Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada

Privacy Matters

The Federal Strategy to Address Concerns About the *USA PATRIOT Act* and Transborder Data Flows

Catalogue No. BT22-104/2005E-PDF
ISBN 0-662-42357-7

This document is available on the Treasury Board of Canada Secretariat
Web site at www.tbs-sct.gc.ca

This document is also available in alternate formats on request.

Table of Contents

Executive Summary

The Government of Canada takes the issue of privacy very seriously, including concerns about possible privacy risks posed by foreign legislation, such as the *USA PATRIOT Act*. *

These laws point to the need for current privacy best practices to become more uniform throughout the federal government and for additional measures to build upon and complement the existing safeguards.

For over a quarter century, Canada has been a world leader in privacy. It has introduced ground-breaking legislation and policies designed to respect the personal information of its citizens.

Recent trends and events, however, have raised new concerns about whether the personal information of Canadians is adequately protected by governments and companies when it travels outside of Canada's borders.

Transborder data flows and contracting

The emergence of new information technologies, such as the Internet, allows information to be transferred quickly and easily across borders. This includes personal information and other sensitive information. The transfer of such information across borders is known as "transborder data flows."

Transborder data flows are becoming more common as companies and governments take advantage of outsourcing, a practice in which a supplier is hired under contract to manage certain activities, often because the institution does not have adequate internal resources to improve efficiency and levels of service. Federal government institutions are among the organizations that contract out or outsource some programs and services.

Information under foreign laws

It is not uncommon for an organization in Canada to outsource the management of personal information about Canadians to a company in the U.S. or elsewhere. Information stored or accessible outside of Canada can be subjected not only to Canadian laws but also to laws in the other country.

---

* "USA PATRIOT" stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."

One such law is the *USA PATRIOT Act*. The Act permits U.S. law enforcement officials to seek a court order allowing them to access the personal records of any person for the purpose of an anti-terrorism investigation, without that person's knowledge.

In theory, it means U.S. officials could access information about Canadians if that information is physically within the U.S. or accessible electronically.

British Columbia court case sparks national debate

In 2004, a court case in British Columbia (B.C.) sparked a national debate on the potential impact of the *USA PATRIOT Act* on the privacy of Canadians.

The British Columbia Government and Service Employees' Union sought an order to stop the provincial government from hiring the Canadian affiliate of a U.S. company to administer the province's medical records, claiming that the contract would make the records vulnerable under the *USA PATRIOT Act*.

The union lost the court case and is appealing. The province, meanwhile, proceeded with the contract using the U.S.-based firm but added new privacy measures.

In addition to the court case, the Information and Privacy Commissioner for B.C. conducted a review. The Commissioner for B.C. concluded that the issue was larger than the *USA PATRIOT Act*, that transborder data flows could make Canadians' information accessible under other foreign laws, and that the matter should be addressed by both the public and private sectors.

The Privacy Commissioner of Canada agreed with the results of the B.C. review, and together with the B.C. Commissioner, called for actions to be taken by the federal government to enhance protection of Canadians' personal information that can flow across borders.

The federal government's strategy

The Government of Canada responded to the *USA PATRIOT Act* concerns and other transborder data issues with a federal strategy. It is confident that the right to privacy related to key federal personal and sensitive information can be both respected and achieved.

The strategy was created with the following factors in mind.

Shared responsibility: The federal government is not alone. Other governments, the private sector, and Canadians themselves all have a role to play in the protection of privacy.

Balanced approach: Privacy needs to be weighed against other important considerations. Among these are the following: the need to ensure that contracting protects privacy and results in improved service to Canadians; international trade agreements that allow for fair and equitable treatment of foreign companies and play a major role in the health of Canada's economy; and the need to protect the public safety and national security.

Build on existing measures: The latest measures are an extension of privacy safeguards put into place long before the *USA PATRIOT Act* was enacted. They complement previous statutes such as the *Privacy Act*, enacted in 1983 to impose obligations on federal government institutions to respect the privacy rights of Canadians. The *Personal Information Protection and Electronic Documents Act* (PIPEDA*)*, which took full effect in January 2004, protects personal information held by the private sector. In addition, the Government of Canada was the first national government in the world to introduce a mandatory *Privacy Impact Assessment Policy*. The Policy requires government departments to build in privacy protection when changing or creating programs and services that collect personal information.

Informational privacy can also find constitutional protection under section 8 of the *Canadian Charter of Rights and Freedoms*.

The federal strategy consists of the following steps.

1. **Awareness:** The government made all of its 160 institutions that are subject to the federal *Privacy Act* aware of the privacy issues raised by the *USA PATRIOT Act*.

2. **Risk identification and mitigation:** Institutions reviewed their contracting and outsourcing arrangements to identify any risks under the *USA PATRIOT Act*, assess the seriousness of those risks, take corrective actions as needed, and report to the Treasury Board of Canada Secretariat (the Secretariat).

Here are the results reported to the Secretariat:

Most of the federal institutions, 83 per cent, had their contracting classified as "no risk" (77 institutions) or "low risk" (57 institutions) under the *USA PATRIOT Act* or other foreign legislation. Of the remaining institutions, many with mandates that include international activities, contracting risks were rated as "low to medium" (19 institutions) and "medium to high" (7 institutions). It should be noted that, if an institution identified only one contract as high risk, the institution was classified in the high risk category. That said, in all cases where risks were identified, institutions have taken, or are planning, remedial actions to mitigate risks.

3. **Guidance on privacy in contracting:** For many years, federal institutions have had privacy and security safeguards in place to protect personal and other sensitive information that is handled or accessible under contract. Risk management strategies are also in place to cope with emerging privacy issues and, where necessary, institutions have outlined further measures to mitigate risk.

Existing Best Practices include the following: Prior to initiating a contract, inspections of private sector facilities may be carried out by government security experts to ensure that adequate protection is available for information handled or stored off government premises by a contractor; the requirement that core information stays at home—in other words, part or all of the work must be completed within the department or within Canada; the return of records or approved destruction of all records at the end of a contract; the inclusion of contractual clauses to address confidentiality; and the signing of non-disclosure agreements.

Guidance document: The government has recently issued a policy guidance document for federal institutions that provides a privacy checklist and upfront advice on considering privacy prior to initiating contracts. It also includes specific considerations for maximizing privacy protection that can be used to develop clauses to include in requests for proposals (RFP) and contracts.

4. **Follow up:** The government will be taking additional steps to further mitigate risk.

Highlights of ongoing measures and those planned for within the next year:

- Follow-up assessment of federal contracting activities, ongoing contract advice, and implementation of risk management strategies for contracting where information may potentially be at risk under the *USA PATRIOT Act* or other foreign laws.
- Ensuring that key government policies are in step with privacy issues and reflect the new global reality.
- The exploration of technology and data architecture solutions to protect information flows, including the use of encryption technology and electronic audit trails.
- Continued monitoring of new technologies, trends, and events to address their possible effects on privacy.
- The development of additional guidelines to cover government-to-government information sharing (within Canada and abroad), auditing of contracts, and technical solutions to protect privacy.
- Increased awareness and training related to transborder data flows and existing federal safeguards.

Highlights of planned measures between one to two years:

- A scheduled 2006 review of the PIPEDA and determination if the federal *Privacy Act* should also be reviewed.
- The development of a privacy management framework to establish high standards of privacy protection throughout the federal government.
- Addressing privacy and transborder data flows for the recently announced Security and Prosperity Partnership (SPP) between Canada, Mexico, and the U.S.

The federal government will also continue to share best practices in protecting transborder data flows with provincial and territorial governments as well as the private sector and foreign governments.

1. Introduction

Role of the Treasury Board of Canada Secretariat

The Treasury Board of Canada Secretariat (the Secretariat) has produced this report to update Parliament and Canadians on the federal strategy in response to privacy concerns about the *USA PATRIOT Act*[*] and the possibility that foreign legislation could affect the protection of Canadians' personal information.

The President of the Treasury Board is the designated minister responsible for issuing government-wide directives and guidelines related to the administration of the *Privacy Act*. The Secretariat supports him in this role and also issues government-wide security, contracting, and procurement policies. The Secretariat was therefore the logical body to co-ordinate government-wide efforts in reviewing the privacy and security of personal information in contracts.

Purposes of the report

This report has the following purposes:

- to inform Canadians of privacy concerns related to the *USA PATRIOT Act* and transborder data issues in general;
- to make Canadians aware of the existing federal framework of privacy-related laws and policies that have made Canada a world leader in privacy; and
- to inform Canadians of the federal strategy addressing any ongoing issues related to transborder data flows.

