Thomas P. DiNapoli
COMPTROLLER

OFFICE OF THE
NEW YORK STATE COMPTROLLER

DIVISION OF STATE
GOVERNMENT ACCOUNTABILITY

OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE

SECURITY OVER PERSONAL INFORMATION

Report 2007-S-78

AUDIT OBJECTIVES

The objectives of our performance audit were to determine whether the Office of Temporary and Disability Assistance (Office) is collecting and maintaining personal information on citizens only to the extent necessary to perform its mission, taking appropriate steps to minimize the risk of unauthorized access to or disclosure of personal information, and prepared to follow statutory requirements should that personal information be breached.

AUDIT RESULTS - SUMMARY

We found that the Office is collecting from the public only personal information that is needed to perform its mission, and has generally taken appropriate steps to ensure the security of that information, especially within its own offices. We also found that the Office is prepared to follow statutory requirements should it become aware that personal information in its possession has been breached.

We reviewed the Office's policies and procedures regarding information security for conformity to the provisions of the State's Cyber Security Policy, as well as other State and Federal laws the Office must comply with. We also observed selected units and local departments of social services (Districts) to assess the overall security awareness among Office and District employees and to determine whether policies and procedures were being followed. Overall, we found that employees of the Office have a higher level of security awareness than do employees of the Districts. The Office needs to do more to ensure that the Districts are taking appropriate steps to keep personal information in Office systems secure. We also found that documents containing personal information are not always kept secure by the Districts.

We reviewed the Office's policies and procedures to determine whether they comply with the Information Security Breach and Notification Act. We also reviewed incidents investigated by the Office. We found that the Office is prepared to follow statutory requirements should personal information in its systems be breached, but may not be able to identify when a breach has occurred at the District level. We also found that Office officials responded appropriately to the single breach they were aware of, including notifying the appropriate parties.

Our report contains six recommendations that the Office should implement to improve its security over personal information.

This report, dated March 27, 2008, is available on our website at: http://www.osc.state.ny.us.
Add or update your mailing list address by contacting us at: (518) 474-3271 or
Office of the State Comptroller
Division of State Government Accountability
110 State Street, 11th Floor
Albany, NY 12236

BACKGROUND

The Office is responsible for supervising programs that provide assistance and support to eligible families and individuals. Staffed by about 2,500 employees, the Office's functions include: providing temporary cash assistance; providing assistance in paying for food; providing heating assistance; overseeing New York State's child support enforcement program; determining certain aspects of eligibility for Social Security disability

benefits; supervising homeless housing and services programs; and providing assistance to certain immigrant populations.

The Office provides direct operational support, supervision, and guidance to the State's local departments of social services (Districts), which are responsible for directly administering most welfare programs. The Districts have approximately 20,000 employees who work with individuals to provide appropriate public assistance services that meet their needs.

In recent years, there have been heightened concerns about identity theft and other criminal misuse of personal information. There have even been some high-profile reports about personal information going astray. But there has not been any systematic review of efforts by State agencies to determine whether New York State residents are at risk of their personal information being misused. Therefore, we have initiated a series of audits of selected State agencies, including the Office, to review and evaluate the security safeguards over personal information they have collected from the public.

For the purposes of this audit, we used the definition of personal information from Article 6-A of the Public Officers Law (also known as the Personal Privacy Protection Law), which was enacted on September 1, 1984. According to the Personal Privacy Protection Law, personal information refers to any information collected by a State agency that can be used to identify a natural person.

AUDIT FINDINGS AND RECOMMENDATIONS

Collection of Personal Information

According to Section 94(1) of the Personal Privacy Protection Law, a State agency should collect only personal information that is needed to accomplish that agency's mission or an authorized program. When collecting personal information, the agency must provide an explanation of why the information is needed, including the purpose for which it will be used and the statutory authority under which it is collected.

The Districts collect personal information from applicants, which is then stored in computer systems managed for the Office by the New York State Office for Technology (OFT). The Districts use this information to administer Statewide social services programs. The Office oversees this system to fulfill its mission to "promote greater self-sufficiency of the State's residents through the efficient delivery of temporary and transitional assistance, disability assistance, and the collection of child support." We reviewed the various forms available on the Office's website and found that applicants for programs the Office oversees must provide the following personal information to the Districts: name, address, telephone number, Social Security number, date of birth, bank account number, and relationship to the applicant (for other individuals who are on the form). However, several different forms are used by the Districts, and not all of these data elements appear on every form.

The most common form used by applicants for various programs administered by the Office includes a "Privacy Act Statement." According to this Statement, collection of each of these data elements by the Districts is necessary for both District and Office purposes, such as determining whether the household is eligible for assistance, monitoring compliance with program regulations, and program management. The statement also references the Federal statutes that require the collection of Social Security numbers.

Based on our review of personal information provided by the public to the Districts and entered in the Office's systems, the Office needs to have this personal information to fulfill its mission. Therefore, we found that the Districts are collecting, on the Office's behalf, only personal information for which the Office has both a business need and a statutory authority.

