POLICY CONCERNING THE IDENTIFICATION AND TREATMENT OF PROTECTED ASSETS AND INFORMATION

Purpose

In accordance with the *Government Security Policy*, the National Film Board (NFB) is required to protect the confidentiality, integrity and availability of the information and assets for which it is responsible. Information and assets must be identified and categorized based on the level of potential injury that could occur if the integrity of the information and assets were compromised.

The purpose of this policy and its associated procedures is to provide standards and guidelines for identifying, classifying, categorizing, marking and protecting assets and information based on their sensitivity.

This policy deals with the identification and treatment of "protected" information: information related to other than the national interest but that requires some protection because of its confidential nature.

Please refer to the *Policy Concerning the Identification and Treatment of Classified Assets and Information* for questions relating to classified information (information related to the national interest or national security).

Application

This policy applies to all employees, managers, directors, members of the board of directors, subcontractors, contract and freelance employees and trainees at the NFB.

Applicable Policies and Legislation

- Access to Information Act (AIA)
- Privacy Act (PA)
- Government Security Policy (GSP)
- NFB personal information protection policy
- Policy and procedures relating to the identification of essential assets and information
- Policy concerning the identification and treatment of classified assets and information

Definitions

- Author - Any person who creates or collects information.
- Assets - Tangible or intangible things that have value and are required to be protected. Assets include but are not limited to information in all forms and media, networks, systems, materiel, real property, financial resources, employee trust, public confidence and international reputation. Assets may be classified or protected.
- Compromise - Unauthorized loss or disclosure, destruction, removal, modification, interruption or use of information.

- Confidentiality - Attribute of information that must not be disclosed to unauthorized individuals, because of the resulting injury to national interests, national security or other interests.
- Availability - Condition of information that must be usable on demand to support operations, programs and services.
- Integrity - Accuracy and completeness of assets and authenticity of transactions.
- Information - Any information, published material or document in a physical form that is collected, created or received and is retained as evidence in the course of complying with legal obligations or conducting business transactions.
- Classified information - Information of importance in the national interest that may qualify for an exemption or exclusion under the *Access to Information Act* or the *Privacy Act*, relating to upholding or preserving the social, political and economic stability of Canada, and including all information the compromise or unauthorized disclosure of which would reasonably be expected to cause injury to the national interest.
- Protected information - Information related to other than the national interest that may qualify for an exemption or exclusion under the *Access to Information Act* or the *Privacy Act* but that necessitates some protection.
- Value - Monetary, cultural, strategic or other worth.

Policy Statement

The policy of the NFB is to provide appropriate protection for the Assets and Information in its custody by ensuring that access to such Assets and Information is limited to authorized persons who need access to them in the course of their duties.

Policy Objective

The objective of this policy is to ensure the confidentiality of Information and Assets designated as Protected Information of the NFB.

Protection of Sensitive Assets and Information

Protection of sensitive Assets and Information is based on the principle of injury, that is, the consequences that could reasonably be expected to result from unauthorized access. The nature of such consequences may vary, but they will ordinarily have a temporary or permanent effect on the Confidentiality, Availability or Integrity of the Assets or Information, of on the Value of Assets.

For clarity, this policy will deal specifically with the Confidentiality of Information and Assets protected by the *Access to Information Act* and the *Privacy Act*. Requirements relating to Availability, Integrity and Value will be addressed in the *Policy and Procedures Relating to the Identification of Essential Assets and Information*.

Loss of Confidentiality means, generally, that an unauthorized person or persons has learned of the existence of a sensitive Asset or sensitive Information and of the nature or location of the Asset or Information or the purposes for which it is used by the NFB. An example of this situation is accidental or intentional disclosure to a person outside the NDB of information that is considered to be sensitive intellectual property (information that is confidential until it is publicly disclosed) of the government or a third party (for

example, disclosure of an invention before a patent application is filed) or confidential information concerning the position of the NFB in the negotiation of specific agreements at the national or international level.

Requirements of the Policy

Protected Information

There are three categories of protected information. The category is identified and coded based on the level of potential injury that could occur if the integrity of the Information were compromised: Protected A – low; Protected B – particularly sensitive, where there is a medium level of potential injury; Protected C – extremely sensitive, where there is a high level of potential prejudice. In case of doubt as to the classification of such Information, the Author must refer to sections 13 to 26, 68 and 69 of the *Access to Information Act* and sections 3 (definition of "personal information"), 7, 8 and 18 to 28 of the *Privacy Act*, a copy of which is attached as Appendix B.

