

# **Public Sector Security Classification Guideline**

7 September 2004

Prepared for the Public Sector CIO Council by

the National CIO Council Subcommittee for Information Protection (NCSIP)

to

Facilitate the Sharing of Electronic Information between Provincial, Territorial,  
Municipal, and Government of Canada Jurisdictions

## **Table of Contents**

1.0	INTRODUCTION	1
	1.1 Security Classification Objective and Scope	1
	1.2 Other Factors to Consider in Protecting Information Assets	1
	1.3 Security Classification Development Methodology	2
	1.4 Background and Justification	2
2.0	CLASSIFICATION SCHEMA	4
	2.1 Classification Table	4
3.0	APPLYING THE SECURITY CLASSIFICATION GUIDELINE	7
	3.1 Applying the Guideline	7
	3.2 Other Operating Issues	7

## **1.0 INTRODUCTION**

### **1.1 Security Classification Objective and Scope**

This Public Sector Security Classification Guideline was developed to facilitate the sharing of electronic information between provincial, territorial, municipal, and Government of Canada jurisdictions. Specifically, this guideline serves as a common reference point so that governments wishing to share electronic information may cross reference their own classification rating to this guideline. Once this is done, jurisdictions can then determine if there is a difference in their ratings then they can agree on any necessary changes or adopt a mutually agreeable combination of security measures and processes. This document provides an initial first step in the risk management of the sharing of electronic information.

This document is not a mandatory standard but is rather a guideline approved by the Public Sector CIO Council (PSCIOC) to be applied by governments on a voluntary basis to facilitate the sharing of electronic information between government jurisdictions. This schema is not intended to impinge upon the classification schemas or security approaches of individual governments. However, governments may adopt this particular classification schema if they wish. The establishment of a commonly understood and accepted Public Sector Security Classification Guideline is required to protect sensitive electronic information that participating jurisdictions wish to exchange.

This guideline is primarily intended for information that is not classified in the national interest (i.e. Confidential Secret, Top Secret). Although this schema does not preclude the sharing of federal classified information with provinces and territories, additional requirements to satisfy the Government of Canada security policy apply. These include:

- security screening (clearance),
- need-to-know,
- appropriate security safeguards, and
- an MOU.

### **1.2 Other Factors to Consider In Protecting Information Assets**

A wide range of criteria needs to be taken into consideration when protecting information assets. These could include financial criteria, privacy requirements, access to information, national security, intellectual property, cabinet confidences, etc. The intent of this guideline is to support security requirements associated with exchanging electronic information across governments. It should be viewed as one part of a suite of tools that need to be considered for interjurisdictional service delivery. For example, other tools could include information sharing agreements, authentication schemes, and

privacy impact assessments. In particular, the PSCIOC has developed a separate guide for interjurisdictional privacy impact assessments.

It is important to note that it is possible for specific legislative requirements to conflict with the classification schema. For example, the confidentiality provisions of some legislation may designate specified information a higher level of protection and the security classification may have to be adjusted accordingly.

### **1.3 Security Classification Development Methodology**

The development of the Public Sector Security Classification Guideline involved the participation of representatives from the provincial and territorial governments, Municipal Information Systems Association (MISA), and Government of Canada. The process followed a risk assessment approach based on determining the impact of a loss to integrity, availability or confidentiality in the information systems of participating jurisdictions. A questionnaire and a short presentation were also developed to assist in the collection and development of this schema. This process involved identifying a reasonable cross-section of various information assets, the threats to these assets, the probability or likelihood that a threat will occur, and if it does occur what the likely impact will be. Information technology security and business area professionals contributed to determining the number of security levels and how they are to be defined and applied. One of the consistent findings in most of the returns is the impact that 'access/freedom of information and privacy' has on the potential schema. Additionally, health and other personal information closely linked to the privacy legislation will form a major segment of information that will be handled by this guideline.

The classification work of other comparable jurisdictions was also considered. The Government of Canada has adopted a scheme to identify confidentiality of information that is sensitive to either the national, or private or non-national interests. Several provincial jurisdictions also have adopted or proposed schema(s). Freedom of Information and Privacy Acts also figure significantly in the current provincial approaches. It is noted that there are significant differences between these classification approaches. (NB: Use of the words 'classify or classification' does not suggest that the information is sensitive to the National Interest).

Finally, this document was further enhanced and edited by discussions involving the NCSIP and the National CIO Subcommittee on Privacy during 2003 and 2004.