Security over Personal Information

Section 94 (1) of the Personal Privacy Protection Law requires State agencies to establish appropriate administrative, technical, and physical safeguards to protect personal information in their possession, though it does not define what is considered "appropriate." The New York State Office of Cyber Security and Critical Infrastructure Coordination's (CSCIC) Cyber Security Policy P03-002: Information Security Policies (revised in December 2005) provides specific information security policy requirements State agencies should implement. Compliance with this policy is mandatory for all State agencies. Any individual who has access to or manages a State agency's information also must comply with this policy.

We evaluated the Office's policies and procedures regarding information security against the provisions of the CSCIC Information Security Policies, the New York State Personal Privacy Protection Law, and the New York State Technology Law. We also included key provisions from other State laws the Office must comply with, such as the New York State Social Services Law. Other than one provision for which CSCIC has not yet issued final standards, we found the Office is in compliance with the CSCIC Information Security Policies and State law requirements we identified as key.

According to Office officials, the two largest systems of records the Office maintains are:

- Welfare Management System (WMS): This system contains information about clients who are receiving social services, such as temporary assistance, food stamps, and Medicaid.

- Child Support Management System (CSMS): This system contains information about clients who are receiving child support services, such as determination of paternity, payment of child support, and search for non-custodial parents.

Individuals applying for social services programs complete an application form and submit supporting documentation. Based on the information submitted, the Districts determine the appropriate services to provide to each applicant. Information from the form is entered into the appropriate system (WMS or CSMS) by District employees. The Districts retain the application form and supporting documentation, and use the information in WMS and CSMS to provide customer services and support. The Office uses the information in these systems to monitor work done by the Districts, but generally does not access individual records.

We conducted interviews and made observations of two Office units and at four Districts (Monroe, Onondaga, Schoharie, and Ulster) to determine the level of security awareness among Office and District employees who use these systems regularly. We focused on areas of high risk for potential security vulnerabilities.

Overall Security Awareness

Overall, we found that employees of the Office have a higher level of security

awareness than do employees of the Districts. At the Districts, application forms and supporting documentation from clients were kept very secure, while documents generated by District employees during the course of the day were less secure.

The Office has developed an online security awareness training that complies with the CSCIC Information Security Policies requirements. Office employees are required to take this training and the Office's Information Security Office tracks to ensure the training is completed. The Office has made this training available to the Districts, but does not require them to use it or even to demonstrate that any security awareness training that complies with CSCIC Information Security Policies requirements is provided to District employees and others with access to personal information. Office officials indicated that their training was intended for Office employees. The Districts, on the other hand, process information for several State agencies and so may have additional security requirements not covered in the Office-developed training. Therefore, Office officials are waiting for CSCIC to provide security awareness training guidelines that could be applied to the District employees. In the interim, according to Office officials, Office staff have covered basic security awareness at conferences for District staff sponsored by OFT.

Access to Office Systems

Office employees, District employees, employees of other State agencies, and contractors have access to information in the Office's systems. To access WMS or CSMS, an individual must have a user ID and a password. User accounts and the level of access to system information are assigned based on job functions provided by the individual's supervisor. The Office has Transaction Terminal Security System (TTSS) Coordinators, who create and manage user accounts for Office employees and contractors. The Districts also have TTSS Coordinators, who handle this function for District employees and contractors. TTSS Coordinators at the Districts work with District managers to ensure that only authorized individuals have access to WMS and CSMS and only to the extent needed to perform their assigned duties.

According to Office officials, TTSS Coordinators are provided with training, manuals, and reference materials. However, one of the TTSS Coordinators at Ulster County with whom we spoke was unaware of these resources. This individual specifically named one reference guide as having no information, even though this guide has an entire chapter on the Transaction Terminal Security System. Therefore, it appears that TTSS Coordinators may not be aware of all available resources and so may not be handling their functions as efficiently and effectively as possible.

One of the security monitoring tools the Office has available for Districts is the Transaction Terminal Security System Violations Report (Report). The Report is generated by OFT, based on parameters specified by the Office. It is provided to the TTSS Coordinators and lists various violations that may indicate unauthorized attempts to access WMS or CSMS that occurred during the previous week, such as invalid user IDs or wrong passwords entered. The TTSS Coordinators are expected to review the report and investigate the violations, taking appropriate actions, if necessary. A cover letter accompanying the Report briefly describes each type of violation on the Report and outlines what should be done. This cover letter, which was developed by the Office, does not provide specifics on

how to investigate and resolve violations. For example, the cover letter states that incorrect passwords are usually the results of typos, but that repeated occurrences should be reviewed promptly. The cover letter does not specify how many repeat occurrences are required before the TTSS Coordinator should review them, what constitutes "prompt" review, or what specific steps the TTSS Coordinator should take during their review. According to Office officials, it is difficult to provide more detailed instructions because the actions needed to resolve an exception depend to a large extent on the situation.

Neither the Office nor the Districts monitor the District TTSS Coordinators to ensure they are receiving and reviewing the Report. At Ulster County, the Report was not going to the appropriate person. The person who received the Report did not review it and the person who was supposed to receive the Report did not notify the Office that she had not received it. This situation went on for several months, during which time it was assumed the TTSS Coordinator was using the Report to monitor the unauthorized access attempts of WMS and CSMS.