For example, sections 13, 14, 15, 16, 21, 68 and 69 of the *Access to Information Act* deal with Information that may not be disclosed (except on certain conditions), possibly for reasons relating to the national interest. Sections 17, 18, 19, 20, 22 and 23 of the *Access to Information Act* deal with other types of Information, including Protected Information relating to the interests of individuals, among other things.

All Protected Information must be declassified when the level of protection in question is no longer necessary, in accordance with the details set out in Procedure 10 in Appendix A.

Only those employees who have the appropriate security level and need to know the Protected Information in order to perform their duties may have access to Protected Information and Assets. Accordingly, employees who require access to Protected Information may be given an appropriate security status by the competent authorities.

Where Protected Information or Assets must be shared with other governments or with foreign, international or private organizations, the Information Management Section (Strategic Planning and Government Relations Branch) must be consulted to ensure that security requirements are met in order to protect the Protected Information or Assets. Any agreement that allows for the sharing of Protected Information shall set out the specific responsibilities of the parties in relation to security, the protective measures to be taken and followed, and security procedures relating to the sharing of the information.

Responsibilities

Authors must identify and categorize the Information they create or collect, assign the appropriate security code to the Information in accordance with this policy, and declassify the Information when the protective measures applicable to the category identified are no longer required.

Managers must ensure that all Information created or collected by a service for which they are responsible is identified and categorized, classified according to the appropriate security level, in accordance with this policy, and declassified when the protective measures applicable to the category identified are no longer required. Managers must also ensure that employees have the appropriate security level before giving them access to Protected Information. The Director of Administration will be responsible for obtaining the various security levels from the government. The manager must submit all requests for such security levels together with the reasons for the request. Where a

security clearance is to be obtained for an employee an investigation must be done by the RCMP concerning the employee and the employee's family, and will include a criminal records check.

Interpretation

All questions relating to the interpretation and application of this policy must be submitted to the of Business Affairs and Legal Services or to the Access to Information Coordinator.

Procedures

The following procedures are set out in Appendix A to this policy and provide details concerning the application of this policy:

1. Classification and categorization of Assets and Information in relation to Confidentiality
2. Identification of Assets and Information in relation to Confidentiality (security classification)
3. Storage of Protected Information and Protected Assets
4. Sharing Protected Information and Protected Assets
5. Transmission of Protected Information on paper medium
6. Electronic transmission of Protected Information
7. Transmission of Protected Information by facsimile
8. Transmission of sensitive Information by telephone
9. Removal of Protected Information from the workplace
10. Declassification of Protected Information
11. Destruction of Protected Information and Protected Assets

Relevant excerpts of the *Access to Information Act* and the *Privacy Act*

Relevant excerpts from the two Acts are set out in Appendix B to this policy, for ease of reference.

Appendix A. PROCEDURES

Procedure 1. CLASSIFICATION

CLASSIFICATION AND CATEGORIZATION OF ASSETS AND INFORMATION IN RELATION TO CONFIDENTIALITY

All NFB Information and Assets must be given appropriate attention. However, certain types of Information and Assets are sensitive or have a particular Value and must be given appropriate protection. Such Information could cause injury to the national interest or to an individual or business if the integrity of the Information were compromised. The *Access to Information Act* and the *Privacy Act*, relevant excerpts of which are set out in Appendix B, provide the legal authority for denying access to certain Information, in the national interest or to protect other interests in respect of which the government has obligations. Security measures must be taken in identifying, handling, storing and destroying such Information to protect the Information and to prevent unauthorized disclosure, modification, loss or destruction.

Authors, that is, the persons who create a document or receive it from another organization, are responsible for assessing its sensitivity and assigning the appropriate security code or category, where applicable, and for subsequent declassification.

Confidentiality

Confidentiality is violated where Protected Information or Protected Assets are disclosed without authorization. Precautions taken to protect the Confidentiality of Information and Assets include the implementation of security measures to ensure that access to Protected Information and Protected Assets is limited to persons who need to access or know the Information in the course of their duties and who have the appropriate security clearance.

