entered through the case-opening process. All of the four districts we visited use direct data entry but limit the opening data entry to specialized units or titles. However, TTSS

does not functionally segregate openings from ongoing case data maintenance – the right to do either is conveyed by Non-Services Data Entry. In this instance, the application right cannot logically be limited to the job duties of the users, a complication that places a premium on monitoring controls to assure management that all openings are appropriate and that all data entered is reasonably-accurate. Given the purpose of the WMS, the most broadly-distributed functions are those allowing inquiry. Therefore, application access cannot be used as a control over the confidentiality of the client data on the system. The ultimate controls over confidential data are the basic access security controls (user ID, password) and the confidentiality policies of the agencies with access to the data.

In response to our preliminary findings, we were told that there are currently no requirements to segregate or separate specific functional duties or WMS functions. As a result, districts may or may not determine such separation to be appropriate; the decision would depend on an individual district's operational work flow and procedures. This localized decision-making can lead to the assignment of overly-broad application rights, resulting in increased risks that data will be manipulated and disclosed inappropriately.

Recommendations

16. Require local social services districts to develop standard functional profiles according to responsibilities that can help supervisors assign, review, and approve specific applications according to their districts' operating procedures.
17. Require local social services districts to develop procedures that require management to approve all functions assigned to users.
18. Restrict an employee's access, when WMS is re-designed, to those functions associated with job responsibilities.
19. Provide local social services districts with guidance on functional duties that should be segregated.

Recommendations (Cont'd)

20. Provide local social services districts with an index that describes WMS transactions allowed under the various TTSS functions.

Monitoring Access

According to 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.

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 for inquiry on site logs, which OFT Security uses to generate a weekly Terminal Security Violations Report that details, by site and date, various types of security violations, including failed sign-ons, incorrect passwords, time-outs, and disallowed transactions. Local security coordinators are responsible for reviewing the report to determine whether there are patterns of violations that should be addressed.

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 had occurred three times that day for that user at that terminal. Although specific violation detail such as time of day is not on the report, the report does allow coordinators to monitor usage by identifying the terminals or users related to the violations. In addition, by making local TTSS inquiries, the coordinator could obtain the details of activity at specific terminals in real time for the current business week, as well as detailed transaction data.

We obtained the reports for the period October 1, 2001 through October 5, 2001, for the four districts we visited, and found

numerous violations in each district. According to these reports, the following violations occurred:

VIOLATION OCCURRENCE BY LOCAL SOCIAL SERVICES DISTRICT FIVE DAYS ENDING 10/5/01

VIOLATION	MONROE (508 users on report)	ONONDAGA (413 users on report)	ULSTER (94 users on report)	SCHOHARIE (16 users on report)	TOTAL
TERMINAL TIMEOUT	6,282	5,659	957	70	12,968
TRANSACTION NOT ALLOWED	455	460	57	12	984
USER ID NOT ON FILE	186 (16 terminals on report with this violation)	183 (15 terminals on report with this violation)	129 (5 terminals on report with this violation)	7 (1 terminal on report with this violation)	505
WRONG PASSWORD	240	107	56	15	418
TERMINAL OR USER ID ALREADY ACTIVE	103	135	27	3	268
TOTAL	7,266	6,544	1,226	107	15,143

The chart shows the total number of occurrences for each type of violation, while the report provides daily violation activity by individual users by terminal as well as the total number of violations committed by each user by terminal by day. For example, in Ulster, one of the reported “User ID Not On File” violations represents 53 failed log-on attempts for that terminal on that date. Actual detail for the individual violations (time of day) is not available on the report and would only be reported in detail upon request.

The effectiveness of this report as a monitoring tool depends both on the usefulness of the information conveyed and the use made of it by the coordinators in the districts. We were told by officials in OTDA and in the districts we visited that the current format detracts from the report’s usefulness, because violations are reported by user ID instead of violation type. Coordinators in the districts we visited told us that the vast number of terminal timeouts choke the report, and that they are not a terribly-meaningful violation. A change in format that would group violations by type instead of by user might increase its usefulness. In that format, user IDs should still be grouped within the violation section so that patterns of violation by particular users would be readily apparent.

Even in its current format, users can employ the report to identify questionable security practices. When we reviewed the reports, we easily found a user who had multiple password

failures on three of the five days, another user who had timed-out daily between six and ten times per day, and a third who had made multiple attempts to access unauthorized budgeting functions.