Physical Safeguards over Personal Information

In general, application forms and supporting documentation from clients are kept very secure, while documents generated by District employees during the course of the day are kept less secure. At one District office, we found documents containing personal information were piled near a printer in the client-intake area. Clients are required to be escorted when in the building, but could still read information since the documents were face-up and had no cover sheet. The Office did indicate that it will issue a directive reminding local District agencies of the mandates regarding the need to safeguard and assure proper handling and disposal of personal information in all forms.

At another District office, there is a contractor who assists Medicaid clients in selecting an HMO. Employees of this contractor, who have their own work area within the District office, have access to WMS. Their work area is set apart with clear glass panels. As a result, their computer screens are visible to anyone entering the building or otherwise walking by the contractor's work area. This contractor works for the Department of Health, not the Office. However, the Office should ensure that Districts are aware of and are following all appropriate safeguards over WMS and CSMS, including physical safeguards such as locating terminal screens to prevent unauthorized people from accessing information.

Office officials stated that they conduct regular site visits of all Districts to evaluate the safeguards in place over CSMS, as the Federal government requires. However, there are currently no regular site visits of these same Districts to evaluate the safeguards in place over WMS. In many Districts, both systems are located in the same building, often accessed by the same people. Many of the safeguards in place apply to both systems. Therefore, the Office could expand the scope of its evaluations to include both CSMS and WMS without significant additional effort.

Office officials stated they intend to issue a directive reminding Districts of legislative and regulatory requirements for the safeguarding of personal information in all forms. As part of this directive, the Office intends to require each District to complete a self-assessment of its information security safeguards. The self-assessment would then be returned to the Office, along with any corrective action plans the District identifies during the course of completing the self-

assessment. Such information could be used by the Office to plan its site visits, but does not negate the need for the Office to visit each District regularly to ensure that information is kept secure.

Disposal of Records Containing Personal Information

The Office does not delete inactive information in WMS and CSMS. Instead, electronic records are coded as inactive and archived. Office policy calls for documents with personal information in them to be disposed of appropriately. For hardcopy records, the employee may shred the document or place it in a confidential bin to be shredded by a vendor. This applies to both records from case files (Districts only) and documents generated during the course of the workday (Districts and Office). However, we found that one of the areas at one District office placed all documents generated during the course of the workday in a recyclable paper bin, without any review to identify those that contain personal information. We also found confidential bins that were not locked at two District offices.

Oversight of District Practices

The Office is required to ensure the security of information in its systems, under both the Personal Privacy Protection Law and CSCIC Information Security Policies requirements. In addition, Section 21 of the Social Services Law grants the Office the authority to promulgate regulations specifying the types of information to be collected and transmitted by each District to the Office, the methods for collection and transmittal of such information, and the procedures for Districts' utilization of the data maintained by WMS. The Office may impose penalties for noncompliance with its regulations. The Office has issued general guidance on information security to Districts, but not specific regulations that must be followed.

According to Office officials, WMS and CSMS belong to OFT (which manages these systems on behalf of the Office), while the information therein belongs to the Districts. Since the information does not belong to a State agency, the Office does not believe that CSCIC Information Security Policies requirements apply to the Districts. Thus, for example, the Office can require security awareness training of the Districts, but cannot require that the training complies with CSCIC Information Security Policies requirements.

We agree that the Office and the Districts share responsibility for security over personal information. However, we found a lower level of security awareness at the Districts when compared with the Office. Therefore, the Office needs to take a more active role regarding the security over personal information, ensuring that the Districts are taking appropriate steps to provide such security. When the Office finds a District that has not done so, the Office should take action against that District, including imposing administrative penalties, if necessary, to ensure compliance.

Response to Security Breaches

In December 2005, Section 208 of the New York State Technology Law went into effect. Also known as Information Security Breach and Notification Act (Act), it requires a State agency to notify an individual when private information either has been or is reasonably believed to have been acquired by someone who is not authorized to be provided with that information. If the private information was encrypted, notification is only required if the encryption key was also acquired. The State agency must also notify the Attorney General's Office, the Consumer Protection Board, and the Office of Cyber Security and

Critical Infrastructure. If more than 5,000 State residents are affected, the State agency must also notify the consumer reporting agencies.

The Act defines private information as personal information in conjunction with Social Security number, driver license, or non-driver ID number. Personal information in conjunction with a bank account or credit card or debit card number is considered private information only if there is also a security code, access code, or password that would allow access to the individual's financial account.

The Office's Information Security Office has developed appropriate breach procedures that include all notification and reporting requirements from the Act. Since the Act went into effect, the Office has identified one reportable breach under the provisions of the Act. The Office notified the individuals involved, as well as the Attorney General's Office, the Consumer Protection Board, the Office of Cyber Security and Critical Infrastructure Coordination, and (because more than 5,000 State residents were potentially affected) the consumer reporting agencies. Based on our review, the breach was handled appropriately.