Supporting facts

Privacy is defined as the fundamental right to control the collection, use, and disclosure of information about ourselves. Security, as it relates to privacy, is the process of assessing threats and risks to information and taking steps to protect it.

* "USA PATRIOT" stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."

2. Background

Today's information economy

Information and knowledge have largely become primary wealth-creating assets throughout the developed world.

Enabled by new technologies, Canada is now an information-based society.

The Internet and sophisticated software make it possible for companies, governments, and individuals to share information easily and to conduct business on an anywhere, anytime basis.

Transborder data flows and contracting

The flow of computerized data, including personal and sensitive information, across any international border, is referred to as "transborder data flows."

Transborder data flows are increasing on a daily basis, in part because of the increased reliance on contracting out, a practice in which companies and governments hire an outside service provider to deliver a program or provide a service, such as managing a database. This can often result in improved efficiencies and levels of service.

Contracting out, or outsourcing, as it is often called, has become a global practice. While an organization may be located in Canada, some of its activities, including the storage and handling of personal information, may be managed by another organization elsewhere in the world.

While transborder data flows have led to greater efficiencies, access to new products and services, and economic benefits, the transfer of personal data across borders has also raised concerns that information could end up in the hands of people for whom it was not intended.

That, in turn, could infringe on privacy.

Privacy is a fundamental right in Canada

Privacy has long been considered a fundamental right in Canada.

The United Nations *Universal Declaration of Human Rights* and the *International Covenant on Civil and Political Rights* enshrine privacy as a core human right or value that goes to the very heart of preserving human dignity and autonomy, as does the *Canadian Charter of Rights and Freedoms*.

For most Canadians, privacy is about control—the right to control one's personal information.

It was not surprising, then, to discover that transborder data flows are a concern for many Canadians, as reported in a recent survey.

Public opinion

A survey conducted earlier this year by EKOS Research Associates Inc. for the Office of the Privacy Commissioner of Canada (entitled *Canadians, Privacy and Emerging Issue*) found that most Canadians expressed concern about personal information transferred across borders.

The survey's results acknowledged that the cross-border transfer of personal information is a complex policy issue, involving important privacy, economic, national, security and other considerations. A copy can be reviewed on the Commissioner's Web site at http://www.privcom.gc.ca/information/survey/ekos_e.asp.

Another recent study (August 2005), *Privacy in the Information Age: Government Services and You*, found that while Canadians worry about governments holding extensive files on citizens, they are willing to make trade-offs for better services as long as appropriate safeguards are in place. That study, which examined the issue of government departments sharing information to improve services, was conducted by a not-for-profit organization called the Crossing Boundaries National Council, which is made up of senior public service employees and elected representatives from other levels of government and the Aboriginal community.

In their report, the Crossing Boundaries National Council recommends that governments establish strong safeguards on access to personal information but have the safeguards flexible enough for branches of governments to share data in new ways without too many obstructions. The report can be found at the following Web site: http://www.crossingboundaries.ca/files/kta_final_report_050805.pdf.

B.C. and the *USA PATRIOT Act*

The issues surrounding transborder data flow of personal information came to the forefront in Canada as a result of a court case launched in 2004 in B.C.

The British Columbia Government and Service Employees' Union sought an order to stop the provincial government from hiring the Canadian affiliate of a U.S. company to administer the province's medical records.

The union claimed that the contract with the U.S.-based company would open up the possibility of having medical records of British Columbians scrutinized by U.S. law enforcement officials under the *USA PATRIOT Act*.

Ultimately, in March 2005, the Supreme Court of British Columbia rejected the union's challenge—the union has since launched an appeal.

In the summer and fall of 2004, the Office of the Information and Privacy Commissioner for B.C. examined the matter, asked for submissions to obtain opinions, and directed recommendations at both the B.C. and federal governments. The Commissioner concluded that this was an issue that went beyond the scope of the province's influence and affected all of Canada.

Supporting facts

***The* USA PATRIOT Act**

- "USA PATRIOT" in *USA PATRIOT Act* stands for "Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism."
- Enacted in 2001 by the U.S. Congress.
- Amends the *U.S. Foreign Intelligence Surveillance Act* to allow the Federal Bureau of Investigation (FBI) to apply for a court order to obtain records, papers, documents, and other items for an investigation related to terrorism or clandestine intelligence activities.
- Under section 215 of the *USA PATRIOT Act*, the FBI could potentially obtain records that are held by companies located in the U.S., or records for which U.S.-based companies have direct access, and requires the companies not to disclose these actions.

The review of the Information and Privacy Commissioner for B.C.

- The Information and Privacy Commissioner for B.C. received 500 submissions from governments, businesses, labour groups, and others, mostly in Canada, but also from the U.S. and Europe.
- There was a general consensus that U.S. authorities could, under some circumstances, use powers under the *USA PATRIOT Act* to access information about B.C. citizens if the information were accessible under U.S. jurisdiction. There was, however, a wide variety of opinion about whether the risk of this actually happening was small or significant.

A global issue

The submissions to the Information and Privacy Commissioner for B.C. raised larger questions about the safeguarding of privacy in an era of economic globalization, widespread fear of terrorism, and transborder data flows.

It was noted that privacy risks exist whenever a transborder data flow occurs since there are anti-terrorism laws and security measures in many other countries that contain powers similar to those of the *USA PATRIOT Act*.

As a result, the report of the Information and Privacy Commissioner for B.C. suggested that existing privacy protection would need to be reviewed by all jurisdictions across Canada and at an international level, in both the public and private sectors.

The Privacy Commissioner of Canada agreed.

Submission from the Privacy Commissioner of Canada

The Privacy Commissioner of Canada, Jennifer Stoddart, made a submission to the B.C. review that applauded the efforts of the Information and Privacy Commissioner for B.C. in examining the implications of the *USA PATRIOT Act*.

She agreed the B.C. situation was part of a broader issue—the extent to which Canada and other countries share personal information about their citizens with each other and the degree to which information transferred abroad for commercial purposes may be accessible to foreign governments.

The Privacy Commissioner of Canada outlined what can be done, including reminding private firms about their obligations under federal and provincial laws and indicating that her office planned to conduct a review of information-sharing agreements between the Governments of Canada and the U.S.

She asked the Government of Canada to review the circumstances related to transborder data flows in which personal information about Canadians may be accessible outside of Canada.

Supporting facts

The Privacy Commissioner of Canada concludes that the* USA PATRIOT Act *is not likely to be the first course of action

The Privacy Commissioner of Canada concluded that the *USA PATRIOT Act* is not likely to be the normal procedure to obtain personal information held in the U.S. about Canadians, a view shared by the Information Technology Association of Canada.

The Commissioner believes it is more likely that other means of obtaining information will continue to be used instead, such as grand jury subpoenas, ordinary search warrants, and existing information sharing agreements, or bilateral mutual legal assistance treaties that have been signed by the governments of Canada and the U.S.

Balancing privacy with other priorities

Both the B.C. and federal privacy commissioners and the Canadian public recognize that addressing issues around transborder data flows is more than just a consideration of privacy interests.

There are other interests at stake, such as significant cost and service efficiencies, and economic benefits from contracting out as well as the need to respect Canada's obligations under its trade agreements and the requirements to protect national security.

Contracting out

Contracting out, or outsourcing, is when an organization hires a company to carry out certain functions to improve efficiencies and levels of service. Companies often outsource to firms that may be located in other parts of the world to handle administrative and data processing tasks so they can concentrate on their core business.

Canada is a major user and provider of outsourcing arrangements and benefits from the practice. Many Canadian companies enter into outsourcing arrangements with U.S.-based businesses to receive and to provide services. Governments also engage in outsourcing to receive services.

Federal government contracting

The federal government has a large number of contractual arrangements in place to carry out functions more cost-effectively.

The vast majority of such contracts are to obtain goods and services for government use. They can range from regular contracts to obtain equipment, software, telecommunications, training courses, or services like temporary help, informatics, consultants, maintenance or repair, to the extremely complex contractual arrangements involving the transfer or delivery of a government program or service function to a contractor.

The federal government encourages innovative arrangements with suppliers to improve efficiency and service to the public. Outsourcing is viewed as a pivotal means of providing more flexible and responsive services to Canadians.

Privacy must, however, always be considered when determining if outsourcing is appropriate.