When we discussed the report with coordinators, they had differing opinions over the seriousness of some violation types. Ulster does not consider the terminal timeouts to be serious violations, and Onondaga does not follow up on them. In Monroe, however, the coordinator discusses such violations with the user's supervisor. The consequences of leaving a session open in a public office can lead to inappropriate disclosure of confidential information. We noted two instances in which the reports listed more than 50 user ID violations for a single terminal on a single day. Those responsible in both districts where these violations were reported did not think they warranted investigation, attributing the incidences to either user ineptitude or mis-keying. However, extensive violations of this type (as well as the use of incorrect passwords) could indicate attempts to penetrate the system.

In Monroe, the coordinator told us she takes actions based on the report by disconnecting users who attempt disallowed transactions, discussing excessive time-outs with supervisors, etc. Coordinators in Onondaga and Schoharie told us they review the report but do not perform as extensive a follow-up on reported violations -- Onondaga's coordinator marks up the report for any violations he decides to follow up on; in Schoharie, improper transactions are highlighted. Ulster officials indicated they had not been receiving the report. We found that the coordinator designated by TTSS in Albany to receive the e-mailed report, did not know she was to receive it and did not have a terminal assigned that could receive the e-mail.

When the report was sent to the districts in hard copy, OFT Security included a cover letter for guidance in its use, but the e-mailed report does not include such guidance. The TTSS manual does not mention the report; it does provide instructions for making site log inquiries, but does not explain why such inquiries should be made or how information obtained through inquiry may be used. As with other security controls, OTDA provides the logical and reporting framework but leaves development and implementation of a system of control to the individual districts. Districts would benefit from any guidance

that OFT Security could provide for using the report and inquiry functions to develop controls.

Recommendations

21. Survey district coordinators to determine if modifying the Terminal Security Violations Report would enhance the reports usefulness and meet coordinator needs.
22. Require security coordinators at local social services districts to follow up promptly on all sensitive or extensive violations and to determine whether corrective action is necessary.
23. Verify that all designated recipients are actually receiving the Terminal Security Violations Report and that required follow-ups are being performed.
24. Develop and distribute guidance to TTSS coordinators at local social services districts on the use of the Terminal Security Violations Report and inquiry functions.

Communication and Training

If management is to be assured that the security of a system is effective, they must educate its users. GAO guidelines recommend that users be informed of the importance of the information they handle, as well as the legal and business reasons for maintaining its integrity and confidentiality. They also recommend that users be required to periodically sign a statement that acknowledges awareness and acceptance of responsibility for security, including the consequences of security violations, and their responsibilities for following all organizational policies, such as maintaining the confidentiality of passwords and physical security over their assigned areas.

According to GAO, the agency should distribute documentation describing security policies, procedures, and individual responsibilities, including expected behavior; and require both new and existing employees to participate in comprehensive security orientation, training, and periodic refresher programs communicating security guidelines.

To assure management that the actual control structure will meet the needs of each district, the TTSS manual delegates responsibility for implementing security controls to the district commissioners. Although the manual provides useful instruction on system use, this instruction is limited to detailed steps in the use of various applications for making security changes, initiating security inquiries, and requesting reports. It does not provide guidance on security control implementation.

When we reviewed communication and training in the districts we audited, we found that policies and procedures were communicated to users in widely-varying degrees. For example, Monroe communicates its security policies through relevant sections in the local data entry manual as well as a requirement that users sign a policy statement that specifically communicates responsibilities for password and terminal session security. On the other hand, Schoharie only requires new users to sign a confidentiality statement that is silent on security issues.

OTDA established an Information Security Office (ISO) within the Division of Legal Affairs during our audit. To date, it has distributed guidance on password security and virus protection to OTDA users, established a web page on security issues that is accessible to the districts as well as OTDA's Albany office, and established an information security advisory work group within OTDA; and is currently developing a training module to be presented to all users within OTDA. However, we found that none of the districts we audited conducts security awareness training. We believe that ISO should share the training module with the local districts as well.

OFT and OTDA officials told us they believe they can do no more than recommend best practices to the districts. They said they do not think they can specifically require the districts to offer security awareness training. On the contrary, it is our belief that, because WMS and TTSS are State resources that are the responsibility of OFT and OTDA, it is the responsibility of OTDA to train all users in appropriate security procedures, including all districts. This could be accomplished by extending the ISO training module to all 58 districts.

GAO points out that security awareness training will educate users about risks and make them less likely to compromise sensitive information and resources. However, the weaknesses

previously mentioned in this report show that managers and users are not as aware of security as they should be. Coordinators could issue warnings not to use certain password combinations that could be identified easily by users. The reports of large numbers of terminal timeouts show that many local users disregard basic session security by leaving applications open at an unattended terminal. Reinforcing basic security concepts would increase the effectiveness of the logical access security of WMS.