To identify occasions when a breach has occurred, the Office and the Districts need to monitor their systems, including WMS and CSMS, for unauthorized access. As discussed, the TTSS Coordinators at the Districts have been provided with the Transaction Terminal Security System Violations Report (Report) as one tool for monitoring access to these systems and identifying potential unauthorized access. However, we found that the TTSS Coordinators at the District appear to be uncertain how to use the Report and do not always review the Report. In addition, they may be unaware of the resources the Office and OFT make available to them. As a result, it is possible for a breach to occur at a District that the Office or the District does not learn about. In such instances, the Office or the District would not be able to investigate and resolve the breach, including notifying affected individuals. The Office and the Districts should work together to ensure that all TTSS Coordinators are aware of their responsibilities and of the resources available to help them.

Recommendations

1. Require all individuals (including District employees and contractors) with access to Office systems, such as WMS and CSMS, to complete the Office's security awareness training or demonstrate completion of equivalent training that complies with CSCIC Policy P03-002.

   (Office officials acknowledge their authority to impose policies and procedures on local Districts, but contend they cannot prescriptively impose the form that information security training must take. Still, officials agreed to include an information security training requirement as a component of a policy directive to local Districts.)

2. Ensure that all TTSS Coordinators are aware of all training, reference materials, and other resources provided by the OFT to assist in keeping personal information secure.

3. Provide more detailed guidance to TTSS Coordinators regarding the use of the Terminal Security Violations Report, including what steps should be taken to investigate potential violations.

(Office officials generally agreed with recommendations 2 and 3 and plan to work with OFT to develop ways to remind TTSS Coordinators of the resources available to them and to provide additional training and guidance where warranted.)

4. Monitor TTSS Coordinators to ensure they are reviewing the Terminal Security Violations Report properly and investigating potential violations.

5. Make regular visits to the Districts to evaluate the physical, administrative, and technical safeguards in place for WMS, as is done for CSMS.

   (Officials generally disagreed with recommendations 4 and 5, stating that routine monitoring and evaluation of information security procedures in the Districts would be burdensome to support. Instead, the Office plans to issue a directive requiring that all Districts perform routine self-assessments and develop corrective action plans.)

   Auditor's Comment: The Office already conducts regular visits to each District to evaluate safeguards in place over CSMS data. Since CSMS and WMS data are frequently used by the same people at the District level, it would seem that expanding these reviews to include WMS data would be less burdensome than the Office's plan to require all Districts to complete self-assessments and corrective action plans.

6. Impose administrative penalties against Districts that do not take appropriate steps to ensure that personal information is secure.

   (Office officials acknowledged their authority to impose penalties and discussed several alternatives available to them. However, their response does not indicate which, if any, of these penalties they plan to employ should Districts fail to adequately safeguard personal information.)

AUDIT SCOPE AND METHODOLOGY

We conducted our performance audit in accordance with generally accepted government auditing standards. We audited the collection and maintenance of personal information obtained from the public by the Office. Our audit covers the period December 7, 2005, through June 8, 2007.

To accomplish our audit objectives, we reviewed applicable State and federal laws and regulations regarding the collection of and security over personal information by the Office, including statutory requirements when such information is breached. We interviewed Office officials and staff to determine the policies and procedures in place, as well as to understand how information flows through the Office. We reviewed the Office's policies and procedures to determine whether they met minimum statutory requirements related to information security. We observed two Office units and four Districts (Monroe, Onondaga, Schoharie, and Ulster) to determine whether these policies and procedures were being followed and to assess the overall security awareness among Office and District employees. We also obtained information on the Office's data classification and risk assessment efforts. We reviewed information on a past breach involving personal information to evaluate the Office's handling of such an incident.

In addition to being the State Auditor, the Comptroller performs certain other

constitutionally and statutorily mandated duties as the chief fiscal officer of New York State. These include operating the State's accounting system; preparing the State's financial statements; and approving State contracts, refunds, and other payments. In addition, the Comptroller appoints members to certain boards, commissions and public authorities, some of who have minority voting rights. These duties may be considered management functions for purposes of evaluating organizational independence under generally accepted government auditing standards. In our opinion, these functions do not affect our ability to conduct independent audits of program performance.

AUTHORITY

The audit was performed 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.

REPORTING REQUIREMENTS

Draft copies of this report were provided to Office officials for their review and comment. Their comments were considered in preparing this report, and are attached as Appendix A. Our rejoinders to the Office's comments are presented in Appendix B.

Within 90 days of 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 the leaders of the Legislature and fiscal committees, advising what steps were taken to implement the recommendations contained herein, and if not implemented, the reasons therefor.

CONTRIBUTORS TO THE REPORT

Major contributors to this report include Frank Houston, John Buyce, Christine Rush, Jennifer Paperman, Laurie Burns, Andrea Dagastine, Sarah Purcell, and Andre Spar.

