4 ELECTRONIC INFORMATION SECURITY AND PRIVACY PROTECTION

BACKGROUND

4.1 There has always been an assumption in democratic societies that citizens have a right to privacy. This is enshrined in *The Universal Declaration of Human Rights* adopted by the United Nations in 1948. Surveys have shown that citizens are deeply concerned that their personal information, especially medical and financial information, should remain confidential. At the same time, it is clearly recognized that governments and businesses need to gather personal information to perform their functions and citizens are willing to entrust aspects of their privacy in return for a benefit.

4.2 *Personal Information* is defined as information about an identifiable individual. It should be noted that statistical aggregations are not normally considered personal information.

4.3 The growth in the collection of electronic personal information and concerns about the protection of privacy led the Federal government to enact the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Additionally, the European Union restricts trade with jurisdictions that lack privacy legislation similar to its own. The core of PIPEDA was the adoption of Canadian Standards Association's (CSA) *A Model Code for the Protection of Personal Information*.

4.4 PIPEDA does not apply to provincial governments. In Nova Scotia, the Freedom of Information and Protection of Privacy Act (FOIPOP) is the primary governing legislation regarding the protection of personal information in government. Section 24(3) of that act requires the "*head*" of a "*public body*" to protect personal information "*....by making reasonable security arrangements...*". A number of other statutes, for example, the Hospital Act and the Social Assistance Act, govern particular departments, with specific rules concerning privacy of particular information.

4.5 These acts all speak of personal information in general terms, not distinguishing between paper records and electronic information. While the legal rules regarding paper records and electronic information are substantially identical, the methods used to protect them are significantly different. In this regard, it is government's responsibility to ensure that adequate security and control policies and practices are in place and properly functioning.

4.6 As stated by the Review Officer in the 2000-2001 *Annual Report of the Nova Scotia Freedom of Information and Protection of Privacy Review Office*:

> *"In my first Annual Report to the Legislature, for the period January 1, 1999 to October 1, 2000, emphasis was placed on access to information. In this Report I will, given the*

prevailing view that privacy is becoming a major social issue in Canada and other countries, spend more time discussing the need to address privacy protection issues."

4.7 Subsequent reports by the Review Officer have continued to devote a significant portion to discussion of privacy issues and cases.

4.8 In 2004-05 we conducted a review of electronic information security and privacy protection for selected government departments and systems.

RESULTS IN BRIEF

4.9 The following are the principal observations from this review.

- The level of assurance provided on the findings and conclusions in this chapter is less than for an audit (i.e., a review provides moderate assurance while an audit provides high assurance). This is because of the type of work we performed. Our evidence was based on management representations and review of applicable documentation. We did not test controls in place at the various departments we reviewed.

- In all the departments we reviewed, departmental staff were aware of security and privacy issues, and all staff were concerned with protecting the privacy of citizens. While this general culture of respect for security and privacy is a very positive condition, we have, however, noted a number of areas where improvements should be considered. In general terms, we believe that these areas for improvement are not due to any lack of concern regarding security and privacy, but rather to differing or competing priorities in departments. In every department, we found that some things were being done well but others needed improvement, and those were not the same in each case.

- There is a need for a comprehensive government-wide privacy policy as well as individual departmental privacy policies. In addition to other matters, these policies should address the following areas which need improvement.

  - Formal training programs in privacy should be included.
  - Detailed risk analysis should be conducted on the personal information collected by the departments.
  - Departmental staff should be required to read and sign confidentiality agreements.
  - Policies and practices should be developed and implemented to control the transmission of personal information.

- Personal information can only be protected if there is effective security in place. Security is a complex issue and can only be addressed by good planning. There is a need for a government-wide comprehensive security architecture and for consistent departmental security architectures.

- The Government of Nova Scotia should continue to assess the implications of the changes enacted by the U.S. government through the Patriot Act which could pose a risk to the security of the personal information of Nova Scotians.

REVIEW SCOPE

4.10 In fall 2002, we conducted a survey of the information technology sections of the government's Corporate Service Units (CSUs). We identified approximately 100 computer systems that might contain personal information, half of which appear to contain significant personal information. It was impractical to examine all of these systems so we selected a sample of eight systems from five different departments (see Exhibit 4.1).

4.11 The scope of this review specifically excluded the new human resources system (eMerge) and the new hospital information system (NShIS). These were excluded due to size and the fact that we are planning specific audits of these systems in the future.

4.12 The objectives of this review were to determine if the policies and practices of government regarding information security:

- are appropriate to protect the electronic information in the custody of government; and

- comply with the requirements of the Freedom of Information and Protection of Privacy Act (FOIPOP) and with those Acts which apply to particular systems.

