8 Service Nova Scotia and Municipal Relations: Registry of Motor Vehicles Information and Technology

Summary

The Department of Service Nova Scotia and Municipal Relations does not have adequate controls to ensure the confidentiality and integrity of the information in its Registry of Motor Vehicles (RMV) systems. Nova Scotians who operate or own a motor vehicle are required to provide personal, sensitive information to the Department and strong controls are needed to protect the privacy and safety of these individuals. Stronger controls are needed to prevent such offences as credit card fraud, identity theft, and drivers having fraudulently-obtained licenses.

Processes to provide access to RMV systems are not documented and the removal of access privileges is deficient. Some users of RMV systems have access to confidential information they do not need to perform their job, and their access privileges are not always removed when they change job responsibilities or leave the Department.

The Department cannot be assured it provides licences, permits and identification cards only to those who are eligible to receive them. Potentially, certificates and cards could be issued based on fraudulent misrepresentations by customers or inappropriate actions of employees.

Privacy policies are not always followed. When processing transactions, some employees make photocopies of sensitive identity documents as part of the process to verify the customer’s identity. Department policy states that such information is not to be retained. Further, any credit card information retained in this manner is against rules established by credit card companies when they authorize the use of their cards for receipt of payments. This is further complicated by the fact that the Department is unable to determine if its employees view this information, as well as other sensitive registry information, for their own personal knowledge or gain.

The Department provides RMV systems access to many other provincial, municipal and federal government entities, as well as some private-sector and non-government organizations. The Department does not have policies or procedures for sharing registry information in the course of business and it is at risk of providing this information in a manner that violates the laws and regulations protecting the privacy of information. Some sharing arrangements are not supported by a signed information sharing agreement, and some arrangements that are supported by agreements are outdated and do not reflect all current standards and legislation.

NOVA SCOTIA

8 Service Nova Scotia and Municipal Relations: Registry of Motor Vehicles Information and Technology

Background

SERVICE NOVA SCOTIA AND MUNICIPAL RELATIONS: REGISTRY OF MOTOR VEHICLES INFORMATION AND TECHNOLOGY

8.1 The Department of Service Nova Scotia and Municipal Relations (SNSMR) operates the Registry of Motor Vehicles (RMV). RMV collects significant amounts of information in a database to support its processing of transactions relating to the operation and ownership of motor vehicles. This information includes names, birth dates, residential addresses, driving histories, vehicle ownership, licence plates, and motor vehicle fines and suspensions, which are used by RMV in its issuance and management of photo identification cards, licence plates, driver's licences, vehicle ownership documents and vehicle permits.

8.2 RMV systems are supported by other systems within the provincial government.

- Judgments and fines under the Motor Vehicle Act are processed through the Department of Justice and are connected to RMV through the Justice Enterprise Information Network.
- The summarized health information stored in RMV systems is supported by information in a separate database, the Road Safety Medical System. SNSMR is also responsible for this database. It contains detailed health information of certain drivers.
- Filenet is an electronic document repository at SNSMR that contains all scanned documents used to support RMV transactions. This includes application forms, statements of insurance, and vehicle purchases and sales certificates.

8.3 Customer service representatives at SNSMR use RMV systems to process transactions and to look up information for customers. Numerous other entities have access to RMV information, such as other provincial government departments (e.g., Community Services); the federal government (e.g., Canada Revenue Agency, Statistics Canada, Elections Canada); municipal governments (e.g., police agencies); and certain private-sector and non-government organizations.

8.4 Much of the information maintained in these systems is personal and sensitive. Proper management of the information technology supporting RMV operations is critical to ensuring the confidentiality and integrity of such information. As well, strong controls are essential to protect the public from negative experiences such as fraud and identity theft.

8.5 In addition, RMV needs strong controls to ensure only properly qualified, competent and safe drivers are licensed to operate a motor vehicle, and only roadworthy motor vehicles are safety approved. Audit work was conducted to address these issues and is reported in Chapter 7 of this Report.