Recommendations

25. Extend the ISO training module to all 58 local social services districts.
26. Require local social services districts to provide all local users with security awareness training and guidance and to provide coordinators with security guidance. Training should include the GAO standards for computer security as described in this report.
27. Require local social services districts to adopt security policies and procedures and communicate them to users.
28. Revise the TTSS manual to cover control objectives such as guidance on implementing controls, separation of duties, monitoring reports and their intended use, and security awareness procedures.

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, district employees must enter data accurately.

Data Element Testing

Local social services districts are responsible for the accurate entry of client demographic and financial data in WMS. The accuracy of this data should be assured through logical system edits and supervisory case review.

WMS offers more than 900 system edits that can verify the completeness of specific data elements, that the data have been entered in the proper format, and that they are compatible with other data elements. If case data has an edit error, WMS requires that the edit be corrected before the case data is updated and an authorization is printed. When we observed case data entry, we noted that the system edits operated as designed.

However, edits cannot guarantee that the data entered represent the data in the source documents. For example, a user may transpose digits when entering a number, but as long as the entered number was the correct length it would pass the edit. In this situation, a review procedure comparing the data entered with the data on the source documents would be necessary to detect the error.

Data updates that have cleared system edits result in the printing of an authorization form (Form 3209). District supervisors are required to review all Form 3209s and sign them as an attestation of approval and accuracy. Three of the four districts we audited are required to review all cases; the fourth, Onondaga, has an approved case review methodology that exempts it from reviewing all authorizations. All four districts use direct data entry, employing a mix of data entry and

review methods; but the two smaller ones have dedicated staff who perform case openings.

To determine the integrity of WMS data, we randomly selected 100 TANF cases (of 13,971), including 25 cases from each of the 4 counties visited. For each case, we obtained data that was in WMS as of November 2001 by printing the case comprehensive and latest budget. We traced selected data elements to source documents in the case files and noted any variances.

We selected nine demographic and budgetary data elements for testing (name of individual active on a case, date of birth for active individual, Social Security number for active individual, name of individuals in household, number of individuals on the case, shelter type, fuel type, actual monthly shelter cost, and gross wages). Although OTDA officials told us they consider all WMS data to be important, we selected these nine data elements for audit purposes because they are relevant to eligibility determination. For evaluation purposes, we used the Federal exception rate calculated under the Aid for Dependent Children Program (AFDC) that preceded TANF. In 1996, the Federal government had sampled state transactions to evaluate the appropriateness of the welfare payments and concluded that an average exception rate of 5.8 percent to 6 percent was acceptable.

Although we sampled 25 cases in each district, the actual number of data elements we tested varied by case depending on the number of individuals in each case. In total, we audited 1,235 data elements and found 59 errors, or a 4.8 percent exception rate. We considered as errors all instances in which the data on the system were found to be either different or incomplete when compared with the data in the source documents.

We found that Onondaga had the fewest number of exceptions, a performance we attribute to its review procedures. This district uses a comprehensive desk guide for case reviews, analyzes results, and uses these results to develop improvement opportunities. In accordance with OTDA policy, the other three districts require supervisory review for every case, but do not have formal guidance and feedback procedures.

While we found that approximately 1 percent of the elements we tested were errors likely to affect public assistance payments, districts should make every effort to verify that employees are entering accurate and complete data in WMS. Inaccurate personal identifiers can impair data matches, and could result in the denial or issuance of inappropriate benefits. Inaccurate budgetary data can also affect a public assistance grant. We provided officials of OTDA and each of the districts with the errors we identified.

From the same case sample, we manually recalculated the budgets for the first 15 sampled cases in each district. For the 60 budgets we recalculated, we found the system had determined benefits correctly in every case.

As previously stated, districts are required to perform supervisory reviews to verify that WMS data is accurate. We found that system edits have been developed for completeness, compatibility, and entry format. Furthermore, our budget recalculations indicate the system is calculating public assistance payments accurately. Finally, our tests comparing selected data elements with those in source documents found errors to be within an acceptable rate. As a result, we believe that the overall eligibility data (demographic and budgetary) at the four districts we reviewed are reasonably-accurate.

Recommendations

29. Verify that case reviews by district supervisors include the matching of selected data with those in source documents, identification of deficient areas, and development of corrective action plans for addressing the deficient areas.
30. Verify that districts correct the errors we found during our case file review.