APPENDIX A - AUDITEE RESPONSE

NEW YORK STATE
OFFICE OF TEMPORARY AND DISABILITY ASSISTANCE
40 NORTH PEARL STREET
ALBANY, NEW YORK 12243-0001

Eliot Spitzer
Governor

David A. Hansell
Commissioner

February 12, 2008

Mr. Frank J. Houston
Audit Director
Office of the State Comptroller
Division of State Government Accountability
123 William Street – 21st Floor
New York, NY 10038

Re: Security Over Personal Information Draft Report #2007-S-78

Dear Mr. Houston:

As requested, the Office of Temporary and Disability Assistance (OTDA) has reviewed the above-mentioned draft audit report (2007-S-78) and offer the following responses and comments.

It is OTDA's view that our prior comments have not been incorporated accurately or fairly into this draft audit document. We are concerned that despite efforts to clarify certain issues during the course of the audit and discussion of preliminary drafts, this version continues to reflect considerable inaccuracies, and fails to recognize agency actions in key areas.

The following reflects our comments regarding factual inaccuracies and additional comments for your consideration in preparing the final report. Page and paragraph reference are provided for each comment.

Page 2 of 9 - right column, first full paragraph:

The Office does have the ability to identify breaches within their computer systems and ensure appropriate response and reporting per the State's Cyber Security Policy and Information Security Breach Notification Act. Information security incidents that occur at the District level involving non-compliance with physical security controls (i.e., handling of documents) are the responsibility of local district agency management. Local districts are responsible for addressing and reporting such incidents to the State, so that the District and State agency can coordinate the appropriate response plan. The fact, as noted in your findings, that Office officials responded appropriately to the single breach reported, including notifying the appropriate parties, rebuts your finding that the Office may not be able to identify when a breach has occurred at the District level.

* ***Comment 1***

Page 3 of 9 - left column, first paragraph, last sentence:

The Office has 2,500 employees, however the number that assist Districts in providing appropriate public services is less than 50.

* ***Comment 2***

"providing temporary assistance for permanent change"

* See State Comptroller's Comments, page 18

Page 3 of 9 - right column, first paragraph:

The information collected from applicants is stored in computer systems maintained by OTDA. The New York State Office for Technology (OFT) manages day-to-day data center operations, terminal security controls, etc.

* ***Comment 3***

Page 4 of 9 - left column, *Security over Personal Information*, second paragraph, last sentence:

As stated during the audit, and further articulated on page 4 of our June 27, 2007 response to the preliminary findings report, OTDA feels the agency is currently in compliance with existing State policy requirements.

During this audit, OSC used a checklist they compiled of the key provisions from the Cyber Security Policy and other State laws, such as the New York State Social Services Law, to evaluate Office policies and procedures.

The report states that the Office is in compliance with all but one item. The one item discussed was classification. As the Information Security Office (ISO) advised during the audit and in comments on the preliminary report, the Office currently classifies assets using the same classification schema as the OFT's data classification standard, which is based on National Institute of Standards and Technology (NIST) standards. Systems are currently classified and thus the Office is in compliance with NYS Policy. As further discussed, while the New York State Office of Cyber Security and Critical Infrastructure Coordination (CSCIC) has not issued final standards, the Office's Information Security Officer is a member of the classification standards workgroup, and reported that the final standards are expected to be based on/similar to the NIST standard. As a result, the Office should be able to adopt the CSCIC standard quickly once it becomes available, and comply with this new standard upon it being issued.

OTDA's Bureau of Information Technology (IT) maintains application inventory documentation that reflects the applicable OTDA Division ('information owner'), program area contact(s) and IT contact(s) ('information custodians') for each of the agency's applications. The agency has identified mission-critical and mission-supporting applications, as well as those that contain sensitive, and/or confidential/personal identifying information. It is anticipated that current classifications need to be reviewed once CSCIC classification standards are issued, however the Office should be fairly well aligned as they are also based on NIST, which will assure ongoing compliance. As further advised during the audit and subsequent discussions, work is underway to refine information related to confidentiality, integrity and availability in preparation. As further advised, OTDA also has Secure System Development Life Cycle protocols – an industry best practice, in place that include information classification as a required component in the security planning process for all new or redesigned systems. As also advised, IT recently implemented an Application Portfolio Management solution designed to improve upon the agency's ability to track and manage our application portfolio, serve as a repository for related documentation, and support categorization, classification review and reporting requirements.

Given the above factors, OTDA feels the agency is currently in compliance with State policy requirements.

Page 5 of 9 - left column, first paragraph, last sentence:

As stated during the audit, and further articulated on page 4 of our June 27, 2007 response to the preliminary findings report, OTDA's efforts have far exceeded conveying basic security awareness at conferences for District staff. OTDA has presented detailed training on proper security controls and practices for personal data as well as specific data sets – i.e., IRS data, federal social security and veteran information, unemployment benefits, employment data, etc., as well as process-related controls – i.e., the training delivered during the rollout of initiatives involving personal data – i.e., electronic document imaging. The Office has also taken the lead in providing information security presentations at statewide

* See State Comptroller's Comments, page 18

regional meetings, New York Public Welfare Association Conferences, annual statewide LAN Administrators Conferences, as well as New York State Cyber Security Conference and Government Technology Conferences, which are attended by State and local agencies. OTDA ISO materials and resources have been distributed at these forums and provided to District staff development coordinators for use in their districts. OTDA's numerous and comprehensive security awareness activities clearly establish that the agency has been extremely proactive in its efforts to convey the importance of information security and safeguarding personal information.