Audit Objectives and Scope

8.6 Early in 2011 we completed an audit of the use of information and technology by the Registry of Motor Vehicles. The engagement was conducted in accordance with Sections 18 and 21 of the Auditor General Act and auditing standards established by the Canadian Institute of Chartered Accountants.

8.7 The purpose of our audit was to determine if there are sufficient controls in place to ensure the protection and accuracy of information collected and stored in RMV systems. Audit fieldwork was conducted between September 2010 and January 2011, which included testing of transactions dated between April 1, 2009 and August 31, 2010.

8.8 Our audit objectives were to assess the adequacy of:

- controls to ensure completeness, accuracy and availability of information collected, produced and reported;
- fraud prevention practices, policies and procedures;
- systems and processes to protect the privacy of information collected and stored; and
- control over information shared with other government entities.

8.9 The majority of the criteria used to audit RMV IT processes and controls were obtained from the IT Governance Institute's framework, *Control Objectives for Information and related Technology (COBIT 4.1)*, which is a widely-accepted international source of best practices for the governance, control, management and audit of IT operations. Other audit criteria were developed specifically for this engagement.

8.10 These objectives and criteria were discussed with, and accepted as appropriate by, senior management of the Department.

Significant Audit Observations

Transaction Controls

Conclusions and summary of observations

The Department of Service Nova Scotia and Municipal Relations has policies and procedures to guide the processing of transactions within RMV systems, but compliance can be improved. We found that processed transactions are reviewed to monitor whether SNSMR policies and procedures are followed, however the timing and nature of these reviews are not consistent across the province. As a result, there is risk that transactions are being processed for customers with invalid identification, thereby providing permits and licenses to ineligible individuals.

8.11 *Collection of information* – Customer service representatives of SNSMR's Service Delivery division collect, assess and input motor vehicle and driver information into RMV systems. They are responsible for ensuring that appropriate forms for each transaction are completed in accordance with departmental policies. Depending on the type of transaction, there are different requirements for the retention of supporting documentation.

8.12 We selected a sample of 90 transactions dated between April 1, 2009 and August 31, 2010 to test whether department policies and procedures were followed. We selected:

- 30 vehicle-related transactions;
- 15 photo identifications and licence renewals; and
- 45 licence testing transactions.

8.13 *Vehicle transactions* – We found that appropriate documentation is retained for transactions related to vehicle registrations, permits and plates.

8.14 *Photo identification cards* – Two photo identification transactions did not have sufficient documentation to indicate that the identity of the applicant was appropriately verified before a card was issued.

8.15 *Driver's licence transactions* – Our testing of driver's licensing transactions included learner's licences (Class 7), upgrading to a newly licensed driver's licence (Class 5N), exiting the graduated driving licensing program (Class 5), and obtaining a new licence through exchange of an existing licence. Our findings were as follows.

- All 12 of the learner drivers in our sample were at least 16 years of age, as required. Of nine instances in which parental consent was required, there was no evidence of consent in one file.

- One of the nine records that required evidence of completion of a driver's education course did not contain sufficient information to identify the driving school.

- There were five transactions that did not record the correct transaction type or previous driver's licence held.

- For one transaction there was no application form on file to document required signatures and the types of identification reviewed.

- All eight newly licensed drivers in our sample completed the proper waiting period before obtaining their Class 5N licence.

- All four drivers in our sample who exited the graduated driver licensing program met the requirements of the program.

- An Interprovincial Records Exchange network check was completed for the 11 licence exchanges in which it was necessary.

- Many licensing transactions require the creation of a new master number. This is the unique identifier for each customer in the registry. Customers must present certain verification documents for these transactions. The type of identification presented and reviewed is to be noted on the application form. The creation of a new master number was required for 27 of the 45 licensing transactions we tested. There was one transaction in which there was no indication on the application form that any of the required identification was presented.

8.16 Employees have their transactions reviewed on a periodic basis to determine if they are following the Department's policies and procedures. These reviews attempt to identify and correct processing errors. While we saw evidence that reviews were being completed, management informed us that the timing and nature of the reviews are not consistent between Service Delivery and Non-service Delivery staff. Therefore, there is risk that errors are not being detected and corrected.