### **1.4 Background and Justification**

In order for governments to exchange sensitive information efficiently, economically and effectively, a common and accepted interjurisdictional approach is needed to classify

electronic information based on sensitivity so that organizations can quickly and safely determine their security requirement obligations. The obligation to protect sensitive information in Canada is often driven by legislative and/or policy requirements. It is not acceptable to argue that “time was of the essence” therefore adequate measures could not be taken. Given the competitive pressures in conducting business today, even public sector organizations are finding that they must make decisions quickly and they will be exposed to liability if they are uncertain about the sensitivity of the information they are handling or what the minimum requirements would be for its protection.

Historically, a major impediment to broad based agreement on exchange of information has been the lack of common practices or guidelines from organization to organization in the security classification of information assets. Without a commonly understood framework in this area, quick and accurate decisions on the safe exchange of information are difficult. Governments require such structures to categorize information holdings that are “sensitive” to national, provincial or private interests.

Ease of information exchange is necessary for governments to meet objectives for efficient, economic and effective service delivery. Information sharing and access is needed especially in an electronic service delivery (ESD) and an electronic business (E-business) environment. These exchanges however, must be secure and timely and must also meet legislative and privacy requirements. Organizations are making significant investments in secure IT and they must protect those investments when the sharing of electronic information occurs. Additionally, legislation and policy requires that the protection of sensitive electronic information assets be guaranteed when arrangements are considered for their exchange.

In summary, when electronic information is shared with external jurisdictions that are not aware of the value or sensitivity of an information asset, it becomes essential that the classification rating be established so that the information protection requirements can be quickly understood, communicated, and acted upon.

## 2.0 CLASSIFICATION SCHEMA

Users of this Guideline will be able to map their sensitive information assets to the schema below for information sharing purposes. Once these mappings are in place much time will be saved and organizations involved in the exchange of sensitive information will be far less exposed to threats.

The schema level examples are defined in terms of confidentiality, availability, and integrity and are defined as follows<sup>1</sup>:

- Confidentiality - preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and propriety information. A loss of confidentiality is the unauthorized disclosure of information.
- Availability - ensuring timely and reliable access to and use of information. A loss of availability is the disruption of access to or use of information or an information system.
- Integrity - guarding against improper modification or destruction, and includes ensuring information non-repudiation and authenticity. A loss of integrity is the unauthorized modification or destruction of information.

### 2.1 Classification Guideline - Table 1

Level	Definition	Examples
High	<p>Could reasonably be expected to <b>cause extremely serious personal or enterprise injury</b>, including any combination of</p> <ul style="list-style-type: none"> <li>a) extremely significant financial loss,</li> <li>b) loss of life or public safety,</li> <li>c) loss of confidence in the government,</li> <li>d) social hardship,</li> </ul> <p>or</p>	<p><b>Confidentiality</b> examples include</p> <ul style="list-style-type: none"> <li>a) information on a police informant or witness protection subject,</li> <li>b) cabinet confidence,</li> <li>c) exploration data in the mineral or oil industry,</li> <li>d) information relating to a sex offender, and</li> <li>e) information relating to the case files of a major crime.</li> </ul> <p><b>Availability</b> examples include</p> <ul style="list-style-type: none"> <li>a) crisis communications during emergencies,</li> <li>b) essential police communications information, and</li> <li>c) emergency health information services.</li> </ul> <p><b>Integrity</b> examples include</p> <ul style="list-style-type: none"> <li>a) information systems used for testing food or</li> </ul>

<sup>1</sup> Standards for Security Categorization of Federal Information and Information Systems, FIPS 199, Department of Commerce, USA