* Comment 4

While OTDA's Information Security Awareness Training (ISAT) online course has been available to local districts since 2006, OTDA cannot prescriptively impose the form information security training must take - i.e., requiring that Districts must specifically take OTDA's ISAT workforce training course. The Office maintains that overall District workforce training requirements would be better met by the planned, more generic CSCIC information security workforce training. Further, it would be difficult if not impossible for a single State agency to enforce such a training mandate, and would place the burden of delivering and assuring District security awareness training on one State agency, when in fact it should be the shared responsibility of the Districts and several State human service agencies (CSCIC, Department of Labor, Department of Health, Office of Children and Family Services, etc.).

* Comment 5

Page 5 of 9 - right column, second paragraph:

While this may have been conveyed by one individual, as stated by OTDA during the audit, and further articulated on page 7-9 of our June 27, 2007 response to the preliminary findings report, OTDA continues to maintain that this information is not accurate and that this finding based on a conversation with just one individual lacks validity.

* Comment 6

Transaction Terminal Security System (TTSS) administration and account management-related direction and training has been routinely provided to TTSS Coordinators by OFT and OTDA in several forms including: system messages, policy directives, LAN ADMINISTRATOR CONFERENCES, training related to implementation rollouts, and Customer Relations Communications regarding Webstar TTSS enhancements (i.e., OFT CRC 082, issued March 16, 2006, regarding the TTSS Application/Function/Transaction Reference (AFTR) tool). As further advised in the TTSS Report cover letters, assistance regarding the contents and use of the report is available from OFT TTSS. District TTSS Coordinators routinely seek and are provided with assistance on TTSS- related questions from knowledgeable and readily available OFT TTSS and Customer Relations staff, and from OTDA program area and Welfare Management System (WMS) Help Desk staff.

The HSEN LAN Administrator's Support Guide contains a 17-page section - Chapter 7: TTSS Legacy, which specifically covers the TTSS, provides detailed information on what it is, instructions as to how it works, and contact information for questions and assistance. It is a known resource that has been well circulated and referenced by both OFT and OTDA, and is readily available/accessible accessible online, and downloadable from the OFT Customer Relations web site. It also contains a specific section entitled *'What if you need help?'* on page 7-17 that directs the reader to the TTSS User Reference book available in hard copy, and electronically in the public folder set up for Legacy TTSS/Coordinators Only/Manual. It further provides an OFT email address and postal address for questions and inquiries regarding TTSS.

Page 5 of 9 - right column, second paragraph:

As stated during the audit, and further articulated in detail on page 8 of our June 27, 2007 response to the preliminary findings report, OTDA disagrees with the statement that the cover letter is not sufficiently detailed as to how to handle the violations reported. OTDA agency ISO and program area representatives have reviewed the instructions in the TTSS Violations Report cover letter and have confirmed that it contains sufficient explanation of each type of violation and actions that should be taken where appropriate. The existing instructions provide sufficient guidance. This said, the report should reflect that the Office has agreed to work with OFT to support further training for TTSS Coordinators on TTSS, reports and resources.

* Comment 7

* See State Comptroller's Comments, page 18

Page 6 of 9 - left column, second paragraph:

As stated during the audit, and further articulated in detail on page 9 of our June 27, 2007 response to the preliminary findings report, review of OFT TTSS has report production and tracking protocols in place, and validated that Violations Reports were consistently being produced and sent to Ulster County TTSS Coordinators.

District Commissioners are responsible for ensuring that their TTSS Coordinators are properly performing their job duties, and that the Office is promptly advised when changes in TTSS Coordinator assignment/duties occur. OFT has annual TTSS Coordinator recertification procedures in place to assure any non-reported changes are identified, reported and resolved.

Page 6 of 9 - right column, second paragraph, last sentence, and third paragraph, last sentence:

As stated during the audit, and further articulated in our June 27, 2007 response to the preliminary findings report routine evaluations would be burdensome to support through site visits. The Office agreed to issue a directive reminding Districts of the legislative and regulatory requirements pertaining to safeguarding personal information, and an accompanying self-assessment document which would be returned to the office for review.

* ***Comment 8***

Page 7 of 9 - left column, first paragraph, last two sentences:

As stated during the audit, and further articulated in our June 27, 2007 response to the preliminary findings report, local Districts are responsible for assuring proper procedures are followed in disposing of their case record documents containing personal information. OTDA will include secure disposal requirements in the planned directive reminding local district agencies of the mandates regarding the need to safeguard and assure proper handling and disposal of sensitive and/or confidential/personal identifying information.

Page 7 of 9 - left column, last paragraph, which continues into right column:

As stated during the audit, and further articulated in our June 27, 2007 response to the preliminary findings report, this information is not accurate. According to Office officials, WMS and CSMS are OTDA computer systems maintained by OTDA. OFT manages day-to-day data center operations and terminal security controls for these and other OTDA systems.