Recommendation 8.1
Service Nova Scotia and Municipal Relations should implement and adhere to a transaction review process for all staff members who enter transactions into the Registry of Motor Vehicles systems.

Access Management Controls

Conclusions and summary of observations

There are deficiencies in the management of access to Registry of Motor Vehicles systems. Some system users have more access than required to perform their jobs. There is no process to identify and remove dormant user accounts. Improper access management increases the risk of unauthorized viewing or use of confidential information.

8.17 *Background* – Access management is the process of providing authorized individuals with computer accounts, setting and changing their ability to access different types of information, and removing those accounts when access is no longer needed. To ensure the security of confidential information in RMV systems, individuals should only be able to access the specific information needed to perform their tasks. When access is no longer required due to job changes or termination of employment, an account should be immediately deactivated. Individuals terminated could retaliate by disclosing, modifying or deleting sensitive information if prompt deactivation of their user accounts does not occur.

8.18 *Access management process* – There are no policies or procedures describing the process that system administrators are to follow to manage access to RMV systems. Requests for access and changes to current access privileges are submitted via email or paper memos. There are no standardized forms with unique identification numbers to control the authorization, tracking and management of access requests.

8.19 There are currently two separate processes to manage access. One process manages access of employees who provide services to customers (Service Delivery). Another process manages access for all other users, whether internal or external to the Provincial government (Non-service Delivery). A separate system administrator manages access for each group. We observed that each system administrator retains different supporting documentation and uses different methods to file that documentation. Multiple processes increase the risk that access is not granted and terminated appropriately.

8.20 We tested samples of newly hired, newly assigned, transferred, and terminated system users to determine if there was adequate management of their access privileges. We found the following areas of concern.

- Non-service Delivery access requests are filed together, but are not catalogued for easy retrieval and review. We found access requests for all of our sample items, but there was no documentation to support the level of access provided to two individuals.

- The time taken to remove system access for Service Delivery employees leaving the Department ranged from three to 425 days. Five accounts had been set as inactive, but there was no record indicating when these accounts were disabled.

- There is no periodic review of user accounts to minimize the existence of dormant accounts. Dormant accounts are active accounts that are not being used by their registered owner. They can become targets for malicious individuals to gain access to a computer system. There is also risk that a terminated employee can provide an existing employee with their username and password, thus providing the existing employee with elevated access to the system.

- Our review of registry user accounts identified that 155 of the 680 accounts are considered dormant.

8.21 We also found poor control over the level of access assigned to some users.

- Employees at the Department of Community Services require inquiry-only access to the registry for specific information. However, they have been assigned more access than needed, which may impact customer privacy.

- We tested ten user accounts with the ability to back out transactions posted to the registry. One of those ten also had the ability to post transactions. No one should have the ability to perform both of these functions because it represents poor segregation of duties and increases the risk of abuse. It was also determined that this individual had changed positions in the Department and should not have retained the ability to back out transactions.

- We tested 59 user accounts with the ability to authorize transactions as supervisors. Four of those individuals no longer required that level of access due to changes in their job responsibilities.

- We identified 14 instances in which access privileges were not updated for changes in personnel. This could lead to individuals who have changed jobs but are still employed by the government accessing information they do not require for their current jobs.

8.22 Without appropriate and consistent processes, managing and controlling access to RMV systems is more difficult. Individuals may gain or retain inappropriate levels of access which can negatively impact the confidentiality, integrity and availability of information in the system.

Recommendation 8.2
Service Nova Scotia and Municipal Relations should improve its management of access to Registry of Motor Vehicles systems, including:

- the use of consistent processes;
- better documentation and tracking of the granting and changing of access privileges;
- provision of access to only the information needed by a system user;
- avoidance of segregation of duties problems;
- more timely deletion of access privileges when they are no longer needed; and
- removal of dormant user accounts.