4.13 Review criteria were developed to assist in the planning and performance of this review (see Exhibit 4.2). These were developed from the CSA's *A Model Code for the Protection of Personal Information* and from the Canadian Institute of Chartered Accountants' *Information Technology Control Guidelines*. These criteria were presented to senior management of the departments reviewed and were discussed in more detail with staff of these departments.

4.14 Our review consisted of interviewing departmental staff and reviewing documentation provided. We did not perform tests to verify if controls described to us were functioning as designed. We identified significant controls and weaknesses in the systems and have discussed these findings with departmental staff.

4.15 In addition to reviewing the eight selected systems, we also interviewed the FOIPOP Review Officer.

4.16 During our review, certain issues of government-wide significance arose and we comment on those as well.

PRINCIPAL FINDINGS

Comprehensive Government-Wide Privacy Policy

4.17 In the Freedom of Information and Protection of Privacy Act (FOIPOP), the Nova Scotia House of Assembly has recognized the need for protection of privacy. That Act sets out a statutory requirement to maintain the confidentiality of personal information and assigns responsibility for achieving that requirement to the head of each public body.

4.18 All the departments reviewed were aware of their responsibilities under FOIPOP. However, implementation of these responsibilities varied from department to department as can be seen in the findings described in the paragraphs which follow. For example, only a few departments have a departmental privacy policy and these vary in detail and scope. Other departments have specific policies that address particular areas of concern. As another example, some departments require staff to sign annual privacy and security statements while others do not. Again, some departments encrypt electronic personal information transmitted electronically but others send unencrypted data.

4.19 One very positive initiative was the development of the *Privacy Impact Assessment* (PIA) process. This was initiated by the Department of Health, and is already policy in that department. It was further developed by the government's Information Management Forum and is now a recommended best practice and has been proposed as a formal policy for all of government. The PIA process requires the completion of a checklist for each project. This checklist requires the identification of the personal information that will be collected by the project, its sensitivity and the planned security controls over that information. As well as the checklist, a user guide has been prepared to assist in its completion.

4.20 A comprehensive government-wide privacy policy would have numerous advantages.

- It would allow consistent treatment of privacy issues.
- It would allow efficiencies in the development of policies and procedures.
- Only a government-wide policy can address issues arising from the U.S. Patriot Act (discussed further below).
- It would clearly articulate where responsibilities for day-to-day security lay, in the CSUs or in the departments.
- It should incorporate certain policies already developed such as the website privacy policy, the wide area network (WAN) security policy and standards, and the PIA process.

Recommendation 4.1

We recommend that the government should develop and implement a comprehensive privacy policy.

Departmental Privacy Policies

4.21 We reviewed eight systems in five departments. As mentioned above, three of five departments reviewed do not have a departmental privacy policy. Our comments follow.

- One of the departments without an overall privacy policy has privacy policies in place over the particular systems we reviewed. However, one of these should be reviewed as the policy is nine years old and is rather narrow in scope.

- One department is in the process of preparing a departmental policy. It should continue with this initiative.

Recommendation 4.2

We recommend that all departments develop and implement a departmental privacy policy, consistent with a government-wide policy, to address the protection of personal information for all departmental business processes.

Comprehensive Security Architecture

4.22 A comprehensive security architecture is a formal, documented, strategy coordinating all aspects of information technology security. It should include provision for the security of personal information. At present a government-wide comprehensive security architecture does not exist. Similarly none of the departments we reviewed have a comprehensive security architecture. However certain policies and guidelines, such as the WAN security policy and standards, the e-mail guidelines and the internet usage guidelines, are in place and will be significant components of a comprehensive security architecture.

4.23 Appropriate security for information technology systems and data requires detailed planning. Information technology is inherently complex and rapidly changing. Ongoing technical knowledge is required to maintain security. Effective security also requires the informed co-operation of non-information technology staff who use applications to deliver service to citizens. The co-ordination of these two groups requires careful planning so that one does not inadvertently undermine the work of the other. Security procedures that are too onerous can delay the delivery of service, while a focus on the immediate delivery of service can undermine security.

4.24 A well-designed security architecture can mitigate the risks arising from the potential conflict between service delivery and security by:

- clearly defining roles and responsibilities;
- establishing communication policies and procedures; and
- providing training to ensure that staff are aware of security and privacy risks.

4.25 A security architecture should also establish a framework for action in the event of a security breach. The architecture should address the particular nature of personal information that may have been compromised in a breach. For example, loss of security over personal information in a large system often means that thousands of people need to be notified which can be a difficult logistical task.