OTDA's position that the Office cannot mandate that local districts take the OTDA ISAT online course is not based on the fact that the information is related to Local District cases. OTDA's ISAT course has been available to local districts since 2006, and has been supplemented by information security presentations at statewide regional meetings, New York Public Welfare Association Conferences, annual statewide LAN Administrators Conferences, and New York State Cyber Security Conference and Government Technology Conferences, which are attended by State and local agencies. However, OTDA cannot prescriptively impose the form security training must take. The Office maintains that overall District workforce training requirements would be better met by the planned, more generic CSCIC information security workforce training. As noted in the draft report, the Districts process information for several State agencies and so may have additional security requirements not covered in the Office-developed training. Further, it would be difficult if not impossible, for a single State agency to enforce such a training mandate, and would place the burden of delivering and assuring District security awareness training on one State agency, when in fact it should be the shared responsibility of the districts and several State human service agencies (CSCIC, Department of Labor, Department of Health, Office of Children and Family Services, etc.).

* ***Comment 5***

* See State Comptroller's Comments, page 18

Page 7 of 9 - right column, second paragraph, last sentence:

As stated during the audit, and further articulated in our June 27, 2007 response to the preliminary findings report, OTDA has administrative authority, and can and does exercise its authority to impose policies and procedures on districts, including mandates for security over personal information maintained at state and local levels. The Office provides training and monitors staff to ensure that confidential/personal identifying information is properly safeguarded.

OTDA can withhold or deny state reimbursement to local district or withhold a portion of the federal block grant for noncompliance with agency security mandates. The state has the authority to impose requirements as it deems appropriate in consideration of federal and state privacy and security requirements, and has the authority to take action against both districts and individuals who fail to comply.

OTDA has agreed to issue a directive reminding local district agencies of the mandates regarding the need to safeguard and assure proper handling and disposal of sensitive and/or confidential/personal identifying information in all forms. OTDA further agreed that an "Information Security Checklist" that addresses administrative, physical and technical controls would be provided as an attachment. Directions will be conveyed to use this checklist to perform routine self-assessments.

Page 8 of 9 - left column, final paragraph:

The statement that the Office needs to monitor their systems for unauthorized access conveys that the State is not meeting its requirement to do so. As stated during the audit, and further articulated in our June 27, 2007 response to the preliminary findings report, OFT and the Office monitor systems for unauthorized access and have multiple layers of security controls in place to monitor and identify when a breach occurs. In the event of a breach of the security of a system 'owned' or licensed by OTDA, the agency recognizes its duty to disclose and notify affected individuals, and has appropriate procedures in place to carry out its responsibilities.

Review of TTSS Violations Reports by TTSS Coordinators is only one of many layers of security controls in place to prevent and detect potential unauthorized access attempts to agency systems. System controls and reports, policies regarding accounts management, passwords, device and network controls and monitoring, database and data center security, and administrative and physical security controls all work in combination to safeguard data and prevent unauthorized access.

OTDA considers safeguarding confidential/personal identifying information in District case records as a shared responsibility of both the state and the local district. Since many types of incidents cannot be identified through technical controls, the Office must rely on District management to meet its responsibility to report breaches occurring within their environment to the State agency. Proper District oversight, account management and incident reporting are the most critical methods for preventing and identifying potential misuse, disclosure and/or unauthorized access to information assets. District management is responsible for assuring that their users adhere to security policies and procedures, and that user account and access permissions requests are based on an individual's job duties, adhere to the principle of "least privilege" and are modified/terminated when circumstances change. OTDA believes local district Commissioners and management fully understand the importance of and the need to promptly and properly report information security concerns to the State.

OTDA regards the statement (on page 9) indicating "TTSS Coordinators at the District appear to be uncertain how to use the report and do not always review the report" as too strong and sweeping, based on the fact that (as the auditors' state on page 5) it was not an actual finding, but rather what auditors were told by a single individual in one District who was receiving the reports but not performing their assigned duties. This said, the report should reflect that the Office has agreed to work with OFT to support further training for TTSS Coordinators on TTSS, reports and resources.

* Comment 6

* See State Comptroller's Comments, page 18

Our specific responses to the individual recommendations are as follows:

Recommendation 1:

Require all individuals (including District employees and contractors) with access to Office systems, such as WMS and CSMS, to complete the Office's security awareness training or demonstrate completion of equivalent training that complies with CSCIC Policy P03-002.

Response - Recommendation 1:

OTDA cannot prescriptively impose the form information security training must take (i.e., requiring that districts must specifically take OTDA's Information Security Awareness Training (ISAT) workforce training course). OTDA's ISAT online course has been available to local districts since 2006; however, OTDA maintains that overall District workforce training requirements are better met by the planned, equivalent CSCIC information security workforce training. Further, it would be difficult if not impossible, for a single State agency to enforce such a training mandate, and would place the burden of delivering and assuring District security awareness training solely on OTDA, when in fact it should be the shared responsibility of the districts and several other State human service agencies - CSCIC, Department of Labor, Department of Health, Office of Children and Family Services.

It is OTDA's position that per State policy, the responsibility to ensure District staff complete information security awareness training remains with the districts. OTDA will include this training requirement as a component of the State policy directive and information security self-assessment checklist the Office is preparing to issue to the local districts.