Fraud Controls

Conclusions and summary of observations

Compliance with fraud prevention policies and procedures is monitored. However, the Department does not have adequate controls to prevent fraudulent transactions by customers or employees. Deficiencies were also found in fraud prevention training. Strong controls over day-to-day processing of registry transactions are critical to preventing fraudulent activity and maintaining the completeness and accuracy of RMV systems information.

8.23 *Monitoring* – The Department has an internal audit group which consists of four individuals who are independent of the customer service representatives. The primary purposes of the group are to monitor exception reports and perform reconciliations of inventory and financial transactions. Inventory consists primarily of licence plates and stickers, blank registration and permit certificates, and blank driver's licences and photo identification cards.

8.24 We found there are regular reports to enable management and internal auditors to watch for unusual transactions and trends. There are also regular reports to reconcile inventories and monitor financial transactions. The internal audit group is responsible for investigating any discrepancies or anomalies identified. We saw documented evidence of the internal audit group's investigations.

8.25 Supervisors are responsible for monitoring inventory, including regular spot-checks of sequentially-numbered documents. We also saw evidence of this process.

8.26 *Prevention of fraudulent transactions* – The Department is at risk of issuing certificates and cards based on fraudulent misrepresentations by customers or inappropriate actions of employees. These weaknesses are not mitigated by the monitoring procedures noted above.

- Customers are required to complete a statement of insurance for some RMV transactions, but staff members do not validate the accuracy of the information submitted.
- Customers who have lost their licence or photo identification are able to send a fax authorizing another individual to pick up their replacement card. There are no procedures to validate the identity of the person sending the fax or the person picking up the new card.
- Learner's licences, medical assessments and accessible parking permits require applicants to obtain specific signatures before the transaction can proceed (e.g., parents, doctors). There is no verification that these signatures are legitimate.

Recommendation 8.3
Service Nova Scotia and Municipal Relations should develop processes for verifying information received from customers, at least on a test basis subsequent to the transaction.

8.27 *Fraud training* – Driver's licences and photo identification cards issued by the government of Nova Scotia are meant to be very secure forms of identification. The documents used to authenticate a customer and validate information they provide need to be assessed to ensure they are authentic. We found that customer service representatives are provided with some guidance and visual aids for assessing the validity of identification documents. However, comprehensive training has only been provided to one member of management.

Recommendation 8.4
Service Nova Scotia and Municipal Relations should provide fraud training to all staff responsible for assessing the authenticity of identification documents.

Privacy Controls

Conclusions and summary of observations

There are documented policies and procedures to protect the privacy of sensitive information maintained by SNSMR. However, there are deficiencies with respect to the collection and retention of unneeded personal information that could subject customers to fraud or identity theft, and could impact on the Province's ability to conduct business using credit cards. There are also deficiencies with respect to the monitoring of access to registry information. Due to the sensitive nature of some of the information collected, it is imperative that registry information be protected from inappropriate exposure.

SERVICE NOVA SCOTIA AND MUNICIPAL RELATIONS: REGISTRY OF MOTOR VEHICLES INFORMATION AND TECHNOLOGY

8.28 *Privacy policies* – The Department has policies regarding the protection of confidential information in accordance with privacy legislation. In addition, all system users are required to sign a confidentiality agreement to document their acknowledgement and understanding of those policies. We found that this requirement is not being enforced for all system users. Without signed agreements, the Department cannot be assured that all system users are knowledgeable of their responsibilities to protect private information.

Recommendation 8.5

Service Nova Scotia and Municipal Relations should enforce the requirement that all system users read and sign a confidentiality agreement before being granted access to Registry of Motor Vehicles systems.

8.29 *Monitoring of information retained* – Department policies and procedures identify documents that customer service representatives are to copy and retain for specific transactions. However, there is no monitoring of information collected.

8.30 When new customers apply for a photo identification card or a driver's license, they must provide multiple pieces of identification. These include one primary piece of identification, such as a birth certificate or passport, and two other pieces of identification that contain a signature. The specific types of identification provided are to be recorded by customer service representatives on the forms that support the transaction. However, there is no requirement to copy and retain such documents.