Supporting facts

Canada is a major beneficiary of outsourcing

The United Nations Conference on Trade and Development produced a report in 2004 called *World Investment Report 2004—The Shift Towards Services*, which states that the countries that have gained the most from overseas outsourcing are Ireland, Canada, Israel, and India. (See http://www.unctad.org/en/docs/wir2004_en.pdf.)

Information technology outsourcing by the federal government

Federal contractual arrangements related to information technology may involve the simple storage or archiving of government information, the operation or management of computerized systems, or the entire information technology function of a government institution or agency.

Information technology services may also be outsourced to support the delivery of a government program or function that involves the collection, use, or disclosure of personal information for a specified period, in which the accountability for the program or function remains with the government.

International trade agreements

In reacting to public concerns about privacy, the Government of B.C. amended its *Freedom of Information and Protection of Privacy Act*. The amendments placed new restrictions on public bodies and service providers from storing, accessing, or disclosing personal information outside Canada.

There are no plans at this time to amend the federal *Privacy Act* in a similar fashion. This is because such an action could encourage other foreign governments to do the same, choking off the economic benefits to Canada from work outsourced to Canadian suppliers. In addition, the federal government must respect international trade agreements that are not binding on provincial governments.

Canada has signed a number of international agreements, including the *North American Free Trade Agreement* and the World Trade Organization (WTO) *Agreement on Government Procurement*.

Any possible changes to Canadian federal laws could only be put in place if the changes fully respected these long established international trade agreements. This is extremely important because the trade agreements play a major role in Canada's economy.

Supporting facts

International trade is vital to Canada

One in every four jobs in Canada is related to international trade.

Businesses, organizations, and governments are not the only groups involved in the global economy. Individual citizens are also participants, and Canadians are among the most avid users of e-commerce.

The need for privacy protection is balanced with the freedom to use a credit card over the Internet to purchase goods and services or to use automated teller machines anywhere in the world.

The most effective ways to protect personal information

Federal privacy laws currently provide appropriate protection of the personal information of Canadians'. These are supplemented by policies that govern the way government institutions do business as well as contract clauses and best practices that specify contractor obligations to protect privacy.

A shared responsibility

Taking a balanced approach to privacy protection is not unique to the federal government: privacy is a shared responsibility.

Other levels of government

Provinces, territories, and local governments all have an obligation to protect information within their control. There are laws and policies, not only federally, but also provincially and territorially, that govern the collection, use, disclosure, retention, and disposal of personal information.

Private companies and organizations

The private sector is accountable for protecting privacy under PIPEDA or similar provincial legislation in a number of provinces. At the time of this report, only B.C., Alberta, and Quebec have privacy legislation similar to PIPEDA—none of the territories or other provinces have such legislation. That said, protecting privacy is more than a case of obeying the law. Respecting privacy laws and following internal policies that help to protect personal information are essential to the trust and confidence of customers.

Canadians

Canadians also have a responsibility to protect personal information. In her August 18, 2004, submission to the Privacy Commissioner for B.C., the Privacy Commissioner of Canada said that Canadians need to accept responsibility for informing themselves by asking who is using their personal information and for what purpose.

Supporting facts

How to protect your privacy

The Privacy Commissioner of Canada's Web site, http://www.privcom.gc.ca/fs-fi/index_e.asp, has a series of fact sheets designed to inform Canadians on how they can take charge of protecting their personal information.

Federal Response: A Continuous Risk-management Approach

Approach comprises 4 steps:

1. Communicate issue to 160 institutions
2. Conduct comprehensive assessment to identify risks and develop mitigation strategy
3. Develop and implement policy guidance on *USA PATRIOT Act* risks
4. Ongoing follow-up

3. The Federal Strategy

The federal government has had effective privacy management practices in place for many years. Most large federal institutions that routinely collect personal information about Canadians keep this information on-site only. For example, Statistics Canada only keeps personal information on its government premises, and the Canada Revenue Agency stores and backs up all Canadian taxpayer information on-site only.

The *USA PATRIOT Act*, however, drew attention to the fact that best practices should be more uniform throughout government. It also drew attention to the need for additional measures that would build upon and complement existing safeguards. The federal government's action plan in response to Canadians' concerns about the *USA PATRIOT Act* followed this approach:

1. **Awareness:** The Secretariat made all 160 federal institutions aware of the latest issues surrounding the *USA PATRIOT Act* and transborder data flows that involved personal and other sensitive information.

2. **Risk identification and mitigation:** The Secretariat asked each institution to conduct a review of its contracts to identify any potential risks related to the *USA PATRIOT Act*, assess the level of those risks, and outline corrective actions to address them.

3. **Guidance on privacy in contracting:**

(a) Federal institutions with identified risks were required to implement corrective action.

(b) To assist institutions, the Secretariat developed a guidance document to be used prior to entering into future contracts. The document includes a privacy checklist for contracts and advice on developing appropriate protective contract clauses.

(c) To share information and best practices, the Government of Canada has been in communication with, and has consulted, a wide range of parties, including its own experts, the Office of the Privacy Commissioner of Canada, and provincial governments.

(d) The federal government has also notified U.S. government officials of concerns in Canada related to the *USA PATRIOT Act* and promoted the use of existing arrangements between national security agencies and law enforcement agencies in the protection of personal and sensitive information.

4. **Ongoing follow up:** The government will monitor potential privacy risks and follow up with additional measures, as required. These will include additional policy guidelines, the scheduled review of PIPEDA, expanded privacy training and awareness and the introduction of a privacy management framework that will outline a privacy governance and accountability structure.

Each component of the federal strategy is examined below in detail, beginning with the review of federal government contracting.

Federal contract review

A major component of the federal government's strategy was a review of contracts. In October 2004, the Secretariat asked all 160 institutions subject to the federal *Privacy Act* to conduct an assessment of their contracting activities and to report on the results.

The review was no small task. The federal government has a large number of contracts and information-sharing agreements in place. For example, Human Resources and Skills Development Canada and Social Development Canada have more than 40,000 Grants and Contribution agreements in place. Foreign Affairs Canada and International Trade Canada have more than 8,000 contractual agreements.

Review objectives

The main objective of the review was to determine if information that is being stored by private companies or is accessible under the terms of a contract was susceptible to disclosure, specifically under the *USA PATRIOT Act*. Institutions were asked to see if any of the companies hired to provide services were based in the U.S. or had affiliations in the U.S. that might allow personal information to be accessible under the U.S. legislation.

The review also involved looking at the nature of contracts to determine if there were sufficient clauses to protect personal information or other sensitive information and, if not, to identify potential weaknesses and produce a plan of corrective action to mitigate any risks.

The review focussed on the *USA PATRIOT Act* because it allowed institutions to more quickly identify any weaknesses and thus raise a flag about whether the institution's contracting might also be vulnerable to any other foreign laws that allow access to personal or other sensitive information. While the emphasis was on information that could be accessed through the *USA PATRIOT Act*, the results would also be an indicator in relation to transborder data flows in general.

Review methodology

Interdepartmental committee

Since the review was to be a large undertaking, an interdepartmental committee was formed.

The committee was led by the Secretariat and consisted of 14 key institutions. Each institution had a role in providing advice to the other committee member institutions and in assisting the overall review process.

The review was conducted in two phases. A preliminary phase was quickly carried out first among 17 federal institutions to identify any major weaknesses among the largest programs. None was found. A more comprehensive review was then carried out by all 160 institutions.

Rating system

Federal institutions were asked to rate the status of their contracting agreements according to categories ranging from "no risk" and "low risk" to "medium risk" and "high risk." The higher the risk, the more vulnerable the contracting could be under the *USA PATRIOT Act* and potentially other foreign laws that could be applied to obtain personal information about Canadians or other sensitive information.

The identification of risks did not mean that a problem actually existed, rather, that there could be a potential problem in the future.

No to low risk: In these cases, information is gathered, maintained, and processed entirely by the Government of Canada without the use of any outside contractor (no risk) or, alternatively, a Canadian contractor is involved with operations only within Canada (low risk).