Monitoring Personal Identifiers

Of the 59 errors found in our case review audit, 21 involved personal identifiers (e.g., first and last name, date of birth). WMS generates numerous Operational Information and Management Reports that provide district personnel and/or State personnel with information that can help them perform

their functions. The districts print and distribute the reports, which are available to the districts according to a set schedule. For example, the WINR5126 Report, "Individuals with Incorrect or No Social Security Number on WMS," is a quarterly document that provides a list of active recipients whose Social Security numbers are recorded on WMS but cannot be validated against Social Security Administration (SSA) data.

This quarterly report, which matches WMS data with SSA data, helps supervisors and workers identify cases that require corrective action. When a problem occurs in any of the personal identifying information fields, codes on the report indicate which identifiers caused the failed validation. Documentation such as birth certificates, marriage certificates, and Social Security cards should be present in the case file, making it possible to follow up on the variance by comparing system data with information in paper records.

We tested district use of the WINR5126 report during our visits to Monroe, Onondaga, Schoharie, and Ulster. We obtained information from WINR5126 reports for these districts that were dated July 14, 2001. According to these reports, the 4 districts had 642 TANF clients with a missing or invalid Social Security number. Of these 642 clients, 424 had been reported for 4 or more quarters, an indication that the resolution is not timely. The following chart reflects the number of WMS cases and individuals in these four districts with invalid or missing Social Security numbers as of July 14, 2001.

Summary of WINR5126 Report as of July 14, 2001						
Districts	Type	Cases	Individuals 2 Quarters or less	Individuals 3 Quarters	Individuals 4 or more Quarters	Total Individuals
Monroe	TANF	499	112	41	369	522
	FS&MA	612	201	83	353	637
Onondaga	TANF	86	32	14	44	90
	FS&MA	279	138	29	122	289
Schoharie	TANF	1	0	0	1	1
	FS&MA	48	11	9	29	49
Ulster	TANF	28	15	4	10	29
	FS&MA	179	68	25	91	184
Total	TANF	614	159	59	424	642
	FS&MA	1,118	418	146	595	1,159

FS & MA (Food Stamps and Medical Assistance)
TANF (Temporary Assistance to Needy Families)

According to the preceding chart, the July report listed 369 TANF clients in Monroe with long-term validation failures (reported for 4 or more quarters). An additional 112 individuals had been added to the report in the 2 most-recent quarters for

Monroe. When we reviewed 12 of the long-term cases reported in this district, we found that the Social Security number validation failure occurred because 10 of the cases had correctable data entry errors (name or number variances from source documents). Use of the report in this district would directly improve data integrity.

We found that not every one of the four districts consistently makes effective use of this report as a monitoring tool. Monroe neither prints nor utilizes the report. In Onondaga, area supervisors distribute the report to workers who are responsible for correcting the Social Security number. However, the district has no supervisory review process. This district has no documented supervisory review process for verifying that corrective action is being taken. Schoharie had just one TANF client with a long-term validation issue. However, even though the error was the result of a misread number, the case had closed without correction. Ulster supervisors generally review the cases reported and follow up on the variances. However, one of the supervisors, who was responsible for resolving six long-term validation failures, did not utilize the report.

We judgmentally sampled 38 of the 424 individuals reported for 4 or more quarters and compared the personal identifying data on the report with that in the source documents in the case files. In the smaller districts, we selected all long-term validation failures; in the two larger districts, we used small judgmental samples. We found 23 instances in which the data on the report did not match the data in the source documents (birth certificates, marriage certificates, driver licenses, Social Security cards). For example, some of these fields could not be validated because a single erroneous digit had been entered during data entry. In some other cases, a district employee did not enter a name correctly on WMS or a client did not communicate a name change to the SSA. In the latter case, the corrective action would involve the client applying for a new Social Security number in a new name.

Data integrity can be impaired if the report is not used to discover and correct data error, and personal identifiers are used for data matches. WMS personal identification data are matched routinely to information in other databases to determine whether the individuals on the case have undisclosed resources. These resources (wages, unemployment insurance, Social Security benefits) could directly affect the determination

of public assistance benefits. Without sound personal identification data, such matches may not be possible or may yield a false result.

Recommendations

31. Re-convey to each district the importance of a valid Social Security number, the value of the WINR5126 report, and the need for timely resolution of Social Security number validation failures.
32. Analyze WINR5126 report statistics to identify districts that appear to have an unusually high number of Social Security numbers not validated by the SSA. Follow up with districts to determine the cause.