In the federal government, Confidentiality is based on the exemption and exclusion criteria set out in the *Access to Information Act* and the *Privacy Act*, which provide the legal authority for the departments and institutions subject to those Acts to refuse to disclose certain information. Under the *Government Security Policy*, departments must identify and categorize Information that could be subject to exemptions or exclusions under the *Access to Information Act* or the *Privacy Act*, based on the degree of injury that could result from a violation of Confidentiality. A large majority of government information is not exempted or excluded under the *Access to Information Act* or the *Privacy Act*, and that information is not ordinarily affected by provisions relating to identification and categorization for the purposes of Confidentiality unless, as a group, it must be protected, or it compromises the Confidentiality of other assets or information by inference.

With respect to Confidentiality, the *Government Security Policy* divides Assets and Information into two broad categories:

- Information and Assets the compromise of which could cause injury to the national interest or national security; and

- Information and Assets the compromise of which could cause injury to an interest other than the national interest or national security.

This policy deals with the second category of Information and Assets.

Other interests include government interests other than interests that could affect the national interest and national security, and the interests of individuals and private organizations.

Protected Information

Assets and Information that do not relate to the national interest or national security are divided into three categories based on the severity of the consequences that could result from compromise of the Assets or Information.

The three categories of Protected Information are:

(1) Protected C (extremely sensitive): applies to the very limited amount of Information that, if compromised, could cause extremely grave injury to a person, organization or government, outside the national interest or national security.

Extremely grave injury includes loss of life and extremely serious financial losses.

Examples of Protected Information - Protected C:

- Information concerning undercover agents, informers, witnesses, protected persons, etc., that could endanger their lives if disclosed;
- Information that could reveal the true identity of persons whose lives would be endangered;
- Information that could lead to a personal or business bankruptcy.

(2) Protected B (particularly sensitive): applies to Information that, if compromised, could cause serious injury to a person, organization or government, outside the national interest or national security.

Serious injury includes significant damage to reputation or loss of competitive advantage, lasting harm or embarrassment which would probably have negative effects on the reputation, financial position, safety, health or well-being of a person or organization. Such injury also includes interference in an investigation into a serious crime or in the preparation of important government policy.

Examples of Protected Information - Protected B:

- personal Information concerning individuals' medical, psychiatric or psychological history, diagnoses, treatments or test results;
- information compiled and recognizable in the course of an investigation into a possible violation of the law;
- Information describing a person's financial situation (assets, liabilities, net assets, bank balances, financial activities and history, or solvency);
- Information containing recommendations or test results, character references or performance evaluations;
- Information concerning a person's racial or ethnic origin or religious or political beliefs or the associations to which the person belongs, or any information about the person's way of life;

- Information containing personal recommendations, character references or personal evaluations;
- Information about eligibility for social benefits or the level of such benefits;
- Information about a completed income tax return.

(3) Protected A (low sensitivity): applies to Information that, if compromised, could be expected to cause injury to a person, organization or government outside the national interest or national security.

Examples of Protected Information - Protected A:

- NFB plans, programs and policies containing Information that should not be disclosed to anyone who is not authorized to receive it;
- personal information such as social insurance number, date of birth, exact salary, contact information, language profile, etc., unless disclosed in accordance with the PA;
- business information exchanged by the NFB and a contractor;
- information relating to the business interests of groups or organizations;
- information or documents relating to the effective operation of government institutions or the government itself;
- confidential information obtained from the private sector that could be used by competitors;
- architectural drawings and techniques and drawings relating to regulated areas such as telecommunications facilities or airport lands;
- third-party business information supplied on a confidential basis and treated as confidential.

Procedure 2. IDENTIFICATION AND MARKING

IDENTIFICATION OF ASSETS AND INFORMATION BASED ON CONFIDENTIALITY (SECURITY CLASSIFICATION)

The Author of a document containing Protected Information or Protected Assets is responsible for marking the document appropriately when it is created or received.

The purpose of marking the security classification of an Asset or Information is to indicate to users what protective measures must be applied to it. It promotes uniform protection when Assets or Information is shared or exchanged. When a security classification cannot be marked on it, other methods should be developed, such as operational procedures and awareness programs, to ensure that people who have access to an Asset or Information know what level of protection is necessary.

The marking must include:

- the appropriate sensitivity level;
- where applicable, the date or event at which declassification is to occur (see Procedure 10, Declassification)

Documents containing Protected Information

Protected Information must be marked PROTECTED in the upper right corner of the cover page of the document, followed by the letter C, B or A.