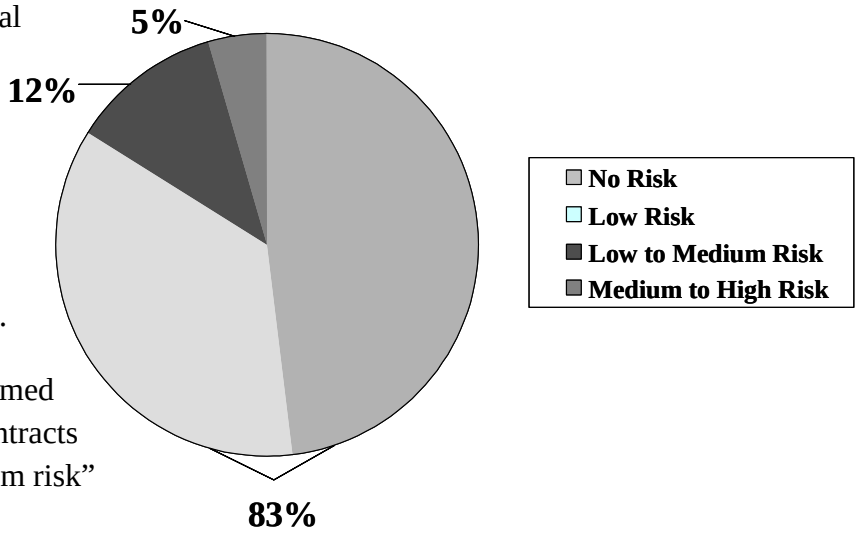
Low to medium risk: Information is located or maintained off-site by a Canadian company located in Canada but is also accessible by a foreign subcontractor, parent company, or affiliate. In these cases, laws from several different countries may apply.

Medium to high risk: The risk is considered to be "medium to high" when information is maintained and processed by a foreign-based company operating in a foreign jurisdiction. In these cases, there is a higher risk because such companies are more accountable to laws in their country than to laws in Canada.

Review results

The vast majority of contracting by the federal government is done inside Canada and therefore has a lower risk factor in relation to the possible application of the *USA PATRIOT Act*.

Of the responses from the 160 federal institutions, 83 per cent had their contracts classified under the “no to low risk” category. Contracts identified at 77 institutions were classified as “no risk” and at 57 institutions, some contracts were identified in the “low risk” category.



There were 19 institutions that informed the Secretariat that some of their contracts were classified in the “low to medium risk” category.

Only 7 institutions, in describing their contracting activities, identified a number of their contracts as having potential risks that could be classified in the “medium to high risk” category.

It should be noted that if an institution indicated that they had one contract that the Secretariat classified in the range of “medium to high risk,” the institution’s final rating was consequently identified as “medium to high risk,”

To see a table of the complete review results to date, please refer to Appendix A.

No to low risk contracts

There are many examples of contracting that represent either no risk or a risk that is low. In certain cases, this is because the federal institution is operating under strict practices and procedures that provide a high standard of data protection. This is the case with Statistics Canada, which is governed by the *Statistics Act*.

Case study: Statistics Canada

The *Statistics Act* requires that only Statistics Canada employees who have taken an oath of secrecy and who have been security cleared can have access to confidential information. Access to confidential information is on a need-to-know basis.

The protection of confidentiality is Statistics Canada’s highest priority. Data classified as confidential under the *Statistics Act* never leave Statistics Canada premises and are never out of the control of the Agency. Furthermore, all confidential statistical information is stored on an

"electronic island" (i.e. none of the systems or networks that contain confidential data have external connections) thus making it impossible for data to be transmitted outside the Agency.

No hacker can get access to these secure data.

Statistics Canada has contracts with U.S. firms including those that are Canadian subsidiaries of U.S. companies. These contracts are for the delivery, development, and maintenance of software and hardware and provide no opportunity of access to confidential information. In fact, all possible precautions have been taken in this respect: for example, all contractors are themselves subject to the penalties under the *Statistics Act*, and they are never allowed onto Statistics Canada premises without being accompanied by regular employees of Statistics Canada. Even if a request were ever to be made by a U.S. authority to any contractor, it would therefore be physically impossible for them to provide any data given that they are never in possession of confidential information.

As a further measure, prior to the 2006 Census, Statistics Canada will conduct three independent security verifications of all census systems in order to validate the protection of confidential census information.

Statistics Canada is an example of a federal government institution where there is no contracting out of personal information that relates to the general public.

Case study: the Secretariat

The review determined that the majority of the contracting carried out for the federal government that involves personal information is for programs and services for federal employees. For example, the Secretariat oversees contracts related to insurance and health plans for federal employees.

The **Public Service Management Insurance Plan** is currently with The National Life Assurance Company of Canada, which has no offices in the U.S. As such, there is "no risk" " of application of foreign legislation for this contract. The situation is similar for contracts related to the administration of the Public Service Dental Care Plan and The Pensioners' Dental Services Plan.

The **Public Service Health Care Plan** and the **Public Service Disability Insurance Plan** are under contract with Sun Life Assurance Company of Canada, which uses the services of another contractor, World Access Canada, for out-of-country and comprehensive claims. World Access Canada has a U.S. counterpart, but the arrangement calls for the U.S. office to be allowed

temporary access to database information only in the event of a disaster in the Canadian office to ensure continuity of service to current and former public service employees.

The use of a U.S.-based office as an emergency back-up only is an example that several institutions identified as "low risk" for contracting agreements.

Personal information considered most at risk

Of the seven institutions that reported some specific contracts that could be classified as having potential medium to high risk in relation to the possible application of the *USA PATRIOT Act*, the majority of them identified their vulnerabilities in terms of contracts related to the processing of employee data such as payroll, pension, personnel security, travel, insurance, and career transition information.

Other vulnerabilities identified by these institutions are related to contracts that involve the following:

- the construction of mission offices, staff quarters and residences for missions abroad (including building plans, specifications, drawings, and security systems);
- the disposal of immigration and consular records;
- the processing of client information for institutions that frequently carry out transactions across the border; and
- the processing of personal or commercial information about Canadians for the purpose of administering and enforcing the *Competition Act*.

For several of these contracts, institutions reported that they are working to minimize risks. Moreover, concerns will be addressed when the contracts come up for renewal, some contracts or arrangements will not be renewed and future contracts will include adequate clauses to ensure maximum security and privacy safeguards.

Risk management strategies and best practices

As part of the review process, federal institutions were asked to report on their risk management strategies, no matter how they classified their contracts.

Each federal institution is accountable for its own contracts and personal information under its control. Since each institution carries out different functions, strategies are customized to the business and client needs of the institution.

The review revealed that many strategies and best practices that were already in place are well suited to deal with some of the challenges related to today's transborder data flows.

Current practices

Most federal institutions have been using privacy and security clauses in contracting agreements to provide a variety of protective measures. Some of the more effective best practices include the following:

- the segregation of personal information being handled under the contract from other records held by the contractor;
- audit trails to closely monitor how information is being handled;
- the limiting of right-to-access based upon specific user profiles;
- approval by the government of any subcontracting;
- the return or approved destruction of all records at the end of a contract;
- the signing of non-disclosure agreements; and
- the use of encryption technology allowing only government officials to view the decrypted data.

Some institutions that process particularly sensitive information ensure that the information is never removed from a federal government site.

In addition, a number of institutions that have information technology contracts limit the contractor's access to data so they can only undertake testing or maintenance.

Expanded practices

In addition to the current practices in place, many institutions reported that they would implement additional mitigating measures to protect privacy as a result of the review findings.

Some indicated they would revise internal policies, practices, systems, training materials, controls, and safeguards to mitigate both existing and future unauthorized disclosure.

These revisions will include the following.

Reviews in advance of and during contracting

- The inclusion of an additional step in the solicitation checklist (used for every service contract) that asks for the review of direct and indirect risks involving personal and proprietary information;
- New internal processes to review all new agreements, including the use of multi-disciplinary teams to review proposed contracting arrangements; and

- The monitoring of all contracts where foreign companies have access to personal or other sensitive information.

Contract clauses

- The requirement that part or all of the work be completed within the institution (especially when health information is involved) or within Canada;
- Ensure that personal information or other protected or classified information is shared with third parties only where warranted;
- Consultation with legal services for all future contracts where personal or sensitive information will be exchanged or provided to third parties to consider inclusion of provisions that prevent disclosure under any foreign legislation; and
- The modification of contract forms to allow contract authorities to better assess risk.

Planning

- The development of risk management approaches related to business and personal information to mitigate risks associated with foreign legislation, which will in turn be incorporated in the institution's corporate risk management framework;
- The amendment of training plans to increase department-wide awareness of risks; and
- The exploration of technology solutions to protect information flows.

Policy guidance

The Secretariat has developed a document that provides policy guidance to assist federal institutions before they decide to become involved in contracting that includes personal or other sensitive information within Canada and across borders.

