**Thomas P. DiNapoli**
**COMPTROLLER**



**OFFICE OF THE**
**NEW YORK STATE COMPTROLLER**

**DIVISION OF STATE**
**GOVERNMENT ACCOUNTABILITY**

# DEPARTMENT OF MOTOR VEHICLES

# SECURITY OVER PERSONAL INFORMATION

## Report 2007-S-79

## AUDIT OBJECTIVES

The objectives of our performance audit were to determine whether the Department of Motor Vehicles (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 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 Department must comply with. We also observed selected units and issuing offices to assess the overall security awareness among Department employees and to determine whether policies and procedures were being followed. With few exceptions, we found the Department has developed adequate policies and procedures 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.

Our report contains one recommendation to further strengthen the Department's security over personal information. Department officials indicated in response to our draft report that this recommendation has been implemented.

This report, dated September 27, 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 issues credentials which establish the identity and license status of drivers, ownership of boats and vehicles, and authenticity of auto-related businesses. In addition, the Department monitors driver training, administers road tests, and enforces the directives of local magistrates and departmental referees. The Department has a workforce of just over 2,800 employees and an annual operating budget exceeding $340 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. 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 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 in 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 RECOMMENDATION

### *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 promote traffic safety, protect consumers, verify identities and issue secure documents, provide information services, and collect revenues for the benefit of the people of this state." To that end, the Department processes a variety of transactions for individuals and businesses. We reviewed Department 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, credit card number, and DMV number (a Department-assigned number used as a primary identifier for most transactions). Not every form requires every element; however, of the data elements collected, only name, address, social security number, date of birth, and DMV number are maintained in the Department's system for tracking license information. Credit card numbers are also stored, but in a separate system with limited access.

Based on our review of personal information collected and programs run by the Department, the personal information collected by the Department is needed to fulfill its mission. Therefore, 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 also 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 laws the Department must comply with, such as the federal Driver's Privacy Protection Act, the New York State Personal Privacy Protection Law and the New York State Technology Law. Other than one provision for which CSCIC has not yet issued final standards, we found 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 laws intended to ensure motorists' 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. We visited units in the central office, as well as issuing offices. Some issuing offices are run by the Department, while others are run by the county in which they are located. All issuing offices are required to follow the same policies and procedures, including those related to information security.

## Intake

The Department receives information in different ways, depending on the transaction. Information is initially provided in person or via the mail. Renewals can be handled online. All applications (initial and renewal) require a form, which is completed by the applicant. Initial applications require supporting documentation, which is used to verify the identity of the applicant, but are usually not copied. All information from the form is entered by the processing clerk. If the applicant is paying via credit card, the credit card number is stored in a separate system, and only certain employees have access to that information. All forms generated during the course of the business day are gathered and placed in a secure location at the issuing offices. Within a few days, the forms and fees collected are reconciled and sent to the central office.

## Information Access

Access to personal information - whether stored in hard copy or electronically - is restricted and assigned to employees based on position and unit needs. All electronic records are maintained by the Department, and may be accessed by central office units and by issuing offices. Paper documents from issuing office locations are kept secure at the issuing offices. Within a few days the issuing offices send the documents to the Department, either the central office or a secure storage facility.

Employee access to information is granted on a business-need basis, with more sensitive data requiring higher levels of approval. Unauthorized access to physical or electronic information and/or unauthorized disclosure of confidential information will subject an employee to disciplinary action and/or criminal prosecution. The Department has the ability to monitor most employee activity and identify unauthorized access. However, the Department primarily reviews employee access when there is some reason to suspect a violation, rather than regularly reviewing reports to identify potential misconduct by employees.

The Department grants access to certain external parties with a business need, such as police and fire departments. External parties must identify specific individuals who will have access, and agree to abide by the Department's information security policies. The Department regularly monitors information access by external parties and will limit or deny access to information if an external party has accessed information inappropriately. We found the Department is effectively monitoring external access to Department records.

Storage and Disposal

The Department has policies and procedures for the proper disposal of official forms and documents, but not for other paper documents containing personally identifiable information that may be generated during the normal course of business. Examples of these items can range from computer-generated reports and printouts to photocopies and simple notes. It is important that these items be shredded or otherwise made unreadable before disposal, since mixing these items in with regular trash increases the risk of unauthorized disclosure and misuse of the information.

The Department contracts with an outside vendor to securely dispose of official documents nearing the end of their required retention period. Similarly, most Department employees with whom we spoke were aware that other items containing personal information should be shredded prior to disposal, even though there was no specific policy requiring this. However, during our field visits, we found staff at one of two central office units did not have ready access to a shredder and therefore were routinely disposing of documents containing personal information simply by placing them in the normal recycling bins. Staff in this unit were less aware of security issues, indicating documents containing personal information were sometimes left on desks overnight in the unlocked office. In contrast, the other unit we visited shredded documents that were no longer needed, stored other documents in locked files and also locked its office each night.

## *Breach Preparedness*

In December 2005, Section 208 of the New York State Technology Law went into effect. Also known as the 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 Coordination. 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.

The Department's Information Security Officer (ISO) is aware of the requirements of the Act and is responsible for coordinating the investigation of breaches. Currently there are no written breach procedures, but the ISO is preparing draft breach procedures which will identify responsibilities and define procedures for various Department units to follow in the event of a breach of personal information.

Since the Act went into effect in December 2005, the Department has had only one reported breach involving an authorized individual from another State agency accessing information for unauthorized purposes. The Department took appropriate steps to notify the affected individuals, the Attorney General's Office, the Consumer Protection Board, and the Office of Cyber Security and Critical Infrastructure. The

Department was not required to notify the consumer reporting agencies, because the breach involved less than 5,000 State residents. Though the case is still open, the individual responsible for the breach no longer has access to Department records. The breach appears to have been handled as required by law.

Overall, we found that the Department is prepared to handle breaches of personal information and is in the process of establishing appropriate procedures for responding to breaches of personal information in its possession.

**Recommendation**

Develop procedures addressing short-term document storage and disposal to ensure all staff are aware of proper security precautions.

(Department officials replied that a policy concerning the storage and disposal of documents containing personal information has been issued and disseminated to all Department employees.)

## 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 April 6, 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 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.

Within 90 days of the final release of this report, as required by Section 170 of the Executive Law, the Commissioner of the Department of Motor Vehicles 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 recommendation 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, Andre Spar, Alina Mattie, and Mary McManus.

## APPENDIX A - AUDITEE RESPONSE

**NEW YORK STATE**
**DEPARTMENT OF MOTOR VEHICLES**
**AUDIT SERVICES**

DAVID J. SWARTS
Commissioner

EDWARD J. WADE
Director of Audit Services

September 12, 2007

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

Re: 2007-S-79 Draft Audit Report

Dear Mr. Houston:

This letter is in reference to the New York State Comptroller's draft audit findings of audit report number 2007-S-79, Security Over Personal Information. Overall, we are satisfied with the outcome of this audit and welcome opportunities to improve our processes.

Please be advised that we have issued a policy concerning storage and disposal of documents containing personal information. This policy has been posted to the Department's intranet site, and an e-mail notice concerning the policy has been sent to all Department employees. We will monitor compliance with the new policy to ensure that documents are disposed of properly.

We will continue to look for improvement opportunities such as these and always welcome a chance to better serve the citizens of this State. If you have any questions concerning this matter, please contact me at (518) 474-0881.

Sincerely,

Edward J. Wade
Director

SIX EMPIRE STATE PLAZA • ROOM 321A • ALBANY, NY • 12228
PHONE: 518-474-0881 • FAX: 518-474-8358