- Protected C, for Assets and Information that, if compromised, could be expected to cause death or extremely serious financial losses;
- Protected B, which refers to "particularly sensitive" Assets and Information and includes all personal and business information, as well as certain information relating to NFB administrative activities;
- Protected A, which refers to Assets and Information that are of low sensitivity because of the negligible consequences that would result if their Confidentiality or Integrity were compromised.

Additional Requirements

A notice is used to indicate that the Information is subject to requirements in addition to the requirements indicated by the security classification (e.g. for Canadian citizens only). Ideally, the notice should appear in the upper right, above the document's security classification.

Marking of Protected Assets or Information on special media

Electronic media

Electronic media include, but are not limited to, fixed hard disks, CDs, DVDs, diskettes, memory sticks, magnetic tapes, USB keys, etc. A security classification corresponding to the categorization of the most sensitive document retained on the electronic medium must be assigned to it. The security markings of the documents themselves must be visible on any monitor or device on which they are displayed, and the media on which they are retained must also be externally marked. Where possible, the security marking must be legible both by persons and by machines.

The Information Technology Security Officer (Administration Branch) may give advice as to how to mark various electronic media.

Graphics, maps, drawings, plans

The sensitivity level must appear beside the title box. Additional markings may be made on the outside so that they are clearly visible when the material is folded or rolled.

Photographs, motion pictures and their contents, videotapes, microfiches, negatives, transparencies and slides

Must be marked so that the recipient or observer is able to know the sensitivity level of the document.

Sound recordings

Sound recordings must contain a clear statement at the beginning and the end concerning the protection or classification of the produce in question, to inform the listener. Recordings are stored in containers or on reels on which the security markings are clearly visible.

Marking of draft documents containing Protected Information

Every draft document that contains Protected Information must be assigned the same classification level at the beginning as the final document will have, and be treated in the same manner.

Procedure 3. STORAGE

STORAGE OF PROTECTED INFORMATION AND PROTECTED ASSETS

Anyone who leaves his or her work station must first store the Protected Information in the person's possession in an appropriate safe or, where the person was working on a computer, activate the password-protected screensaver.

Information retained on paper medium

Protected Information, Protected Assets and the containers in which they are stored must be kept in areas where effective control is exercised over access in accordance with the security requirements for the category (protected) and level of protection (Protected A, Protected B or Protected C) of the Assets or Information.

"Protected A" and "Protected B" Information must be stored, at a minimum, in a locked drawer or container or a locked office to which access is restricted to persons with a need to know. All locking office equipment and doors with standard locks are approved for the storage of Assets and Information of this type.

"Protected C" Information must be stored in locked filing cabinets or safes approved by the *RCMP Security Equipment Guide* and kept in a security area.

Protected category Assets and Assets that have a Value (laptop computers, cellular telephones, petty cash boxes, etc.) must be stored in a locked drawer or container to reduce the risk of theft. It is not necessary to store laptop computers that are in locked offices in a locked filing cabinet.

When an office is on the ground floor near windows, a threat and risk assessment must be done to confirm that the security measures in place are adequate.

Information retained on electronic medium

Protected Information must be retained on the NFB's corporate network and access to that network must be subject to pre-established requirements relating to access privileges.

Protected Information should not be retained on the hard disk of a computer unless it is encrypted. When the document is completed, it should be transferred to the corporate network as soon as possible.

Only the Informatics Division (Administration Branch) may decide what type of secure encryption will be used to retain sensitive Information at the NFB.

Reference

- The *Security Equipment Catalogue* published by PWGSC contains a list of security equipment approved by the *RCMP Security Equipment Guide* for National Master Standing Offers:

http://publiservice.gc.ca/services/icpsss-spicsn/security/items-e.html

Procedure 4. SHARING INFORMATION

SHARING PROTECTED INFORMATION AND PROTECTED ASSETS

Protected Information and Protected Assets may be shared only with persons who have a need to know and have a valid security clearance / reliability status corresponding to the classification / categorization of the Assets or Information.

Sharing sensitive Information with an audience

Everyone who transmits Protected Information orally must take great care to ensure that every person in the audience has an appropriate, valid security clearance and a need to know, and should further ensure that the premises are adequately protected for the transmission of such Information.

When Protected Information must be disclosed orally, the audience must be informed of the nature of the Protected Information and of the level of security assigned to it.

Any transmission of Protected Information to an audience outside the NFB should be documented.

Sharing Protected Information and Protected Assets with other governments or organizations

When Information is disclosed to other governments or organizations, the NFB representative must ensure that there are agreements or memoranda of understanding in place providing that the organization will apply the necessary administrative, technical and physical measures to protect the Information.