The document is meant to help institutions in first identifying and assessing potential privacy risks and then, if necessary, in taking appropriate measures. Its objective is to ensure the Government of Canada meets legal and policy obligations to safeguard personal information.

Advice on make-or-buy decisions

The guidance document emphasizes front-end protection of personal information through the use of contractual language and other measures. The idea is to put in place the necessary measures to mitigate privacy risks as much as possible before the contracting process is even initiated.

The document also reminds institutions that government policy requires that a business case be made for contracting, outlining the advantages to Canadians. If a business case is made, privacy implications are considered in consultation with appropriate internal officials—a step that must be completed before any process to acquire an outside supplier.

Other recommendations in the document include the following:

- establishing control, where appropriate, so it is understood that the information is the property of the Government of Canada;
- making contract reviews a mandatory component of each contract in the event of a change in status or ownership of the company;
- stipulating that information be kept confidential and used only for purposes related to the contract or arrangement and that other uses or disclosures are to be approved by the Government of Canada;
- making employees of contracted firms sign written confidentiality agreements;
- specifying that information is to be segregated from other company records and information holdings and shall be delivered to the Government of Canada upon request;
- specifying the involvement and responsibilities of all subcontractors, agents, consultants, and advisors; and
- stipulating that an electronic audit trail is required for information stored in a database in order to easily determine who has access and when.

The guidance document is not meant to be used in isolation of other procurement and policy advice. It also does not advocate a universal approach since the circumstances for each institution and each contracting situation are different and need to be viewed on a case-by-case basis.

Each institution is accountable for its contracting and should therefore consider measures outlined in the document in consultation with its legal and privacy advisors.

Advice on contractual clauses

The guidance document contains advice on developing appropriate clauses that can be used, where appropriate, to address the risk of potential disclosure to foreign governments. These clauses, which should be addressed in the request-for-proposal process for bidders, are especially relevant where there may be a higher level of privacy risk, as in the case of collecting and storing health, income, or personal financial information.

Before such sample clauses are used, changed, or adapted, institutions are told they must consult their legal services and privacy officials to ensure the clauses are properly used and are not in conflict with obligations under existing international agreements.

Range of clauses

The guidance document suggests various clauses that can be built into contracts to ensure enhanced privacy protection.

Canadian control: Federal institutions should ensure that the Government of Canada maintains control over the information and can request the information at any time from the contractor.

Site inspections: Contracts can allow the government institution to inspect the contractor's premises.

Permission needed: Suppliers can be obligated to always ask for approval to disclose information.

Limited access: Access to information can be limited. For example, a contract should include a clause that states the information cannot be accessed for purposes not related to the contract, including any disclosure or access by a foreign-based parent company, other affiliates, or third parties such as subcontractors and agents not directly involved in the contract or arrangement.

Auditing: Especially when personal information or other protected or classified information is being accessed, there should be a requirement to have the supplier keep an audit trail to confirm that those who accessed information had the authority to do so and to allow the government institution to conduct audits.

Notification of breach: When a contractor becomes aware of a breach of confidentiality, he or she should be contractually obligated to notify the government. The terms of the contract should encourage reporting and quick remedial action on the part of the contractor.

The contractor should be required to accept the responsibility of wrongful disclosure and pay costs associated with the appropriate notification of individuals whose information may have been disclosed. The government may also require termination of the contract if there is a breach of confidentiality.

Subcontracting: A contract can stipulate whether any subcontracting is allowed. If so, subcontractors, including those operating outside of Canada, should be accountable to the same privacy restrictions as the contractor. The federal institution can also require that its written approval be obtained before a contractor can use any subcontractors.

Privacy checklist

To assist institutions in ensuring that adequate privacy protection clauses will be included when contracting out or outsourcing a government program or service-delivery function, the guidance document includes a privacy checklist. The checklist will be made available to all federal institutions on the Secretariat's Web site as a user-friendly electronic tool.

Any single strategy is likely to be insufficient in protecting personal information from disclosure outside Canada.

Federal institutions are therefore using a combination of strategies to prevent disclosure that includes a wide range of tools, such as contractual provisions, auditing, risk assessment, and technology.

Other activities

In addition to the guidance document, the federal government is engaged in communications and consultations with organizations and individuals to share information, increase awareness about transborder data issues, and receive advice.

PIPEDA: The Privacy Commissioner of Canada is calling on Canadian businesses to continue to respect the privacy rights of Canadians concerning information the private sector possesses on individual Canadians, as legislated under PIPEDA.

Dialogue with the U.S.: Canadian and U.S. officials have discussed issues relating to cross-border information sharing. U.S. officials have been informed of the federal action plan, how Canadians perceive privacy issues and the *USA PATRIOT Act*, and the federal government's desire to have a continuing dialogue on achieving the right balance between privacy rights and effective law enforcement.

Continued co-operation between Canada and the U.S. will promote uninterrupted trade and other business between the two countries while respecting each country's concerns and needs.

Office of the Privacy Commissioner of Canada and the provinces: The Government of Canada, the Office of the Privacy Commissioner of Canada, and provincial governments are sharing information with each other and with the private sector on best practices to protect the security and privacy of Canadians and the interests of Canadian businesses.

4. Action Plan of the Privacy Commissioner of Canada

The Privacy Commissioner of Canada is also pursuing a vigorous agenda to address concerns over transborder data flows.

The Commissioner, in her August 18, 2004, submission to the Office of the information and Privacy Commissioner for B.C. (entitled *Transferring Personal Information about Canadians Across Borders—Implications of the* USA PATRIOT Act) indicated her interest in the following:

- conducting an audit of the transfer of personal information through information-sharing agreements between Canadian and U.S. departments and agencies;
- holding discussions between representatives of the Public Safety and Emergency Preparedness Canada and the U.S. Department of Homeland Security on personal information management practices of federal entities on both sides of the border;
- supporting a review and revision of the *Privacy Act*;
- pursuing the creation of a national security committee of parliamentarians; and
- participating in the 2006 legislative review of the PIPEDA, which contains privacy safeguards for the private sector.

For more information on how to protect your privacy and other planned privacy initiatives of the Privacy Commissioner of Canada, visit the Commissioner's Web site: http://www.privcom.gc.ca.

5. Building on the Existing Foundation

Protecting privacy is not new in Canada. In fact, Canada has been a world leader in privacy protection for more than 25 years.

Privacy advocates and government officials in other parts of the world have looked to Canada for leadership in privacy protection because of a series of progressive laws and policies.

The latest measures the government has introduced have been designed to build upon and complement the existing foundation, not to work in isolation from them.

Laws governing information collected by the federal government

The *Canadian Charter of Rights and Freedoms:* When the federal government outsources a government program or a service-delivery function to a private sector entity, this entity will be required to comply with the Charter in the performance of those functions. It has long been recognized that section 8 of the Charter, which protects against unreasonable searches and seizures, extends to protect informational privacy. When the federal government deals with information about which one holds a reasonable expectation of privacy, some form of reasonable lawful authority is usually required to authorize the intrusion that may be caused by the handling of such information.

The *Privacy Act:* Privacy was first legislated in 1978 under Part IV of the *Canadian Human Rights Act*, but in 1983 the *Privacy Act* was enacted. The *Privacy Act* created obligations for federal government institutions to respect the privacy rights of Canadians by placing limits on the collection, use, disclosure, retention, and disposal of personal information. It became the standard for privacy legislation in Canada forming the basis for provincial privacy laws that would follow. (See http://laws.justice.gc.ca/en/P-21/index.html.)

Other statues with privacy protection: The *Privacy Act* is not the only law protecting personal information collected by the federal government. Other laws covering specific information, such as the *Income Tax Act*, the *Statistics Act*, the *Employment Insurance Act*, the *Old Age Security Act*, and the *Canada Pension Plan*, include additional protection of the privacy of Canadians.

PIPEDA and the private sector

Companies, associations, labour unions, and non-profit groups must also operate within the law. The private sector law related to privacy is called the *Personal Information Protection and Electronic Documents Act* (PIPEDA). Starting in 2001, it was introduced in stages and was in full effect by 2004. PIPEDA applies rules to any organization involved in commercial activity for the collection, use, and disclosure of personal information. For example, under PIPEDA, a person has the right to know why a business wants to collect their personal information. Where provinces have privacy laws that are substantially similar to PIPEDA, these govern provincially regulated private sector operations within their borders. (See http://laws.justice.gc.ca/en/P-8.6.)