MAJOR CONTRIBUTORS TO THIS REPORT

William Challice

Richard Sturm

Donald Geary

Nadine Morrell

Mark Ren

Randy Partridge

Mike Breer

Mark Radley

Marticia Madory



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) 474-7870 - Fax

Brian J. Wing
Commissioner

February 10, 2003

Re: **Draft Audit Report: OTDA Welfare Management System General and Application Controls - 2001-S-35**

Dear Mr. Challice:

The following is the New York State Office of Temporary and Disability Assistance (OTDA) response to the Office of State Comptroller (OSC) recommendations offered in the draft report entitled "Office of Temporary and Disability Assistance Welfare Management System General and Application Controls.

General Comments

The draft report states that preliminary copies of the matters contained in your report were provided for review and comment, and that OSC has considered OTDA's comments, as appropriate, in preparing your report. However, we must once again express our extreme concern and disappointment at the fact that the findings and recommendations as presented substantially fail to incorporate extensive comments and supporting information provided by OTDA and Office For Technology (OFT) representatives throughout the audit process.

*
Note
1

The findings and recommendations as presented do not reflect points we have consistently made in previous responses, and considerable substantiating information OTDA and OFT representatives have provided through numerous discussions, meetings and written responses. For example, the burdensome impact on users and the system if password change rules were to be made more prescriptive, and our position and perspectives regarding district responsibility to ensure proper access and security administration protocols are followed, as supported by the legal opinion provided by OTDA Counsel, are not properly reflected.

*
Note
1

We have also consistently expressed concerns regarding the GAO standards OSC used. The sources and standards referenced during the audit process were designed for open systems, and as such are not entirely relative to a mainframe environment. 45 CFR does not call for application of a specific industry standard in reviewing systems security. Information security and the technical mechanisms in place to ensure it must be designed to fit the environment and business needs. One-size-fits-all audit standards are therefore not appropriate.

*
Note
2

All references to "weaknesses reported to OTDA and OFT but not included in this report" should be reworded to say: "some deviations from industry guidelines and best practices were observed and noted to OTDA and OFT staff separate from this report so they could be reviewed for risk management".

"providing temporary assistance for permanent change"

As this is a "redacted" report, the "unredacted" version should include the above details and be delivered to OTDA and OFT.

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

1. **Recommendation:** *Modify and convey a security policy that includes local social service districts and clearly defines administrator roles and responsibilities and encompasses all of the local social services districts.*

Response: Roles and responsibilities for Local Network and Security Administrators as documented in the Human Services Network (HSN) LAN Administrator Manual and the TTSS Security Coordinator's Reference Manual were provided to OSC during the audit. We believe these are sufficiently clear in conveying administrator roles and responsibilities, and encompasses local districts.

2. **Recommendation:** *Extend the ISO mission to include local social services districts.*

Response: We are of the opinion that taking a more prescriptive role in the supervision of local district operations would exceed our legislative authority. OTDA Counsel's Office has rendered an opinion that while clearly both the agency and local districts are obligated to keep social services data confidential, there is no higher duty regarding WMS data and no legislative authority for the State to impose burdensome requirements on local district practices involving security and confidentiality as it pertains to WMS data. See attached OTDA legal opinion.

3. **Recommendation:** *In conjunction with OFT, define and document the roles and responsibilities of OFT, HSN network management staff for WMS, and verify that their duties have been segregated properly.*

Response: As previously stated, roles and responsibilities were supplied to OSC for Local Network and Security Administrators as documented in the Human Services Network LAN Administrator Manual and the TTSS Security Coordinator's Reference Manual. We believe these manuals are sufficiently clear to meet requirements.

4. **Recommendation:** *In conjunction with OFT, establish a formal written document defining OFT's network and WMS responsibilities.*

Response: As noted in our response to the recommendation 1, network administration roles and responsibilities are documented in the LAN Administrator's Guide supplied to OSC. There is no distinction made for a WMS Network. It is a Human Services Network shared by 3 agencies.

5. **Recommendation:** *Provide local social services districts with guidance on how to implement adequate security procedures for WMS.*

Response: As previously stated, Local Districts have and do receive guidance in this area. Latitude exists for districts to apply TTSS guidelines. OTDA previously responded that they will work with OFT to consider enhancements to the TTSS procedures manual according to findings.