Information that the NFB receives from other governments or organizations must also be retained at an appropriate level based on its Author's intent and in accordance with the agreements or memoranda of understanding that the NFB has signed with the government or organization.

Reproduction and distribution of Protected Information

When Protected Information is reproduced it is essential to keep in mind that the Information may be distributed only to persons who have a reliability status and an operational need for access to the Information. If the situation warrants, copies of Information categorized Protected C will be controlled in the same manner as Classified Information categorized Secret.

Classified Information categorized Secret may be reproduced and distributed only with the approval of the Author, the recipient of the original or either person's Director. Each copy must be numbered, the copy number must appear on the cover page of each copy, and a distribution list must be kept in the file.

Procedure 5. TRANSMISSION ON PAPER MEDIUM

TRANSMISSION OF PROTECTED INFORMATION ON PAPER MEDIUM

All Protected Information must be properly packaged and identified to avoid any intentional or accidental disclosure during shipping.

For internal mail and mail sent outside the NFB, use two sealed envelopes. Put the security classification only on the inside envelope; however, the address should appear on both envelopes. The inside envelope should be marked: "To be opened by addressee only" (in the case of Information intended for the addressee only).

Send the documents by priority post, registered mail, a private courier service or diplomatic bag. The delivery service must provide proof of sending, shipping and delivery.

An authorized employee who has an appropriate security clearance may also transport Protected Information and Protected Assets between NFB offices. The employee must be responsible for the security of the Information and Assets while they are in transit. A lockable briefcase or other secure container (with a label showing the return address or telephone number, in case of loss), must be used, unless the Information and Assets are too extensive. If the vehicle is left unsupervised, the Information and Assets must be placed in the locked trunk of the vehicle or, if that is not possible, at least out of sight in the locked vehicle.

Procedure 6. ELECTRONIC TRANSMISSION

ELECTRONIC TRANSMISSION OF PROTECTED INFORMATION

Protected Information may be transmitted to a computer that is connected to the corporate network, provided that it is first ascertained that the person who will receive the Information has a reliability status and a need to know the Information transmitted.

Information with Protected A or Protected B classification may not be transmitted to a computer outside the corporate network unless the Information has first been encrypted and the person who will receive the Information has a reliability status and a need to know the Information transmitted.

Protected C Information must not in any event be transmitted outside the NFB by e-mail.

Encryption methods

Only the Informatics Division (Administration Branch) may decide what type of secure encryption will be used to retain sensitive Information at the NFB.

Procedure 7. TRANSMISSION BY FACSIMILE

TRANSMISSION OF PROTECTED INFORMATION BY FACSIMILE

Protected Information may be transmitted by conventional facsimile, provided that the sender has first ascertained that the recipient is expecting the Information and that the

Information cannot be read by an unauthorized person or a person who does not have a need to know.

Procedure 8. TRANSMISSION BY TELEPHONE

TRANSMISSION OF SENSITIVE INFORMATION BY TELEPHONE

Cordless telephone

A cordless telephone may not be used for the transmission of sensitive Information unless it has the capability to encrypt the message and the encryption process has been approved by the NFB's Informatics Services Security Specialist (Administration Branch).

Regular telephone

A conventional telephone may not be used for the transmission of any sensitive Information.

Procedure 9. REMOVAL FROM THE WORKPLACE

REMOVAL OF PROTECTED INFORMATION FROM THE WORKPLACE

Protected Information may be temporarily removed from the workplace by an employee if the employee's authorized supervisor (director) determines that the benefit for the NFB in doing this is greater than the additional risk it involves for the security of the Information; Protected Information may be removed from the workplace only on the following conditions:

- In the case of Protected Information, written authorization (in the form of an e-mail) must first be obtained from the NFB Commissioner or the director of the employee's branch;
- a secure briefcase must be used for transporting the Information;
- the period for which the authorization is valid must be stated;
- the Information to which the authorization applies must be clearly stated;
- a copy of each authorization given must be placed in the file containing the Information to which it applies and be left there;
- the departure and return dates for the Information in question must be monitored by the person who gave the authorization;
- a copy of the Information borrowed must be placed in the file containing the Information and be left there during the period for which it is borrowed.

Procedure 10. DECLASSIFICATION

DECLASSIFICATION OF PROTECTED INFORMATION

Information must be classified "protected" only for the period for which it is necessary.