Federal policies

In addition to laws, the federal government also operates under a series of policies and guidelines. Many of these include the consideration of privacy before proceeding with a government program, service, or contract.

***Privacy Impact Assessment Policy*:** The Government of Canada became the first national government in the world to make privacy a mandatory consideration in the creation or changing of government programs and services that collect personal information. Federal institutions must conduct a privacy impact assessment to learn how privacy may be affected, identify any risks to privacy, and create a plan to mitigate those risks. (See http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/siglist_e.asp.)

***Government Security Policy*:** Security is also part of the existing framework. Without a secure infrastructure in place to keep information safe and prevent it from being tampered with or accessed by unauthorized personnel, privacy is at risk. The *Government Security Policy* outlines procedures for the safeguarding and storage of information. (See http://www.tbs-sct.gc.ca/pubs_pol/gospubs/TBM_12A/gsp-psg_e.asp.)

Additional policies: A wide range of other policies protects both the privacy and security of personal and sensitive information. These include policies on the management of government information, contracting, and risk management.

Roles of federal institutions

In addition to laws and policies, certain federal organizations have mandates that further aid in the protection of privacy and security.

Public Works and Government Services Canada (PWGSC): PWGSC carries out physical on-site inspections of premises that store information under the government's control. These premises must receive a government issued security clearance prior to handling government information and any person with access to the information must also be security cleared.

Office of the Privacy Commissioner of Canada: The Privacy Commissioner of Canada looks out for the privacy rights of Canadians. The Commissioner can investigate complaints that are made under either the *Privacy Act* or PIPEDA. The Commissioner also serves as an advocate for privacy rights, carries out privacy research, and publishes information about privacy best practices. Upon reasonable grounds, the Commissioner also has the power to audit the information practices of organizations in the private sector.

Federal experience and expertise

Over the years, the federal government has acquired a great deal of experience and expertise in protecting personal information leading to the development of best practices.

A good example of this is the Government On-Line Initiative (GOL). GOL has successfully acquired the trust of Canadians concerned about on-line security and confidentiality. In fact, 70 per cent of Canadians in a recent survey said they used a Government of Canada Web site in the past 12 months.

GOL has earned this trust as a result of a communications infrastructure known as "Secure Channel," which allows secure and reliable electronic transactions with federal departments. Canadians can obtain an epass, a set of electronic credentials that allow secure two-way transmission of sensitive information.

Good communication through privacy statements and notices on department and agency Web sites also contributes to building trust. Such statements and notices tell individuals about the institution's privacy policies and inform visitors of how their personal information will be used before they provide it.

For more information on the existing foundation, please see Appendix B.

6. Follow-up Actions—The Way Ahead

Risk management is a continuous process. Consequently, the Government of Canada's work on the *USA PATRIOT Act* and the larger issue of transborder data flows will extend beyond the publication of this report.

Steps will be taken to ensure that federal institutions continue to monitor risks and that risk mitigation and avoidance strategies are in place.

The following is a list of measures that the government will undertake in the short- (zero to six months), medium- (six months to a year), and long-term (one to two years).

Federal institutions

Federal institutions have an ongoing responsibility to ensure that their risk mitigation strategies related to the *USA PATRIOT Act* are in place and that they have taken concrete steps to identify and minimize potential privacy risks when considering future contract needs.

1. The Secretariat

Ongoing and within six months

1.1 Continue meeting with the seven federal institutions that identified some contracts that were rated in the "medium to high risk" category in order to assess if implementation plans are commensurate with the risks identified in the institution's comprehensive assessments;

1.2 Provide general advice and support for all federal institutions on departmental risk implementation plans; and

1.3 Disseminate guidance on the *USA PATRIOT Act* and other similar foreign legislation to government security experts as part of the recently revised standard under the *Government Security Policy* entitled *Security and Contracting Management Standard.*

Six months to one year

1.4 Launch a government-wide assessment approximately one year following the distribution of this report, to determine

- the level of success of implementation of the measures recommended in the guidance document; and

- whether risk exposure for the *USA PATRIOT Act* and transborder data flows has decreased, remained static, or increased since the original assessment.

1.5 Issue guidance to federal institutions on information-sharing agreements to address the broader issue of how Canadians' personal information is being shared with other jurisdictions within Canada and with other countries. The guidance will help to ensure that the personal information of Canadians is treated with at least the same standard of privacy measures mandated in federal legislation and policies for government-to-government information sharing within Canada and abroad.

1.6 Provide best practices in building privacy into design through technological and architectural solutions, such as the use of encryption, the segregation of databases, and audit trails based on consultations with other jurisdictions and the private sector.

1.7 Develop, in collaboration with the internal auditing community, an internal audit guide to assess privacy in contracting.

One to two years

1.8 Design, develop, and communicate a privacy management framework that sets out the Government of Canada's privacy vision and strategy. The Framework will provide the foundation for a comprehensive privacy risk management and accountability infrastructure that will ensure that there is a balance between the privacy rights of individuals and the requirement to fulfill other public interest goals and program mandates. Ultimately, it will establish high standards of privacy protection. This work is to be carried out in partnership with the Office of the Privacy Commissioner of Canada.

2. Industry Canada

Within six months

2.1 Work with the Office of the Privacy Commissioner of Canada to develop tools and identify opportunities for increasing awareness of transborder data flow issues among businesses and the general public.

One to two years

2.2 Lead work on the recently announced Security and Prosperity Partnership of North America (SPP), a trilateral agreement between the governments of Canada, Mexico, and the U.S. The *Framework of Common Principles for Electronic Commerce with Mexico and the United States*, agreed to under the SPP in June 2005, includes a work element respecting privacy and transborder data flows. Potential issues for discussion include

common approaches to the protection of personal information, the balance between privacy and security, and the need for transparency and oversight in the use of personal information for law enforcement and national security purposes.

2.3 In 2006, PIPEDA is scheduled to be reviewed by a parliamentary committee. The review will provide the opportunity to discuss the effectiveness of PIPEDA to address a variety of privacy issues and concerns.

3. Department of Justice Canada

One to two years

3.1 The Department of Justice Canada will continue its ongoing review and assessment of its privacy laws, including the *Privacy Act*. If the Government of Canada determines that the *Privacy Act* is to be renewed, the department will work with the Secretariat and other stakeholders to determine if the reformed Act should define the responsibilities and potential requirements of those who transfer personal information outside the public sector and outside Canada.

3.2 The Department of Justice Canada will work in close collaboration with the Secretariat to ensure that the Secretariat develops and launches policy guidance on information-sharing agreements and contractual arrangements that reflect appropriate privacy protective measures to address the broader issue of how the personal information of Canadians is being shared with other jurisdictions within Canada and with other countries.

4. Public Works and Government Services Canada

Within six months

4.1 Communicate and make available the sample clauses and contracting guidance or advice to all PWGSC procurement officers.

4.2 Build awareness of the *USA PATRIOT Act* and the issue of transborder data flows by covering these topics in the current privacy training module of the Security in Contracting course designed for PWGSC procurement officers.

5. Canada School of Public Service

Six months to a year

5.1 Develop and deliver courses and modules to build awareness about privacy, transborder data flows, and contracting for all levels of employees and for all communities of practice (including information technology specialists, privacy specialists, business program managers, and policy experts). A similar program has been undertaken for information management in government.