Recommendation 2:

Ensure that all TTSS Coordinators are aware of all training, reference materials, and other resources provided by the OFT to assist in keeping personal information secure.

Response - Recommendation 2:

OTDA will work with OFT to issue an OFT Customer Relations notice reminding TTSS Coordinators and WMS/CSMS Coordinators of OFT assistance, training, reports and resources available for TTSS Coordinators.

Recommendation 3:

Provide more detailed guidance to TTSS Coordinators regarding the use of the Terminal Security Violations Report, including what steps should be taken to investigate potential violations.

Response - Recommendation 3:

OTDA will work with OFT to conduct a review of existing guidance, and where deemed necessary provide further guidance for TTSS Coordinators on the use of the TTSS Violation Report.

Recommendation 4:

Monitor TTSS Coordinators to ensure they are properly reviewing the Terminal Security Violations Report and investigating potential violations.

Response - Recommendation 4:

OTDA will include this as a component of the State policy directive and information security self-assessment checklist the Office is preparing to issue to the local districts (see also response to Recommendation 5).

Recommendation 5:

Make regular visits to the Districts to evaluate the physical, administrative, and technical safeguards in place for WMS, as is done for CSMS.

Response - Recommendation 5:

As stated above and articulated in our June 27, 2007 response to the preliminary findings report, OTDA will issue a directive reminding local district agencies of the mandates regarding the need to safeguard and assure proper handling and disposal of sensitive and/or confidential/personal identifying information in all forms, along with an "Information Security Checklist" that addresses administrative, physical and technical controls. Directions will be conveyed regarding the use of this checklist by the districts to perform routine self-assessments. Districts that identify deficiencies in their procedures will be required to include corrective action plans in the completed checklist that they submit for OTDA's review and approval. OTDA staff will review the corrective action plans that districts submit when they self-assess as being noncompliant and will follow-up as deemed necessary.

Recommendation 6:

Impose administrative penalties against Districts that do not take appropriate steps to ensure that personal information is secure.

Response - Recommendation 6:

As stated during the audit and articulated in our June 27, 2007 response to the preliminary findings report, and further comments provided above, OTDA has administrative authority, and can and does exercise its authority to impose policies and procedures on districts, including mandates for security over personal information maintained at state and local levels, and the provision of training and monitoring of staff to ensure that confidential/personal identifying information is properly safeguarded. OTDA can withhold or deny state reimbursement to local district or withhold a portion of the federal block grant for noncompliance with agency security mandates. The state has the authority to impose requirements as it deems appropriate in consideration of federal and state privacy and security requirements, and has the authority to take action against both districts and individuals who fail to comply.

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,

James P. White, Director
Bureau of Audit and Quality Improvement

"providing temporary assistance for permanent change"

APPENDIX B - STATE COMPTROLLER COMMENTS ON AUDITEE RESPONSE

1. Our audit found that the Office is prepared to respond appropriately when it becomes aware of a breach. However, we also found there is less assurance that the Office will identify or otherwise become aware of all breaches, especially at the District level, in part because the staff, who are responsible for monitoring system access, do not always understand their roles and responsibilities in the process.

2. The final report has been modified to clarify agency staffing.

3. The final report has been modified to clarify the Office's role in managing the Office's systems.

4. Although Office officials view the agency's outreach efforts as proactive and having far exceeded what is needed to convey basic security awareness, many of the venues they cite (such as LAN Administrator and Government Technology conferences) are normally attended by technology professionals who should already be aware of basic security requirements. Our audit tests showed a lower level of security awareness by District staff who actually handle personal information on a daily basis, which we attributed at least in part to the fact that the Office does not require districts to demonstrate that all staff have received appropriate training.

5. We agree that the local Districts and the State agencies with which they work all share a responsibility to ensure that staff are appropriately trained to protect private information. We believe the Office should take the lead in this effort, since the fact that others may share the responsibility does not absolve the Office of its duty to ensure that its data is protected.

6. Office officials are correct that the finding is based on interviews with one District's TTSS Coordinator. However, this individual is the person whom the District assigned to be responsible for ensuring that access to both WMS and CSMS data is limited to authorized persons and for authorized purposes. The fact that a person in this position is unfamiliar with pertinent aspects of these responsibilities or the resources available for assistance is a serious risk that limits the Office's assurance that security breaches will be identified.

7. Our report already recognizes that Office officials find it difficult to provide more detailed instructions in the context of the cover letter accompanying the security violation report. We are pleased that OTDA has chosen to provide more training to TTSS coordinators as the means by which it will implement our recommendation to provide more detailed guidance on the use of the report and the investigation of potential violations.

8. Office officials state that it would be too burdensome to conduct routine monitoring of security safeguards at the District level. However, as our report indicates, the Office already conducts regular visits to each District to evaluate safeguards in place over CSMS data. Since CSMS and WMS data are frequently used by the same people at the District level, it would seem that expanding these reviews to include WMS data would be less burdensome than the Office's plan to require all Districts to complete self-assessments and corrective action plans.