Thomas P. DiNapoli
COMPTROLLER

OFFICE OF THE
NEW YORK STATE COMPTROLLER

DIVISION OF STATE
GOVERNMENT ACCOUNTABILITY

DEPARTMENT OF TAXATION AND FINANCE

SECURITY OVER PERSONAL INFORMATION

Report 2007-S-77

AUDIT OBJECTIVES

The primary objectives of our performance audit were to determine whether the Department of Taxation and Finance (Department) 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 personal information be breached.

AUDIT RESULTS - SUMMARY

We found that the Department is only collecting personal information from the public which is needed to perform its mission, and has taken appropriate steps to ensure the security of that information. We also found that the Department is prepared to follow statutory requirements should personal information in its possession be breached.

We reviewed the Department's mission statement, programs, and statutory authority to collect information. We also examined the forms used by the Department to collect personal information from the public. We found that the Department is only collecting personal information from the public needed to perform its mission.

We reviewed the Department'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 tax laws the Department must comply with. We also observed selected units to assess the overall security awareness among Department employees and to determine whether policies and procedures were being followed. We found that the Department has taken appropriate steps to ensure the security of personal information in its possession.

We reviewed the Department's policies and procedures to determine whether they comply with the Information Security Breach and Notification Act. We also reviewed potential breaches investigated by the Department. We found that the Department is prepared to follow statutory requirements should personal information in its possession be breached. In addition, the Department has responded appropriately to breaches, including notifying the appropriate parties.

This report, dated August 29, 2007, 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 Department administers the State's tax laws and serves as the State's general tax collection agency. The various taxes collected and administered by the Department include Corporation, Personal Income, Sales, and other miscellaneous taxes. Annually, the Department collects over $52 billion in State tax revenue and over $33 billion in local taxes on behalf of municipalities. The Department has a total workforce of nearly 5,000 employees, and an annual operating budget exceeding $435 million.

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. However, 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 Department, to review and evaluate their information security practices over personal information 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

Collection of Personal Information

According to Section 94(1) of the Personal Privacy Protection Law, a State agency should only collect 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 mission of the Department is to "collect tax revenue and provide associated services in support of government services in New York State." To this end, the Department receives income and other tax forms from individuals and businesses. We reviewed all tax forms available online and found that the Department collects the following elements of personal information from the public: name, address, telephone number, social security number, date of birth, and bank account number. Not every form requires every element, however.

According to the Department's "Index of Privacy Notifications," collection of each of these data elements is necessary to determine and administer tax liabilities and, when authorized by law, for certain tax offset and exchange of tax information programs. The Tax Law provides statutory authority to collect such information. We found that the Department is collecting only personal information for which it 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 (revised in December 2005) provides specific information security policy requirements State agencies should implement. Compliance with this policy is mandatory for all State agencies.

We evaluated the Department's policies and procedures regarding information security against the provisions of the Cyber Security Policy P03-002, as well as other State and federal tax laws the Department must comply with, such as the Taxpayer Browsing Protection Act and Article 9-A of the New York State Tax Law. Other than one provision for which CSCIC has not yet issued final standards, the Department is in compliance with the Cyber Security Policy P03-002 requirements we identified as key. The Department is also in compliance with State and federal tax laws intended to ensure

taxpayers' personal information is kept secure.

We conducted interviews and made observations to determine the level of security awareness among Department employees. We focused on areas of high risk for potential security vulnerabilities.

Intake

The Department receives tax information electronically only. Paper forms are submitted to a vendor, which scans the documents and provides the Department an electronic database of the information from the forms, as well as the scanned images. The electronic database is transferred directly to the Department's systems. The scanned images are sent to the Department via a courier. The original paper forms are shipped to a Department warehouse and secured. The vendor is required, by its contract, to ensure the security of personal information to the same level as the Department itself. The Department regularly audits compliance with contractual requirements, including information security, and has not found any violations by its vendor.