Appendix A: Detailed Review Table

Institution	No Risk	Low Risk	Low to Medium Risk	Medium to High Risk
Agriculture and Agri-Food Canada	X			
Atlantic Canada Opportunities Agency	X			
Atlantic Pilotage Authority Canada	X			
Bank of Canada		X		
Belledune Port Authority	X			
Blue Water Bridge Authority		X		
British Columbia Treaty Commission	X			
Business Development Bank of Canada			X	
Canada Border Services Agency		X		
Canada Council for the Arts		X		
Canada Deposit Insurance Corporation		X		
Canada Firearms Centre		X		
Canada Industrial Relations Board	X			
Canada Lands Company Limited		X		
Canada Mortgage and Housing Corporation		X		
Canada-Newfoundland Offshore Petroleum Board	X			
Canada-Nova Scotia Offshore Petroleum Board	X			
Canada Post Corporation				X
Canada Revenue Agency		X		
Canada School of Public Service	X			
Canada Science and Technology Museum			X	
Canadian Air Transport Security Authority			X	
Canadian Artists and Producers Professional Relations Tribunal	X			
Canadian Centre for the Independent Resolution of First Nations Specific Claims	X			
Canadian Centre for Occupational Health and Safety	X			
Canadian Commercial Corporation			X	
Canadian Cultural Property Export Review Board	X			
Canadian Dairy Commission		X		
Canadian Environmental Assessment Agency	X			
Canadian Food Inspection Agency				X
Canadian Forces Grievance Board	X			
Canadian Grain Commission	X			
Canadian Heritage	X			
Canadian Human Rights Commission		X		
Canadian Human Rights Tribunal	X			
Canadian Institutes of Health Research		X		

Institution	No Risk	Low Risk	Low to Medium Risk	Medium to High Risk
Canadian International Development Agency			X	
Canadian International Trade Tribunal		X		
Canadian Museum of Civilization	X			
Canadian Museum of Nature			X	
Canadian Nuclear Safety Commission			X	
Canadian Polar Commission	X			
Canadian Radio-television and Telecommunications Commission		X		
Canadian Security Intelligence Service		X		
Canadian Space Agency		X		
Canadian Tourism Commission		X		
Canadian Transportation Agency		X		
Canadian Wheat Board		X		
Citizenship and Immigration Canada			X	
Commission for Public Complaints Against the Royal Canadian Mounted Police	X			
Communications Security Establishment			X	
Copyright Board Canada		X		
Correctional Service Canada			X	
Courts Administration Service		X		
Defence Construction Canada	X			
Department of Finance Canada	X			
Department of Justice Canada				X
Economic Development Agency of Canada for the Regions of Quebec	X			
Elections Canada		X		
Environment Canada			X	
Export Development Canada			X	
Farm Credit Canada		X		
Federal Bridge Corporation Limited	X			
Financial Consumer Agency of Canada Note: Responses provide examples of confidentiality agreements and contract clauses		X		
Financial Transactions and Reports Analysis Centre of Canada	X			
Fisheries and Oceans Canada			X	
Foreign Affairs Canada Note: The response from Foreign Affairs Canada/International Trade Canada covers contract categories common to all federal institutions.				X
Fraser River Port Authority	X			
Freshwater Fish Marketing Corporation		X		

Institution	No Risk	Low Risk	Low to Medium Risk	Medium to High Risk
Great Lakes Pilotage Authority Canada	X			
Gwich'in Land and Water Board	X			
Gwich'in Land Use Planning Board	X			
Halifax Port Authority		X		
Hamilton Port Authority	X			
Hazardous Materials Information Review Commission Canada	X			
Health Canada Note: The recently created Public Health Agency of Canada is covered under Health Canada			X	
Historic Sites and Monuments Board of Canada	X			
Human Resources and Skills Development Canada		X		
Immigration and Refugee Board		X		
Indian and Northern Affairs Canada		X		
Indian Residential Schools Resolution Canada	X			
Indian Specific Claims Commission Note: Indicated “no risk” although not required to respond				
Industry Canada				X
Infrastructure Canada		X		
International Centre for Human Rights and Democratic Development	X			
International Development Research Centre			X	
International Trade Canada (See Foreign Affairs Canada)				X
Laurentian Pilotage Authority Canada	X			
Law Commission of Canada		X		
Library and Archives Canada	X			
Mackenzie Valley Environmental Impact Review Board		X		
Mackenzie Valley Land and Water Board	X			
Military Police Complaints Commission of Canada	X			
Montreal Port Authority		X		
Nanaimo Port Authority		X		
National Arts Centre		X		
National Capital Commission	X			
National Defence			X	
National Energy Board		X		
National Farm Products Council	X			
National Film Board		X		
National Gallery of Canada	X			
National Parole Board	X			
National Research Council Canada	X			

Institution	No Risk	Low Risk	Low to Medium Risk	Medium to High Risk
National Round Table on the Environment and the Economy	X			
Natural Resources Canada			X	
North Fraser Port Authority	X			
Northern Pipeline Agency Canada	X			
Northwest Territories Water Board	X			
Nunavut Water Board		X		
Office of the Auditor General of Canada Note: A policy issue concern was expressed about personal information handled under PWGSC contracts common to all institutions (travel, AMEX, etc.)		X		
Office of the Commissioner of Official Languages	X			
Office of the Correctional Investigator	X			
Office of the Inspector General, CSIS Note: See Public Safety And Emergency Preparedness Canada	X			
Office of the Ombudsman, National Defence and Canadian Forces	X			
Office of the Superintendent of Financial Institutions Canada	X			
Pacific Pilotage Authority Canada	X			
Parks Canada	X			
Patented Medicine Prices Review Board	X			
Pension Appeals Board	X			
Port Alberni Port Authority	X			
Prince Rupert Port Authority		X		
Privy Council Office	X			
Public Safety and Emergency Preparedness Canada	X			
Public Service Commission of Canada	X			
Public Service Human Resources Management Agency of Canada	X			
Public Service Integrity Office	X			
Public Service Staff Relations Board Note: Replaced by the Public Service Labour Relations Board in the spring of 2005		X		
Public Works and Government Services Canada				X
Quebec Port Authority	X			
RCMP External Review Committee	X			
Royal Canadian Mint	X			
Royal Canadian Mounted Police		X		
Saguenay Port Authority		X		
Sahtu Land and Water Board	X			
Sahtu Land Use Planning Board	X			
Saint John Port Authority		X		
Science and Engineering Research Canada	X			

Institution	No Risk	Low Risk	Low to Medium Risk	Medium to High Risk
Security Intelligence Review Committee	X			
Sept-Îles Port Authority			X	
Social Development Canada		X		
Social Sciences and Humanities Research Council of Canada	X			
St. John's Port Authority		X		
Standards Council of Canada		X		
Statistics Canada	X			
Status of Women Canada	X			
Telefilm Canada		X		
The Jacques Cartier and Champlain Bridges Incorporated		X		
The National Battlefields Commission	X			
The Seaway International Bridge Corporation, Ltd.		X		
Thunder Bay Port Authority		X		
Toronto Port Authority		X		
Transport Canada		X		
Transportation Safety Board of Canada	X			
Treasury Board of Canada Secretariat		X		
Trois-Rivières Port Authority	X			
Vancouver Port Authority		X		
Veterans Affairs Canada			X	
Western Economic Diversification Canada		X		
Windsor Port Authority		X		
Yukon Surface Rights Board	X			
Total	77	57	19	7

100-per-cent response rate

Appendix B: Existing Foundation Details

1. Transborder data flow goes back in time

In 1987, the House of Commons Standing Committee on Justice and Human Rights and the Solicitor General of Canada reported on a three-year review of Canada's *Privacy Act*.

The committee recommended a study be conducted on transborder data flows related to the personal information of Canadians. The government commissioned such a study, which was released in 1990. It confirmed that there were significant flows of personal information moving to other countries. Since that time transborder data flows have increased dramatically.

The study was the first official confirmation of a potential problem for Canada and, in the years that followed, the federal government introduced and applied a series of safeguards, which are today being reviewed and updated.

2. How personal information is kept

Some Canadians believe that the federal government has a single file of information about them or that it is all contained in one database. In fact, each federal institution that collects, stores, and uses personal information keeps its own separate files for each of the government programs and services for which the information is needed. There are a number of files depending on what type of contact individuals have had with the government.

Each institution is responsible for the information under its control and must not share that information with outside parties or even each other, unless so authorized under Canada's *Privacy Act*.

The Secretariat disseminates *Info Source* publications each year, two of which contain personal information bank (PIB) descriptions that provide a summary of the types of information about individuals that is held by each federal institution. One *Info Source* publication describes PIBs relating to information about federal employees. The second *Info Source* publication contains PIB descriptions relating to all other individuals about whom the federal government holds information.

The publications are available for viewing at http://www.infosource.gc.ca/index_e.asp.

3. The *Privacy Act*

The Government of Canada's enactment of Part IV of the *Canadian Human Rights Act* in 1978, later replaced by the *Privacy Act* in 1983, illustrated its recognition of the importance of the protection of individual privacy and set the standard for similar privacy laws in the provinces.

Canada's *Privacy Act* imposes obligations on federal government institutions (all federal departments, most federal agencies, and some Crown corporations) to respect the privacy rights of Canadians by placing limits on the collection, use, disclosure, retention, and disposal of personal information.

Under the *Privacy Act*, Canadians have the right to access information that is being kept about them and to request corrections if they feel their personal information is out of date or inaccurate.