Protected Information must be declassified when the protection is no longer required.

Information in NFB possession may be declassified only by the Author or by users after consultation with the Author, together with the departmental security officer, the Director of Business Relations and Legal Services or the Access to Information Coordinator.

Changes to security classifications must be made in ink and be dated and initialled by the authority responsible for the change. When there is documentation to support the change, it must be noted on the document.

Where there is a memorandum of agreement or an agreement between the NFB and any other government, department or organization, the Information must be declassified in accordance with the terms of the agreement. Information may also be returned to the department, institution or government of origin for declassification purposes.

The Information Management Section (Strategic Planning and Government Relations Branch) must be consulted when discussions occur concerning the declassification of Information shared with a foreign government, an international organization or an institution under a memorandum of agreement or an agreement.

The Information Management Section (Strategic Planning and Government Relations Branch) must be consulted before declassifying Information relating to telecommunications security (COMSEC).

Authors of documents must arrange for automatic declassification at the time the Information is created or collected by selecting a specific date or a particular event relating to the declassification. For example, a document could be marked "Protected B until approved by Treasury Board".

In the case of electronic documents, the same information must be entered under the document's security classification.

An automatic 10-year expiry date should apply to "Protected A" Information, in addition to the specific dates and events that result in declassification. However, the automatic expiry date would not apply to "Protected B" Information, which includes individuals' personal information (for example, medical records), or "Protected C" Information (for example, information protected to protect witnesses).

The risks associated with using an automatic expiry date are acceptable, given declassifying a document is not equivalent to making the document public. The normal review process applicable to any access request continues to apply.

Protected Information and Protected Assets must be declassified when it is determined that disclosing them would create no risk of injury to an individual or business (other than the national interest). The Information may cease to be sensitive over time or on the occurrence of particular events. Declassifying a document is not equivalent to making the document public. The normal review process applicable to any access request continues to apply.

Information or Assets must be declassified to a lower level (for example, from Protected C to Protected A) if the injury to the personal or private interest has decreased. Information may also be declassified from the "Classified Information" category to the "Protected Information" category, with the appropriate security

classification, if there is no longer a risk of potential injury to the national interest but there is still a risk of injury to private interests or interests not related to the national interest.

Procedure 11. DESTRUCTION

DESTRUCTION OF PROTECTED INFORMATION AND PROTECTED ASSETS

Information on paper medium

Protected Information for which the retention period has expired must be destroyed only by the Information Management Section (Strategic Planning and Government Relations Branch) by one of the following methods:

- using an approved shredder;
- using the government's destruction services.

Information on electronic medium

Information on electronic medium for which the retention period has expired must be destroyed only by the Information Management Section (Strategic Planning and Government Relations Branch) in cooperation with Informatics Services (Administration Branch). If the Information Management Section does not have the necessary equipment or facilities, it will use the government's destruction services.

Appendix B – Relevant excerpts from the law

Access to Information Act (R.S., 1985, c. A-1)

Here are the relevant provisions applicable for the current policy.

Information obtained in confidence

13. (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Act that contains information that was obtained in confidence from

(a) the government of a foreign state or an institution thereof;

(b) an international organization of states or an institution thereof;

(c) the government of a province or an institution thereof;

(d) a municipal or regional government established by or pursuant to an Act of the legislature of a province or an institution of such a government; or

(e) an aboriginal government.

Where disclosure authorized

(2) The head of a government institution may disclose any record requested under this Act that contains information described in subsection (1) if the government, organization or institution from which the information was obtained

(a) consents to the disclosure; or

(b) makes the information public.

Definition of "aboriginal government"

(3) The expression "aboriginal government" in paragraph (1)(e) means

(a) Nisga'a Government, as defined in the Nisga'a Final Agreement given effect by the *Nisga'a Final Agreement Act*;

(b) the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the *Westbank First Nation Self-Government Act*;

(c) the Tlicho Government, as defined in section 2 of the *Tlicho Land Claims and Self-Government Act*; or

(d) the Nunatsiavut Government, as defined in section 2 of the *Labrador Inuit Land Claims Agreement Act*.

R.S., 1985, c. A-1, s. 13; 2000, c. 7, s. 21; 2004, c. 17, s. 16; 2005, c. 1, ss. 97, 107, c. 27, ss. 16, 22.