Storage and Access

Access to personal information - whether stored in hard copy or electronically - is restricted and assigned to employees based on position and unit needs. The hardcopy tax forms are kept in secure storage facilities, while scanned images and electronic data are stored on the Department's mainframe. According to the Department's security policy, access to information is granted on a strict need-to-know basis and unauthorized access to physical or computer tax files, access beyond the scope of an employee's assigned duties and responsibilities, or unauthorized disclosure of confidential information will subject an employee to disciplinary action and/or criminal prosecution. Employees are made aware of this policy and required to sign an "Agreement to Adhere to the Secrecy Provisions of the Tax Law and the Internal Revenue Code." The Department monitors access to electronic information by its employees daily and investigates anomalous behavior. The Department makes its information security policies and procedures available to all Department employees via its intranet. In addition, the Department reinforces the importance of security awareness through formal and informal training, plus a monthly security tip email sent to all employees. Based on our limited tests of general controls, Department employees are aware of and following appropriate procedures to ensure personal information is kept secure.

Disposal

The Department has retention schedules for tax forms in its possession, both hard copy and electronic. The retention schedules are based on requirements in the Tax Law. Documents in electronic format are simply deleted; documents in hardcopy are destroyed by an outsider vendor. The same outside vendor also handles disposal of documents generated by the Department during the normal course of business which contain personal information. Department employees we spoke with were aware of and were following the proper process for disposing of personal information.

Overall, we found that the Department has taken appropriate steps to ensure the security of personal information in its possession or that of its vendors.

Response to 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's license or non-driver's ID number. Personal information in conjunction with a bank account or credit card or debit card number is only considered private information if there is also a security code, access code or password which would allow access to the individual's financial account.

When the Act first went into effect, the Department's Office of the Deputy Inspector General was responsible for investigating breaches. There were no written procedures, though a process was established. The Department subsequently created the Information Security Office, which is now responsible for investigating breaches. The Information Security Office is in the process of developing written procedures. We reviewed the draft procedures and found they include all notification and reporting requirements from the Act.

Since the Act went into effect in December 2005, the Department has identified and fully investigated 15 breaches. Out of these 15 breaches, only four required notification under the provisions of the Act. In each of these four instances, the Department notified the individuals involved, as well as the Attorney General's Office, the Consumer Protection Board, and the Office of Cyber Security and Critical Infrastructure. None involved more than 5,000 State residents, so the Department was not required to notify the consumer reporting agencies. Based on our review of Department documentation, all 15 breaches were handled appropriately.

Overall, we found that the Department has established appropriate procedures for responding to breaches of personal information in its possession, and that New York State taxpayers and others who provide personal information to the Department will be informed should their personal information be breached.

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. Our audit covers the period December 7, 2005 through March 23, 2007.

To accomplish our audit objectives at the Department, we reviewed applicable State and federal laws and regulations regarding the collection of and security over personal information by the Department, including statutory requirements when such information is breached. We interviewed Department officials and staff to determine the policies and procedures in place, as well as to understand how information flows through the Department. We reviewed the

Department's policies and procedures to determine whether they met minimum statutory requirements related to information security. We observed selected units to determine whether these policies and procedures were being followed and to assess the overall security awareness among Department employees. We also obtained information on the Department's data classification and risk assessment efforts. We reviewed information on past breaches involving personal information to evaluate the Department's handling of such incidents.

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 Department officials for their review and comment. Their comments were considered in preparing this report and are attached as Appendix A.

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

STATE OF NEW YORK
DEPARTMENT OF TAXATION AND FINANCE
W.A. HARRIMAN CAMPUS
ALBANY, NY 12227

Barbara G. Billet
Acting Commissioner

July 24, 2007

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

Dear Mr. Houston:

Thank you for the opportunity to comment on the findings in your draft audit report, "Security over Personal Information, (2007-S-77)."

As a Department, we have always been serious in our commitment to collect only appropriate personal information from the taxpayers of the State of New York and to safeguard that information from unauthorized access or disclosure.

We are especially pleased with your findings that the Department only collects personal information from the public needed to fulfill our mission, and that we have taken the appropriate steps to ensure the security of that information. In addition, as noted in your report, the Department has policy and procedures in place that comply with statutory requirements should personal information in our possession be breached.

Sincerely,

Barbara G. Billet

Barbara G. Billet
Acting Commissioner