8.31 During our testing of RMV transactions we noted that photocopies of identification documents are sometimes included in registry files. We believe that retaining copies of identification documents would help control the risk of employees issuing fraudulent cards, and the Department should have a policy to retain such photocopies. However, the photocopies we found included customer's social insurance numbers, credit card numbers, card bearer names, expiry dates and the three-digit security numbers located on the back of credit cards. All documentation used to support such transactions, including the photocopied identification documents, is electronically scanned, backed up to electronic media, and uploaded to an electronic file repository. During this process, no sensitive private information is redacted or encrypted. Accordingly, this sensitive information can be viewed by individuals who have access to the electronic file repository, as well as by those who scan and destroy the paper copies. This places customers at increased risk of identity theft and fraudulent use of their credit cards.

8.32 All entities receiving payment by way of credit cards must follow the payment card industry's data security standard. This standard prohibits the retention of credit card numbers unless they are encrypted. Further, the standard does not allow the retention of the three-digit security number in any format. In the event credit card information is used fraudulently due to the Department's poor data retention practices and noncompliance with credit card industry standards, the government could be fined, or even lose its ability to accept credit card payments.

SERVICE NOVA SCOTIA AND MUNICIPAL RELATIONS: REGISTRY OF MOTOR VEHICLES INFORMATION AND TECHNOLOGY

Recommendation 8.6
Service Nova Scotia and Municipal Relations should create and enforce policies to prevent the retention of personal information that is not required to complete a transaction.

8.33 *Monitoring access to information* – The various users of RMV systems require different levels of access to information to perform their assigned duties. This includes the ability to view private information of thousands of individuals, such as names, birth dates, residential addresses, driving histories, vehicle ownership, licence plates, and motor vehicle fines and suspensions.

8.34 System users can view such sensitive information for personal use, gain or knowledge because no one is monitoring users' access to such information. Reports can be generated from system access logs to allow monitoring, but this is not happening. In addition, RMV's logs of users' actions contain only 14 days of data, so they cannot be used to investigate suspicious events that have occurred before that time span.

Recommendation 8.7
Service Nova Scotia and Municipal Relations should develop access log reports and use them to monitor for inappropriate access to Registry of Motor Vehicles' customer records.

Sharing of Information

Conclusions and summary of observations

SNSMR is currently misinforming some customers by indicating that their information is not being shared. Additionally, the Department does not have a policy for its sharing of registry information to fulfill business obligations. Some sharing arrangements are not supported by a written agreement, and some arrangements that are supported by agreements are outdated and do not reflect all current standards and legislation. As a result, SNSMR is at risk of providing information that is in violation of laws and regulations protecting the privacy of information.

8.35 *Privacy statement* – The Department is restricted by the Freedom of Information and Protection of Privacy (FOIPOP) Act from disclosing personal information obtained from Nova Scotians to persons or entities outside of the provincial government, unless certain criteria are met. However, Section 5(3) of the Act permits the Registry to disclose personal information if an information sharing arrangement was in place before the FOIPOP Act was proclaimed in 1993.

8.36 A privacy statement provided to customers conducting online transactions states *"We do not disclose your personal information to other organizations or individuals, except as required to fulfill the purpose(s) of the transaction or only to the extent required by law."* This is not an accurate statement. Every year, the Department prepares a report containing the names, addresses and master numbers of Nova Scotia drivers in its motor vehicle registry and provides it to The War Amps to support its key tag service. Whereas this sharing of information is permitted by the Freedom of Information and Protection of Privacy Act, the Department's privacy statement is inconsistent with the practice. Further, there is no need to provide The War Amps with master numbers.

Recommendation 8.8
Service Nova Scotia and Municipal Relations should have a process to ensure privacy statements provided to customers are accurate.

Recommendation 8.9
Service Nova Scotia and Municipal Relations should have a process to ensure only necessary information is shared with external organizations.

8.37 *Policies for sharing information* – SNSMR shares information from RMV systems with other provincial government departments (e.g., Community Services); the federal government (e.g., Canada Revenue Agency, Statistics

Canada, Elections Canada); municipal governments (e.g., police agencies); and certain private-sector and non-government organizations.