4.26 The protection of privacy is just one of the goals of a security architecture. Any well-developed strategy produces considerable benefits and a security architecture will produce additional benefits beyond better privacy security including the following:

- provision of enhanced security in an efficient and effective manner;
- compliance with legislative requirements;
- reduction of uncertainty and potential conflict by defining such policies as departmental rights to e-mail and employee information; and
- provision of departmental security policies, procedures and standards as well as procedures for changing them.

4.27 While each department has unique infrastructure and system requirements, they are part of the overall government environment. Since some systems are shared across government, for example, GroupWise and the Wide Area Network (WAN), there is a need for a government-wide Comprehensive Security Architecture. A security breach in one department could put other departments at risk.

Recommendation 4.3

We recommend that a government-wide comprehensive security architecture be developed and implemented and that departmental comprehensive security architectures, consistent with the government-wide architecture, be developed and implemented.

Personal Information Risk Analysis

4.28 Security controls are not free. Resources would need to be committed to develop or acquire, implement and operate controls. The resources may be money or staff time or both. To efficiently utilize scarce resources, they should be committed to areas where they will be most effective. A risk analysis is the best way to determine security needs. None of the departments reviewed have conducted a formal security risk analysis. While most departments have implemented some controls over personal information, a formal risk analysis might reveal areas of risk not previously identified or areas where efficiencies could be realized.

Recommendation 4.4

We recommend that a formal security risk analysis be conducted, by department, regarding personal information. This might appropriately be a part of the development of a security architecture as recommended above.

Privacy Training

4.29 Individuals expect that their personal information will be protected but also that it will be used only for the purpose for which it was obtained. Training is necessary to ensure staff understand the essentials of confidentiality and how information should be used to effect the purpose for which it was obtained.

4.30 Led by the Department of Justice's FOIPOP Coordinator's office, training in privacy has been provided for a number of years. We have been informed that over 1,000 civil servants have been provided with this training. Training such as this should certainly continue. However this training is only delivered when a department requests it.

4.31 As noted above, three departments do not have a departmental privacy policy. Such a policy would set training standards. Without such standards, there can be no certainty that the proper staff will receive the proper training at the proper time.

Recommendation 4.5

We recommend that departments, as part of their departmental privacy plan, implement a formal training program.

Confidentiality Agreements

4.32 A key control in the protection of privacy is that each staff member be aware of privacy. This can be encouraged by having staff read and sign a confidentiality agreement. Such an agreement reminds the employee of the seriousness of confidentiality and allows management to effect appropriate disciplinary procedures should a breach of confidentiality occur. For maximum effectiveness, these agreements should be renewed annually.

Recommendation 4.6

We recommend that all staff with access to personal information be required to read and sign a confidentiality agreement as a condition of employment and that this agreement be renewed annually.

Transmission of Personal Information

4.33 The electronic transmission of data generates risks of inadvertant disclosure. A lower, but still significant, risk is that data might be unlawfully intercepted. In either case, encryption can provide protection to the transmitted data. Only two departments were regularly encrypting electronic personal information prior to transmitting it outside of their offices. High quality encryption software is not expensive and can be set to function automatically.

4.34 The transfer of paper documents, or electronic information on recordable media, also has risks. Departments should formulate policies concerning acceptable transmission methods that consider the significance of the personal information and the associated risks.

Recommendation 4.7

We recommend that all personal information sent electronically be encrypted and that policies be established to define acceptable transmission methods.

U.S. Patriot Act

4.35 The U.S. Patriot Act was passed in response to the attack of 9/11. Its goal was to increase the powers of the U.S. government to deal with terrorist attacks. It increased the ability of the U.S. government to acquire information. Section 215 of the Patriot Act is the section that is relevant to Canadian privacy. This section amends the Foreign Intelligence Surveillance Act (FISA) to ease the conditions under which a warrant may be issued by the U.S. Foreign Intelligence Surveillance Court. The hearings of this court are held in secret and its proceedings may not be disclosed. The warrants can be issued to a U.S. corporation that controls a foreign corporation. The warrant can require information in the control of that foreign corporation to be delivered to the U.S. security agencies. If that information was personal information under the control of a Canadian corporation, then the release of such information would be contrary to Canadian law. If such an order was issued, it would place the Head of a Canadian subsidiary of a U.S. corporation in the position of having to decide whether to violate U.S. law or Canadian law.

4.36 Furthermore, it is illegal under the Foreign Intelligence Surveillance Act to disclose that such a warrant has been issued. In other words, the head of the U.S. corporation or its Canadian subsidiary is expressly forbidden from notifying clients that the request was made or that information was provided. Failure to comply with these provisions is punishable by fines and/or imprisonment.