	<ul style="list-style-type: none"> <li>e) major political or economic impact</li> </ul>	<ul style="list-style-type: none"> <li>water supplies that could result in loss of life or severe illness,</li> <li>b) information systems related to emergency health care,</li> <li>c) law enforcement information,</li> <li>d) extremely large financial transaction transfers, and</li> <li>e) extended loss of service resulting in the need to institute manual processes.</li> </ul>
Medium	<p>Could reasonably be expected to <b>cause serious personal or enterprise injury</b>, including any combination of</p> <ul style="list-style-type: none"> <li>a) loss of competitive advantage,</li> <li>b) loss of confidence in the government program,</li> <li>c) significant financial loss,</li> <li>d) legal action, or</li> <li>e) damage to partnerships, relationships and reputations.</li> </ul>	<p><b>Confidentiality</b> examples include</p> <ul style="list-style-type: none"> <li>a) compromise of personal medical or health information,</li> <li>b) information on a completed tax return form,</li> <li>c) information describing personal finances,</li> <li>d) eligibility information for social benefits, and</li> <li>e) disclosure of trade secrets or intellectual property.</li> </ul> <p><b>Availability</b> examples include</p> <ul style="list-style-type: none"> <li>a) payments of benefits to Canadians, and</li> <li>b) financial and management information systems.</li> </ul> <p><b>Integrity</b> examples include</p> <ul style="list-style-type: none"> <li>a) information assets relating to food or water supply that would not meet expected standards of quality and would not cause illness,</li> <li>b) information assets relating to non-emergency health care,</li> <li>c) financial transactions and payments, and</li> <li>d) information that could be used for criminal purposes (e.g., false identity or impersonation.)</li> </ul>
Low	<p>Could reasonably be expected to <b>cause significant injury to individuals or enterprises</b> including any combination of</p> <ul style="list-style-type: none"> <li>a) limited financial losses,</li> <li>b) limited impact in service level, or</li> <li>c) performance, embarrassment and inconvenience</li> </ul>	<p><b>Confidentiality</b> examples include</p> <ul style="list-style-type: none"> <li>a) basic or “tombstone” personal information,</li> <li>b) status of a government evaluation of a company product, and</li> <li>c) unauthorized release of job applicants’ names.</li> </ul> <p><b>Availability</b> example is</p> <ul style="list-style-type: none"> <li>a) denial of service resulting in status of social assistance application not being available.</li> </ul> <p><b>Integrity</b> examples include</p> <ul style="list-style-type: none"> <li>a) information assets relating to administrative information such as volume and type of customer orders and</li> </ul>

		<p>b) operational procedure assets relating to non-critical activities.</p>
<p>Un-classified</p>	<p>Will <b>not result in injury</b> to individuals, governments or to private sector institutions and <b>financial loss will be insignificant.</b></p>	<p>The type of information, if lost, changed or denied <b>would not result in injury to an individual or government organization</b></p> <p><b>Confidentiality</b> example is</p> <p>a) information of public knowledge that can be found on most government web sites and would include such information as the government telephone books, advertisements for job opportunities in the various ministries, government-wide initiatives such as Government-On-Line, public health information, job classification level and range of pay scale.</p> <p><b>Availability</b> example is</p> <p>a) certain delay to access the information is tolerable</p> <p><b>Integrity</b> example is</p> <p>a) internal information of an organization with no legal effect</p>

### **3.0 APPLYING THE SECURITY CLASSIFICATION GUIDELINE**

#### **3.1 Applying the Guideline**

The following guidance is provided in order to apply this guideline

1. A rollout process may need to be developed by jurisdictions that plan to formally adopt it. This will ensure that all relevant system owners, departments, and agencies are notified of its purpose and benefit.
2. An individual may be assigned with the responsibility of overseeing its application.

#### **3.2 Other Operating Issues**

When jurisdictions share electronic information, there are many related operating issues that require consideration and go beyond just determining the classification level of electronic information. Some of these issues are presented as guidance below:

1. Specific requirements unique to each jurisdiction, such as requirements of information classification or privacy covered by legislation, policies, or standards, may need to be documented and specified.
2. The electronic information and related storage media that is transferred shall be suitably marked and identified so that recipient organizations are able to implement the appropriate protective measures.
3. The transfer of the electronic information whether on physical media, via electronic networks, or via the Internet shall be consistent with the classification rating.
4. The storage and access of the electronic information at the recipient's site shall also be consistent with the classification rating. This may include backup measures, encryption, firewalls, intrusion detection systems and related internal or external network defences, physical protection of media and related storage devices, handling and disposal of media and printouts, user authorization and authentication, and other measures as required.
5. Specific classification issues may also need to be addressed, for example, the duration of classification ratings and including any declassification dates or triggers and any related consultation which may be necessary, such as contacting the office of origin or appropriate freedom of information or privacy co-ordinator.
6. An agreement, such as an MOU, may be necessary in more formal situations to document the terms of the arrangement and perhaps incorporating some of the

issues listed above. Legal and privacy experts need to be consulted as part of the MOU process.

In conclusion, this Security Classification Guideline will support risk management processes in selecting the appropriate safeguards, but it does not prescribe minimum safeguards. The first step in any risk management process is to identify the sensitivity of the information and other assets. The impact statements and associated injury test cited in Table 1 will assist in this process.