8.38 These sharing arrangements should be carefully administered in accordance with the FOIPOP Act, which states:

> *"24 (1) Personal information should not be collected by or for a public body unless:*
>
> *(a) the collection of that information is expressly authorized by or pursuant to an act,*
>
> *(b) that information is collected for the purpose of law enforcement; or*
>
> *(c) that information relates directly to and is necessary for an operating program or activity of the public body."*

8.39 Section 26 (a) of the FOIPOP Act also calls for the monitoring of information sharing arrangements to determine if information provided is being used *"for the purpose for which that information was obtained or compiled, or for a use compatible with that purpose."* Section 24(3) states *"The head of a public body shall protect personal information by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure or disposal."*

8.40 We believe signed information sharing agreements are needed to ensure compliance with provincial legislation, as well as to secure the use of such sensitive information. We found that most of the Department's information sharing arrangements are supported by memoranda of understanding or other forms of agreement, and they generally address the maintaining of data security and confidentiality.

8.41 However, some of the information sharing agreements were outdated and did not reflect current standards or legislation. If the level of care over shared information is not defined, disclosure of personal information could occur, and such disclosure could result in legal proceedings against the government. An outdated agreement indicates that it may not reflect current business needs, standards, laws and regulations. This increases the risk of misuse or poor control of information that is shared.

8.42 We did find some cases in which information was being shared without a signed agreement. When agreements do not exist, applicable regulatory or privacy requirements are not defined and agreed upon. This increases the risk of inappropriate use or disclosure of such information.

8.43 The Department does not have a policy to guide its administration of information sharing arrangements. This makes it more difficult for the Department to ensure that registry information is being shared for valid business purposes and that all applicable legislation is being followed.

Recommendation 8.10
Service Nova Scotia and Municipal Relations should develop and follow a comprehensive policy with respect to the sharing of Registry of Motor Vehicles' customer information. The policy should indicate all external parties receiving information from and providing information to the Registry of Motor Vehicles, and set out requirements to administer information sharing agreements on a continual basis.

IT Security Controls

Conclusions and summary of observations

Personal information is not secure in the test environment or the training environment of RMV systems. A related database, the Road Safety Medical System, has weaknesses in the security of its data. These deficiencies expose sensitive personal information to inappropriate use by persons who can access registry systems.

8.44 *Training environment and test environment* – The Department regularly makes copies of the data in its registry system (the live environment) to maintain two other separate computer environments. One is used to train employees and the other to test software changes. This allows training and testing activities to occur without slowing down registry systems and delaying service to customers.

8.45 We observed that the training environment does not require a unique username or password to access it, allowing unauthorized government employees to have full access to the personal information in the database. This includes names, birth dates, residential addresses, driving histories, vehicle ownership, licence plates, as well as motor vehicle fines and suspensions.

8.46 The test environment normally requires a username and password for access. However, during our audit, the Department disabled user authentication in the test environment for two days to test a change to its registry system. For these two days the information in the system was exposed to potential unauthorized access.

Recommendation 8.11
Service Nova Scotia and Municipal Relations should control access to the Registry of Motor Vehicles' training environment and test environment with the same level of rigor used for its live environment. Alternatively, it should not use data from its live systems in its training and test environments.

8.47 *Road Safety Medical System* – SNSMR obtains medical information for some licensed drivers as part of its mandate to preserve the safety of the driving public. The Road Safety Medical System (RSMS), isolated from other Department systems, is used to retain this sensitive personal information. Any updates to the registry for this information are performed manually and are summary in nature. Accordingly, details of medical information are recorded only in the RSMS.

8.48 Access to RSMS should be limited to specific employees who process medical records. We reviewed RSMS user accounts and found that seven of the 21 accounts pertain to individuals who no longer require access to the system. Their access privileges should have been removed.