6. **Recommendation:** *Monitor local social services districts to verify that they are following proper security practices, including:*

- *Reviews of violation logs or tending violations.*
- *Verification that districts have installed only software that has been authorized, and*
- *Periodic assessments of the appropriateness of district employee access rights.*

*
Note
3

*
Note
4

*
Note
5

*
Note
4

*
Note
4

* See State Comptroller's Notes, Appendix C

Response: As previously stated, the Local Districts are responsible for physical and personnel security in the districts. Our reading of the statute leads us to conclude that assuming a more prescriptive posture in local district operations would exceed OTDA's legislative authority. See attached OTDA legal opinion.

*
Note
5

7. **Recommendation:** Enforce the requirements of the service-level agreement by requiring OFT to:

- Develop a comprehensive Disaster Recovery Plan that considers the detailed aspects delineated in this report, including the conduct of a disaster-simulation exercise to confirm its viability.
- Verify that the Disaster Recovery Site has been equipped with proper environmental controls, including a fire suppression system and an uninterrupted power supply;
- Verify that the Disaster Recovery Site equipment can meet the agency's emergency needs; and
- Evaluate the locations of the Disaster Recovery Site and the New York State Data Center in terms of vulnerability to the effects of a single event (e.g., loss of power and/or communication lines).

Response: An extract of the OTDA Business Continuity Plan was provided to substantiate the fact that a data center/mainframe disaster recovery plan exists. Work on the Disaster Recovery Site is well underway and expected to be completed within the first Quarter of 2003. OTDA and the OFT Data Center are working together to determine final requirements.

*
Note
6

8. **Recommendation:** Work with OFT to adjust the security settings for the network operating system to the recommended levels unless adequate justification can be given for settings that provide a lower level of security.

Response: We disagree. The concept of a "weaknesses" cited in the finding is misleading since it is based on Microsoft's recommended settings. OFT has chosen their settings based upon security industry guidelines, which are in fact, more rigorous than Microsoft's settings.

*
Note
7

9. **Recommendation:** Develop a remote access policy that will address the weaknesses identified by this audit, including adequate controls over remote dial-up access.

Response: As we have told OSC auditors on many occasions, authorized remote access to WMS does not exist. The HSN also has a remote access policy in place. However, if an individual were to attempt to circumvent the policy, TTSS controls would prevent unauthorized individuals from gaining access.

*
Note
8

10. **Recommendation:** In conjunction with OFT, improve physical security controls over information systems by addressing the weaknesses identified during this audit.

Response: There is a question as to which weaknesses this specifically refers to, Data Center and/or Local District physical security. For those weaknesses specific to the Data Center, we will review the findings and make changes where appropriate.

11. **Recommendation:** In conjunction with OFT, develop and implement written procedures for clearing sensitive information and software from equipment and media taken out of service or otherwise transferred.

Response: We will examine OSC's evidence supporting this recommendation and make changes where appropriate.

12. **Recommendation:** *Improve user ID and password controls by addressing the weaknesses identified during this audit.*

Response: As previously advised, this will be considered during WMS redesign.

13. **Recommendation:** *Require local social services districts to establish clear procedures for communicating personnel changes (e.g., adds, deletes, title/responsibility changes, and name changes) to the security coordinators.*

Response: OTDA is of the opinion that we do not have the legislative authority to "require" these things be done. As we have done in the past, we will continue to provide guidance. Also see response to recommendation #2.

14. **Recommendation:** *Require local social services districts to distribute periodic memos to supervisors of all WMS users reminding them of their responsibility to provide timely notice to the security coordinators for employment changes.*

Response: See response to recommendation 2.

15. **Recommendation:** *Provide local social services districts with Authorized Functions Reports more frequently than annually (e.g., every six months). Require security coordinators to review the reports to verify the appropriateness of the individuals and functions listed.*

Response: These reports can be requested on-line as frequently as needed.

16. **Recommendation:** *Require local social services districts to develop standard functional profiles according to responsibilities that can help supervisors assign, review, and approve specific applications according to their districts' operating procedures.*

Response: See response to recommendation 2.

17. **Recommendation:** *Require local social services districts to develop procedures that require management to approve all functions assigned to users.*

Response: See response to recommendation 2.

18. **Recommendation:** *Restrict an employee's access, when WMS is redesigned, to those functions associated with job responsibilities.*

Response: As previously discussed with OSC, we have tried to identify job profiles and have been unable to develop them, somewhat due to the large number of civil service job titles and the reality that small and medium districts have individuals doing multiple jobs.

19. **Recommendation:** *Provide local social services districts with guidance on functional duties that should be segregated.*

Response: Because of the wide variation in staffing patterns in the 58 districts, we do not believe it would be practical to prescribe how functional duties should be segregated. We will, however, issue a reminder to the districts on the importance of internal control considerations in the assignment of functional duties.