Federal-provincial affairs

14. The head of a government institution may refuse to disclose any record requested under this Act that contains information the disclosure of which could reasonably be expected to be injurious to the conduct by the Government of Canada of federal-provincial affairs, including, without restricting the generality of the foregoing, any such information

(a) on federal-provincial consultations or deliberations; or

(b) on strategy or tactics adopted or to be adopted by the Government of Canada relating to the conduct of federal-provincial affairs.

1980-81-82-83, c. 111, Sch. I "14".

International affairs and defence

15. (1) The head of a government institution may refuse to disclose any record requested under this Act that contains information the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada or the detection, prevention or suppression of subversive or hostile activities, including, without restricting the generality of the foregoing, any such information

(a) relating to military tactics or strategy, or relating to military exercises or operations undertaken in preparation for hostilities or in connection with the detection, prevention or suppression of subversive or hostile activities;

(b) relating to the quantity, characteristics, capabilities or deployment of weapons or other defence equipment or of anything being designed, developed, produced or considered for use as weapons or other defence equipment;

(c) relating to the characteristics, capabilities, performance, potential, deployment, functions or role of any defence establishment, of any military force, unit or personnel or of any organization or person responsible for the detection, prevention or suppression of subversive or hostile activities;

(d) obtained or prepared for the purpose of intelligence relating to

(i) the defence of Canada or any state allied or associated with Canada, or

(ii) the detection, prevention or suppression of subversive or hostile activities;

(e) obtained or prepared for the purpose of intelligence respecting foreign states, international organizations of states or citizens of foreign states used by the Government of Canada in the process of deliberation and consultation or in the conduct of international affairs;

(f) on methods of, and scientific or technical equipment for, collecting, assessing or handling information referred to in paragraph (d) or (e) or on sources of such information;

(g) on the positions adopted or to be adopted by the Government of Canada, governments of foreign states or international organizations of states for the purpose of present or future international negotiations;

(h) that constitutes diplomatic correspondence exchanged with foreign states or international organizations of states or official correspondence exchanged with Canadian diplomatic missions or consular posts abroad; or

(i) relating to the communications or cryptographic systems of Canada or foreign states used

(i) for the conduct of international affairs,

(ii) for the defence of Canada or any state allied or associated with Canada, or

(iii) in relation to the detection, prevention or suppression of subversive or hostile activities.

Definitions

(2) In this section, "defence of Canada or any state allied or associated with Canada"
«*défense du Canada ou d'États alliés ou associés avec le Canada* »

"defence of Canada or any state allied or associated with Canada" includes the efforts of Canada and of foreign states toward the detection, prevention or suppression of activities of any foreign state directed toward actual or potential attack or other acts of aggression against Canada or any state allied or associated with Canada;

"subversive or hostile activities"
«*activités hostiles ou subversives* »

"subversive or hostile activities" means

(a) espionage against Canada or any state allied or associated with Canada,

(b) sabotage,

(c) activities directed toward the commission of terrorist acts, including hijacking, in or against Canada or foreign states,

(d) activities directed toward accomplishing government change within Canada or foreign states by the use of or the encouragement of the use of force, violence or any criminal means,

(e) activities directed toward gathering information used for intelligence purposes that relates to Canada or any state allied or associated with Canada, and

(f) activities directed toward threatening the safety of Canadians, employees of the Government of Canada or property of the Government of Canada outside Canada.

1980-81-82-83, c. 111, Sch. I "15".

Law enforcement and investigations

16. (1) The head of a government institution may refuse to disclose any record requested under this Act that contains

(a) information obtained or prepared by any government institution, or part of any government institution, that is an investigative body specified in the regulations in the course of lawful investigations pertaining to

(i) the detection, prevention or suppression of crime,

(ii) the enforcement of any law of Canada or a province, or

(iii) activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*,

if the record came into existence less than twenty years prior to the request;

(b) information relating to investigative techniques or plans for specific lawful investigations;

(c) information the disclosure of which could reasonably be expected to be injurious to the enforcement of any law of Canada or a province or the conduct of lawful investigations, including, without restricting the generality of the foregoing, any such information

(i) relating to the existence or nature of a particular investigation,

(ii) that would reveal the identity of a confidential source of information, or

(iii) that was obtained or prepared in the course of an investigation; or

(d) information the disclosure of which could reasonably be expected to be injurious to the security of penal institutions.