8.49 Given the sensitive nature of the information contained within RSMS, and the ability of all government employees to access the login screen for the application, the use of strong passwords is critical. Our review of configuration settings for RSMS identified that it does not force users to create strong passwords. This increases the risk of someone cracking a password and inappropriately accessing sensitive personal information.

Recommendation 8.12
Service Nova Scotia and Municipal Relations should increase the security around the data in its Road Safety Medical System by regularly reviewing user accounts to ensure all accounts are still required, and by changing the configuration settings of the system to require stronger passwords.

8.50 *Oracle database* – The Oracle database supporting RMV systems is shared with the vital statistics registry. We reported in our November 2010 Report, based on our audit of the vital statistics registry, that the Oracle database had not been patched since 2008. We reviewed the current status of the database and determined that it has still not been patched. Patches are software changes issued by software vendors, many of which are intended to correct identified security vulnerabilities. They should be implemented as soon as they are tested in order to provide adequate security against hackers and malicious users.

Recommendation 8.13
The Chief Information Office should test and implement security patches for its Oracle database in a timely manner.

RESPONSE: SERVICE NOVA SCOTIA AND MUNICIPAL RELATIONS

Response: Service Nova Scotia and Municipal Relations

Service Nova Scotia and Municipal Relations (SNSMR) is pleased to provide a response to the Auditor General's review of Registry of Motor Vehicles Information and Technology.

We appreciate the extensive work done by the Auditor General's staff to identify areas that can be improved in the management of the delivery of this program. This review has provided SNSMR with a number of recommendations that, when implemented, will improve our operations.

SNSMR recognizes the importance of minimizing the risk of unauthorized access to the Registry of Motor Vehicles, ensuring that licenses, permits, and identification cards are only provided to eligible recipients, and that privacy policies and practices are defined, are current, and are followed.

The Auditor General's recommendations for SNSMR are accepted in principle and work has begun to implement many of these recommendations. We are confident that the implementation of these recommendations will strengthen both the business process and information technology for the Registry of Motor Vehicles.

Recommendation 8.1
Service Nova Scotia and Municipal Relations should implement and adhere to a transaction review process for all staff members who enter transactions into the Registry of Motor Vehicles systems.

SNSMR agrees with this recommendation. SNSMR has a transaction review process for Service Delivery staff, which represents 95% of users. This will be expanded to include all departmental staff in the next 18 months.

Recommendation 8.2
Service Nova Scotia and Municipal Relations should improve its management of access to Registry of Motor Vehicles systems, including:

- ***the use of consistent processes;***
- ***better documentation and tracking of the granting and changing of access privileges;***
- ***provision of access to only the information needed by a system user;***
- ***avoidance of segregation of duties problems;***
- ***more timely deletion of access privileges when they are no longer needed; and***
- ***removal of dormant user accounts.***

SNSMR agrees with this recommendation. SNSMR will continue to improve the current user account lifecycle management processes to ensure that all network, application, operating system and database accounts are current and assigned the appropriate privileges.

Recommendation 8.3
Service Nova Scotia and Municipal Relations should develop processes for verifying information received from customers, at least on a test basis subsequent to the transaction.

SNSMR agrees with this recommendation and has processes in place to verify information based on the associated risk. For example, an accessible parking permit tag is not considered a high risk transaction. In cases where there is reason to suspect wrong doing, which the Auditor General notes that SNSMR regularly runs reports to watch for unusual transactions or trends (8.24), SNSMR does make contact with customers and authorizing agents.

RESPONSE: SERVICE NOVA SCOTIA AND MUNICIPAL RELATIONS

Recommendation 8.4
Service Nova Scotia and Municipal Relations should provide fraud training to all staff responsible for assessing the authenticity of identification documents.

SNSMR agrees with the recommendation. SNSMR recently invited the Internal Audit staff from the Department of Finance to develop and deliver fraud awareness materials and training to several front line staff. This has been well received and we will continue to seek, develop, and deliver training programs that enhance our operations and reduce our risk of fraud.

Recommendation 8.5
Service Nova Scotia and Municipal Relations should enforce the requirement that all system users read and sign a confidentiality agreement before being granted access to Registry of Motor Vehicles systems.