20. **Recommendation:** *Provide local social services districts with an index that describes WMS transactions allowed under the various TTSS functions.*

Response: As previously stated, this was provided in the past. OTDA will work with OFT to assess if this needs to be brought up to date.

*
Note
5

*
Note
5

*
Note
9

*
Note
5

*
Note
5

* See State Comptroller's Notes, Appendix C

21. **Recommendation:** *Survey district coordinators to determine if modifying the Terminal Security Violations Report would enhance the reports usefulness and meet coordinator needs.*

Response: A survey of district TTSS coordinators could be developed to determine if any modifications are needed to enhance the TTSS Violations Report.

22. **Recommendation:** *Require security coordinators at local social services districts to follow up promptly on all sensitive or extensive violations and to determine whether corrective action is necessary.*

Response: See response to recommendation 2.

23. **Recommendation:** *Verify that all designated recipients are actually receiving the Terminal Security Violations Report and that required follow-ups are being performed.*

Response: These reports are E-mailed on a regular basis to districts' security coordinators.

24. **Recommendation:** *Develop and distribute guidance to TTSS coordinators at local social services districts on the use of the Terminal Security Violations Report and inquiry functions.*

Response: See response to recommendation 2.

25. **Recommendation:** *Extend the ISO training module to all 58 local social services districts.*

Response: OTDA will consider the feasibility of extending this training when it is available.

26. **Recommendation:** *Require local social services districts to provide all local users with security awareness training and guidance. Training should include the GAO standards for computer security as described in this report.*

Response: See response to recommendation 2.

27. **Recommendation:** *Require local social services districts to adopt security policies and procedures and communicate them to users.*

Response: See response to recommendation 2.

28. **Recommendation:** *Revise the TTSS manual to cover control objectives such as guidance on implementing controls, separation of duties, monitoring reports and their intended use, and security awareness procedures.*

Response: This was provided in the past. OTDA will work with OFT to assess if this needs to be brought up to date.

29. **Recommendation:** *Verify that case reviews by district supervisors include the matching of selected data with those in source documents, identification of deficient areas, and development of corrective action plans for addressing the deficient areas.*

Response: We are considering ways to implement this recommendation.

30. **Recommendation:** *Verify that districts correct the errors we found during our case file review.*

Response: We will do this.

31. **Recommendation:** *Re-convey to each district the importance of a valid Social Security number, the value of the WINR5126 report, and the need for timely resolution of Social Security number validation failures.*

*
Note
5

*
Note
10

*
Note
5

*
Note
5

*
Note
5

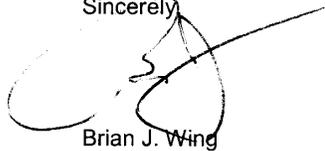
Response: On September 30, 2002, OTDA issued informational letter 02 INF 29 to the districts re-conveying the importance of valid Social Security numbers in the WMS.

32. **Recommendation:** *Analyze WINR5126 report statistics to identify districts that appear to have an unusually high number of Social Security numbers not validated by the SSA. Follow up with districts to determine the cause.*

Response: We will consider how best to implement this recommendation.

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,

A handwritten signature in black ink, appearing to read "Brian J. Wing". The signature is fluid and cursive, with a long horizontal stroke extending to the right.

Brian J. Wing

Attachment

William P. Challice
Audit Director
NYS Office of the State Comptroller
110 State Street
Albany, NY 12236

**Office of Temporary and Disability Assistance
Counsel's Office**

Brian J. Wing
Commissioner

John E. Robitzek
General Counsel

Memorandum

To: Dorpfeld, David
From: DAVID KELLOGG
cc: Deborah Snyder, Bob Mastro, Thomas Ryan, Gary Adams
Date: October 28, 2002
Subject: OTDA's Authority to Mandate Welfare Management Systems (WMS) Procedures on local social services districts (LSSDs)

CONFIDENTIAL ATTORNEY WORK PRODUCT

You have requested that I review and comment on the opinion of 8/26/02 by Albert Brooks and Patricia Sutter of the OSC's Counsel's Office which held that this Office has the responsibility to 1) monitor and supervise LSSD administration of WMS and 2) "ensure the confidentiality of the data collected as part of its oversight function". Although the conclusions in the memo standing alone are not particularly problematic, my perception is that the memo is being interpreted to mean that the Department has greater power over LSSD data collection and utilization in conjunction with WMS than over work of LSSDs generally, an interpretation that leaves me with substantial reservations.