4.37 In his report *Privacy and the U.S. Patriot Act*, released in October 2004, the British Columbia Information and Privacy Commissioner states:

> *"We cannot ignore the fact that U.S. courts have upheld subpoenas ordering corporations to disclose records located outside the U.S., even when a foreign law prohibits the disclosure."*

4.38 The implications of these powers are wide sweeping and should be of concern to government. For example, if a U.S. security agency wanted to identify members of a group that it had concluded might constitute a risk, it could attempt to explore Canadian data, say health or educational information. If that data, or even the backup tapes of that data, were in the custody or control of a U.S. corporation, or a Canadian subsidiary of a U.S. corporation, a secret FISA warrant could be issued. If the company was a subsidiary of a U.S. corporation, it would probably

comply, and would be forbidden to disclose that the information was requested and provided. As this whole process is secret, no Canadian authority would be consulted by the U.S. security agency. No one would review the reasonableness of this search.

4.39 One of the companies used by the Nova Scotia government to store backup tapes is a wholly-owned Canadian subsidiary of a U.S. corporation. Also, the government's mainframe computer system, and numerous smaller servers, are housed at a data centre managed by another wholly-owned Canadian subsidiary of a U.S. corporation.

4.40 We have been informed that government has conducted an inter-departmental review to assess the risks arising from the U.S. Patriot Act and a report has been submitted to the Minister of Justice. We requested a copy of this report but were denied access to the full report due to reasons of "*Cabinet Confidentiality*" and "*Solicitor-Client Privilege*." We were provided with some sections of the report but we are unable to comment on the report since significant sections were omitted.

Recommendation 4.8

The government should continue to monitor the potential implications of the U.S. Patriot Act as it relates to the security and privacy of personal information held by, or on behalf of, the government of Nova Scotia.

CONCLUDING REMARKS

4.41 We found that in all departments reviewed, staff were aware of security and privacy concerns and issues and were concerned with protecting the privacy of citizens. While this general culture of respect for security and privacy is a very positive condition, as previously noted, there are a number of areas that could be improved. The development and implementation of comprehensive government-wide security and privacy policies should serve to address and resolve the matters we have set out in this report.

4.42 We believe that the deficiencies we have identified are not due to any lack of concern regarding security and privacy but, rather, to differing priorities across the departments. In every department, we found that some things were being done well but others needed improvement.

Exhibit 4.1

Electronic Information Security and Privacy Protection Systems Reviewed

Department	System Name
Education	Student Assistance
Community Services	Employment Support and Income Assistance (ESIA)
Health	Mental Health Outpatient Information System (MHOIS)
Service Nova Scotia & Municipal Relations	Registry of Motor Vehicles (RMV)
Service Nova Scotia & Municipal Relations	Registry of Statistical Information and Events (ROSIE)
Justice	Civil Index II
Justice	Justice Enterprise Information Network (JEIN)
Justice	Restorative Justice

Electronic Information Security and Privacy Protection Review Criteria

Exhibit 4.2

Protection of Personal Information Criteria

These are derived from the CSA Standard *A Model Code for the Protection of Personal Information.*

Personal Information is information about an identifiable individual.

- The organization must recognize its responsibility for Personal Information it has collected and should designate an employee as being responsible for protection of that information.
- The purpose for which Personal Information is collected should be identified by the organization. Information should only be collected for that purpose and should only be used for that purpose. Unless inappropriate, the consent of the individual should be obtained and the purpose clearly explained to them.
- The Personal Information should be as accurate as possible and there should be a process to allow an individual to review and request corrections of inaccuracies in their Personal Information.
- Personal Information should be secured by appropriate controls, both manual and automated.

Protection of Electronic Personal Information Criteria

These are derived from CICA's *Information Technology Control Guidelines*.

- If Electronic Personal Information is transferred to or from the organization, then there should be controls to ensure the integrity, reliability and appropriate confidentiality of the information.
- There should be a clear assignment of responsibility for the security of Electronic Personal Information. The assignment should ensure that the boundaries of responsibility for protecting electronic information and for protecting Personal Information are clearly defined so as to prevent gaps in control.
- The organization's security architecture should identify the special needs of Electronic Personal Information. Such identification should also reflect differing degrees of sensitivity of Electronic Personal Information.
- Access to Electronic Personal Information should be controlled both physically and logically.
- The infrastructure containing the Electronic Personal Information should be appropriately and securely housed.
- Application files, databases and data warehouses should provide assurance that Electronic Personal Information stored and delivered for processing is complete, accurate and authorized.