SNSMR agrees with this recommendation. An employee responsibility package containing a number of policies and protocols, including a confidentiality agreement, is signed by all Service Delivery front line employees each year. Over the next 18 months, this will be rolled out to all employees who have access to the RMV system.

Recommendation 8.6
Service Nova Scotia and Municipal Relations should create and enforce policies to prevent the retention of personal information that is not required to complete a transaction.

SNSMR agrees with this recommendation. Service Delivery has provided a reminder to front line staff that secondary identification may not be copied or retained. In addition, a process has been established to identify situations where staff do not adhere to this process prior to the sensitive information being

RESPONSE: SERVICE NOVA SCOTIA AND MUNICIPAL RELATIONS

scanned. The incidents will also be reported to ensure the matter is addressed with the appropriate staff.

Recommendation 8.7
Service Nova Scotia and Municipal Relations should develop access log reports and use them to monitor for inappropriate access to Registry of Motor Vehicles' customer records.

SNSMR agrees with this recommendation. Access logs exist but are not consistently used for monitoring purposes. Over the next 12 months, SNSMR will initiate an analysis to determine the most efficient approach to meet this recommendation.

Recommendation 8.8
Service Nova Scotia and Municipal Relations should have a process to ensure privacy statements provided to customers are accurate.

SNSMR agrees with this recommendation. SNSMR will revise our privacy statements within 3 months.

Recommendation 8.9
Service Nova Scotia and Municipal Relations should have a process to ensure only necessary information is shared with external organizations.

SNSMR agrees with this recommendation. SNSMR will review where information is shared with external organizations and ensure that only necessary information is provided.

Recommendation 8.10
Service Nova Scotia and Municipal Relations should develop and follow a comprehensive policy with respect to the sharing of Registry of Motor Vehicles' customer information. The policy should indicate all external parties receiving information from and providing information to the Registry of Motor Vehicles, and set out requirements to administer information sharing agreements on a continual basis.

SNSMR agrees with this recommendation. SNSMR has initiated work to establish a comprehensive policy and to review all existing information sharing arrangements. It is expected that this review will be completed within 12 months.

Recommendation 8.11
Service Nova Scotia and Municipal Relations should control access to the Registry of Motor Vehicles' training environment and test environment with the same level of rigor used for its live environment. Alternatively, it should not use data from its live systems in its training and test environments.

SNSMR agrees with this recommendation. SNSMR is evaluating data masking technologies that will replace sensitive information with realistic but not real data. We expect this recommendation to be implemented within 18 months.

Recommendation 8.12
Service Nova Scotia and Municipal Relations should increase the security around the data in its Road Safety Medical System by regularly reviewing user accounts to ensure all accounts are still required, and by changing the configuration settings of the system to require stronger passwords.

RESPONSE: SERVICE NOVA SCOTIA AND MUNICIPAL RELATIONS

SNSMR agrees with this recommendation. This will be included in the comprehensive practice and protocols established in support of recommendation 8.2.

Recommendation 8.13
The Chief Information Office should test and implement security patches for its Oracle database in a timely manner.

SNSMR has forwarded this recommendation to colleagues at the Chief Information Office for consideration.

RESPONSE: CHIEF INFORMATION OFFICE

Response: Chief Information Office

The Chief Information Office would like to thank the staff of the Auditor General for their courtesy and professionalism while conducting this audit. One of the responsibilities of the Office is to supply infrastructure support services to departments including Service Nova Scotia and Municipal Relations. We are committed to providing quality secure services to our client departments.

The Chief Information Office has recently taken on the support responsibilities from the Corporate Service Units and from Corporate IT Operations for a good deal of government's infrastructure. Much of the efforts to date have been in rationalizing infrastructure and services, simplifying our technical environment and continuously working to evolve and advance our security measures as technology changes. We are focused on adopting best practices for the processes that support the infrastructure environment.

The Auditor General's recommendation related to the Chief Information Office is accepted in principle. Work began last fiscal year to address this recommendation and will continue until completed.