Clearly both the Department and local social services districts have an obligation to keep social services data confidential in accordance with Section 136 of the Social Services Law and other applicable provisions of law. However, the reference to confidentiality in SSL 21.3 clearly is nothing more than a reiteration of what exists in SSL 136; there is absolutely no reference in that paragraph to the administrative relationship between the State and LSSDs. It is paragraph two of Section 21 which provides the most support for the idea that the Department has a greater responsibility for supervising confidentiality of WMS data than exists in the context of its general supervisory powers. Specifically, the Department is given authority to "promulgate regulations, specifying the types of information to be collected and transmitted ... the methods for collection and transmission of such data ... and the procedures for utilization of such data by [LSSDs]" in regard to WMS. The regulations promulgated by the Department in response to that language are found at 18 NYCRR 655; they contain no charge supporting the concept that districts have a higher duty regarding WMS data than they do with regard to data generally. Moreover, since, with minor exceptions not herein relevant, LSSDs are the source of WMS data, provision for such higher security standards would be logically contraindicated.

An examination of the structure of SSL 21 and the milieu in which it was passed supports the idea that the Department's determination not to promulgate confidentiality standards and procedures in 18 NYCRR 655 was consistent with legislative intent. A perusal of Section 21 as a whole makes it clear that the Legislature had as a primary focus the idea that WMS was to assist local districts in their extant duty to administer public assistance and care. Paragraphs two and five of the original Section 21 very specifically focused on local concerns and made clear a legislative determination that WMS must not result in additional financial burdens in the form of administrative costs be foisted on LSSDs. WMS was to be a statewide registry that assisted the then State Department of Social Services in supervising LSSDs by putting information formerly resident only in LSSD hands into a database directly accessible by the State; that such an intention and the implementation thereof should result in a greater confidentiality burden being placed on LSSDs was not something the Department could justify in 1980 when Part 655 was promulgated and, in fact, still cannot be justified.

State Comptroller's Notes

1. Contrary to OTDA's response, we did consider both their verbal and written comments regarding our preliminary findings, when we prepared the draft report. We intentionally did not disclose details of security weaknesses we considered sensitive, and as such, we did not disclose certain comments or facts provided by OTDA officials. Disclosing those facts would have presented a potential security risk by providing readers with valuable system information.
2. The GAO designed the material used during this audit to provide guidance to auditors on the scope of issues that generally should be considered in any review of computer-related controls over the integrity, confidentiality, and availability of computerized data. We agree that information security and the technical mechanisms in place to ensure it, must be designed to fit the environment and business needs. Our audit used both GAO guidance and general industry standard/practices to identify opportunities for OTDA, OFT, and local districts to improve their existing control structure.
3. The preliminary copies of the matters contained in this report were provided to OTDA officials, and were not redacted.
4. We reviewed the HSN LAN Administrator Manual and the TTSS Security Coordinator's Reference Manual and found that the manuals do not describe specific responsibilities rather they only describe generic responsibilities (i.e., "Network Security is responsible for all aspects of TTSS"). Local LAN administrator responsibilities are also not discussed in these manuals.
5. 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.
6. OTDA did not provide us with an extract of the OTDA Business Continuity Plan to substantiate the fact that a data center/mainframe disaster recovery plan exists. In December 2002, OFT drafted an interim disaster recovery plan that indicates, in the event of an emergency, they will follow the recovery procedures prescribed by the customer agency (OTDA) to restore that agency's processing. However, OFT reported that OTDA has not provided recovery procedures for WMS.
7. As cited in our audit (Security of the CONNECTIONS System Supporting Child Welfare Services, Report 2001-S-51, issued March 6, 2002), security features should be customized on the basis of need and environment. However, OFT officials did not explain how their security settings are based on need and

environment. They provided no specific explanations indicating why their security settings had to be changed from the settings recommended by the technical reference manual. Given their sensitive nature, we cannot disclose the details relating to these settings but have discussed them with appropriate OTDA and OFT officials.

8. We discussed, with agency officials, our concern regarding remote access. Based on our closing conference, we believed that OTDA and OFT understood our position. Details regarding remote access were redacted from this report.
9. We indicated the report is available on request. OTDA officials did not indicate in their response if they will require that security coordinators review the Authorized Functions Reports to verify the appropriateness of the individuals and functions listed.
10. As stated in the report, we found that not all districts receive the Terminal Security Violations Report. For example, Ulster County was not receiving the report because the person OFT electronically mailed it to did not have a computer to receive it. That is why we recommended that OTDA officials verify that recipients actually received the report. OTDA officials did not respond to our recommendation to verify receipt of this report.