The *Privacy Act* is based upon internationally accepted principles for protecting personal information that state that every individual should have the right to know the following:

- what personal information is being collected about him or her;
- when and how the personal information will be disposed of;
- how the personal information will be used;
- under what circumstances the personal information can be disclosed; and
- how to obtain access to correct personal information on file.

4. Other statutes

The *Privacy Act* is not the only statute protecting personal information under the control of the Government of Canada. Section 8 of the *Canadian Charter of Rights and Freedoms* can afford further protection with respect to the handling of personal information.

Many other laws that govern how the federal government handles personal information also contain privacy measures, many of which provide additional protection.

For example, certain categories of personal information receive additional protection under such statutes as the *Income Tax Act*, the *Statistics Act*, the *Employment Insurance Act*, the *Old Age Security Act*, and the *Canada Pension Plan*.

5. *Privacy Impact Assessment Policy*

In 2002, the Government of Canada became the first national government in the world to make privacy a mandatory consideration in the changing or creating of government programs and services that collect personal information.

The *Privacy Impact Assessment Policy* requires that federal institutions conduct a thorough analysis that identifies any actual or potential effects on privacy. The policy further requires that a plan be put into place explaining how any potential privacy risks will be reduced or eliminated.

A series of guidelines accompany the policy designed to help government institutions make their assessments for identifying and addressing privacy issues before they become actual problems.

In some cases, funding for a government program can be denied until a proper assessment is conducted and all institutions must make the results of their assessments public.

6. Secretariat policies and guidance

The Secretariat, in its capacity of providing recommendations and advice to the Treasury Board, oversees a range of policies, directives, guidelines, and regulations.

In addition to the *Privacy Impact Assessment Policy*, the Secretariat is responsible for the following:

- *Policy on Privacy and Data Protection*
- *Contracting Policy*
- *Risk Management Policy*
- *Integrated Risk Management Framework*; and
- *Government Security Policy.*

7. Security measures

The existing federal foundation addresses not only privacy but also the security of data. Without a secure infrastructure in which to keep information, privacy is at risk. Both are therefore important and complement each other.

Canada's *Government Security Policy* and security provisions for government contracting work are designed to keep personal information secure.

All federal government institutions must adhere to the *Government Security Policy* when sharing Government of Canada information. This policy contains procedures for safeguarding and storing information, and the policy and related security standards must be followed when contracting out.

8. Public Works and Government Services Canada

Public Works and Government Services Canada (PWGSC) plays a major role in the security of government-held information.

PWGSC carries out physical on-site inspections of private company premises used to store information under government control. Such premises must receive a security clearance, and all employees with access to the information must be cleared to the level of reliability status.

If information leaves Canada, PWGSC ensures that the company (and its employees) in the other country meets the Government of Canada's security requirements.

PWGSC is responsible for the following contracting and security-related documents:

- *Standard Acquisition Clauses and Conditions Manual*; and
- *Industrial Security Manual*

9. The private sector and the *Personal Information Protection and Electronic Documents Act*

So far, this document has focussed on safeguards that apply only to information under the control of the federal government.

Millions of transactions also take place in the private sector daily.

Personal Information Protection and Electronic Documents Act

The federal law that protects personal information held by the private sector is called the *Personal Information Protection and Electronic Documents Act* (PIPEDA).

PIPEDA applies to all private organizations, including companies, associations, labour groups, and non-profit groups.

PIPEDA came into force in three stages. The first, in 2001, applied to federal undertakings or businesses, such as banks, airlines, and railways. In 2002, the Act was extended to cover personal health information. The final stage, in 2004, extended rules for the collection, use, and disclosure of personal information to any organization engaged in commercial activity.

Some of the major rules under PIPEDA include the following:

- PIPEDA requires that organizations inform individuals about the purpose for which they are collecting, using, or disclosing their personal information, such as name, age, medical records,

marital status, and income. Under PIPEDA, organizations are also obligated, upon request, to inform individuals of the information the organization holds about them and to comply with any request that inaccuracies be corrected.

- Businesses must obtain the individual's consent when they collect, use, or disclose personal information, except in some circumstances, such as information needed for an investigation or an emergency where lives or safety are at risk.
- In situations where an organization is outsourcing the processing of personal information to a third party, the organization is required to ensure, through contractual means, that the information is protected according to the requirements of PIPEDA. This obligation exists regardless of the geographical location of the third party, be it in Canada or abroad.
- Organizations are required to establish security safeguards to ensure that the personal information that is in their custody is protected from unauthorized access, use, or disclosures, as well as copying or modifications.
- Under PIPEDA, individuals may complain to the Privacy Commissioner of Canada about how organizations handle their personal information.

Alberta, B.C., and Quebec have privacy laws that are substantially similar to PIPEDA. Organizations subject to these laws have been exempted from PIPEDA for transactions that occur within those provinces. PIPEDA continues to apply to the cross-border movement of information that takes place in the course of commercial activity. PIPEDA also continues to apply to federally regulated organizations, such as telecommunications companies, radio-broadcasters, banks, and airlines.

10. Office of the Privacy Commissioner of Canada

The Privacy Commissioner of Canada is an officer of Parliament who reports directly to the House of Commons and the Senate.

The Commissioner is an advocate for the privacy rights of Canadians with powers that include the following:

- investigating complaints and conducting audits and compliance reviews under two federal laws the *Privacy Act* and the PIPEDA;
- publishing information about personal information-handling practices in the public and private sector;
- conducting research into privacy issues; and
- under PIPEDA, promoting awareness and understanding of privacy issues by the Canadian public.

The Privacy Commissioner of Canada works independently from any other part of the government to investigate complaints from individuals with respect to the federal public sector and the private sector.

11. Federal government on-line experience

In addition to the existing framework of privacy safeguards mentioned previously, the Government of Canada also has a great deal of experience in protecting on-line information. In fact, Canada has been recognized as a world leader in making government programs and services available over the Internet.

Government On-Line

Canada's Government On-Line (GOL) Initiative started in 1999, and today 34 federal government departments and agencies provide citizens and businesses with access to a wide range of quality, seamless electronic government services.

The Government of Canada understands that seeking and maintaining the trust of Canadians is paramount to the successful delivery of on-line services. Levels of confidence in terms of security and privacy have a significant effect on Canadians' adoption and use of government services provided through the Internet channel.

In a December 2004 public opinion study on government service and satisfaction, 75 per cent of respondents said the security and confidentiality of personal information was the most important aspect of conducting business on-line.

Other survey results show that GOL has earned the trust of Canadians. The following data are taken from a study conducted by EKOS Research Associates Inc. in 2003 entitled *Rethinking the Information Highway*.

- 53 per cent of Canadians expect they will do most of their transactions with the Government of Canada over the Internet or using e-mail in the next five years;
- 70 per cent of Internet users have used a Government of Canada Web site in the past 12 months;
- 1.2 million Canadians visit the Canada Site every month;
- 34 per cent of Canadians say their most recent contact with the Government of Canada was over the Internet; and
- users of Government of Canada services on the Internet report an 80-per-cent satisfaction rating of these services.

Secure Channel and epass

Secure Channel is a portfolio of infrastructure services that forms the foundation of GOL. Its primary goals are to provide citizens and businesses with secure, private on-line access to all federal government services.

Secure Channel allows

- cross-departmental and cross-jurisdictional service delivery;
- protection of government information technology services from Internet-based security attacks; and
- a suite of value-added services to support delivery of on-line services.

Within the Secure Channel is epass, a system that confirms Internet users are who they say they are and assures users that they are dealing with the government organization with which they want to deal.

To get an epass, clients validate their identity using shared secrets (information that only they and the department or agency in question know); then they choose a user identification and password.

Using an epass, clients can send personal information through the Internet, knowing that only the intended recipients will receive it. They can even electronically sign documents, making it unnecessary to go to an office to complete a transaction. An epass also makes it easier for clients to navigate between various on-line services because they do not have to register more than once with each program or remember multiple passwords if they choose to use the same epass for all programs.

The Government of Canada has issued over 900,000 epasses to Canadians.

Privacy notices

Canadians are kept informed about the privacy policies of each government institution through privacy notices, which are mandatory on every government Web site.

In addition to general notices, a privacy notice statement appears before every request for personal information. This statement notifies the Web site user why the information is needed, how it will be collected, stored, and disclosed, and then asks for the user's consent before the transaction is completed.

The statements appear as a first step in filling out any application form on a Government of Canada Web site providing information necessary to make an informed decision about whether to apply for a government program or service over the Internet, choose another communication channel, such as the telephone, or to opt out entirely if the program or service is voluntary.