Security

(2) The head of a government institution may refuse to disclose any record requested under this Act that contains information that could reasonably be expected to facilitate the commission of an offence, including, without restricting the generality of the foregoing, any such information

(a) on criminal methods or techniques;

(b) that is technical information relating to weapons or potential weapons; or

(c) on the vulnerability of particular buildings or other structures or systems, including computer or communication systems, or methods employed to protect such buildings or other structures or systems.

Policing services for provinces or municipalities

(3) The head of a government institution shall refuse to disclose any record requested under this Act that contains information that was obtained or prepared by the Royal Canadian Mounted Police while performing policing services for a province or municipality pursuant to an arrangement made under section 20 of the *Royal Canadian Mounted Police Act*, where the Government of Canada has, on the request of the province or municipality agreed not to disclose such information.

Definition of “investigation”

(4) For the purposes of paragraphs (1)(b) and (c), "investigation" means an investigation that

(a) pertains to the administration or enforcement of an Act of Parliament;

(b) is authorized by or pursuant to an Act of Parliament; or

(c) is within a class of investigations specified in the regulations.

1980-81-82-83, c. 111, Sch. I “16”; 1984, c. 21, s. 70.

Records relating to investigations, examinations and audits

16.1 (1) The following heads of government institutions shall refuse to disclose any record requested under this Act that contains information that was obtained or created by them or on their behalf in the course of an investigation, examination or audit conducted by them or under their authority:

(a) the Auditor General of Canada;

(b) the Commissioner of Official Languages for Canada;

(c) the Information Commissioner; and

(d) the Privacy Commissioner.

Exception

(2) However, the head of a government institution referred to in paragraph (1)(c) or (d) shall not refuse under subsection (1) to disclose any record that contains information that was created by or on behalf of the head of the government institution in the course of an investigation or audit conducted by or under the authority of the head of the government institution once the investigation or audit and all related proceedings, if any, are finally concluded.

2006, c. 9, s. 144.

Investigations, examinations and reviews under the *Canada Elections Act*

16.3 Subject to section 541 of the *Canada Elections Act*, the Chief Electoral Officer may refuse to disclose any record requested under this Act that contains information that was obtained or created by or on behalf of a person who conducts an investigation, examination or review in the performance of their functions under the *Canada Elections Act*.

2006, c. 9, s. 145.

Public Sector Integrity Commissioner

16.4 (1) The Public Sector Integrity Commissioner shall refuse to disclose any record requested under this Act that contains information

(a) obtained or created by him or her or on his or her behalf in the course of an investigation into a disclosure made under the *Public Servants Disclosure Protection Act* or an investigation commenced under section 33 of that Act; or

(b) received by a conciliator in the course of attempting to reach a settlement of a complaint filed under subsection 19.1(1) of that Act.

Exception

(2) Subsection (1) does not apply in respect of a record that contains information referred to in paragraph (1)(b) if the person who gave the information to the conciliator consents to the record being disclosed.

2005, c. 46, s. 55; 2006, c. 9, s. 221.

Public Servants Disclosure Protection Act

16.5 The head of a government institution shall refuse to disclose any record requested under this Act that contains information created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act* or in the course of an investigation into a disclosure under that Act.

2005, c. 46, s. 55; 2006, c. 9, s. 221.

Safety of individuals

17. The head of a government institution may refuse to disclose any record requested under this Act that contains information the disclosure of which could reasonably be expected to threaten the safety of individuals.

1980-81-82-83, c. 111, Sch. I “17”.

Economic interests of Canada

18. The head of a government institution may refuse to disclose any record requested under this Act that contains

(a) trade secrets or financial, commercial, scientific or technical information that belongs to the Government of Canada or a government institution and has substantial value or is reasonably likely to have substantial value;

(b) information the disclosure of which could reasonably be expected to prejudice the competitive position of a government institution or to interfere with contractual or other negotiations of a government institution;

(c) scientific or technical information obtained through research by an officer or employee of a government institution, the disclosure of which could reasonably be expected to deprive the officer or employee of priority of publication; or

(d) information the disclosure of which could reasonably be expected to be materially injurious to the financial interests of a government institution or to the ability of the Government of Canada to manage the economy of Canada or could reasonably be expected to result in an undue benefit to any person, including such information that relates to

(i) the currency, coinage or legal tender of Canada,

(ii) a contemplated change in the rate of bank interest or in government borrowing,

(iii) a contemplated change in tariff rates, taxes, duties or any other revenue source,

(iv) a contemplated change in the conditions of operation of financial institutions,

(v) a contemplated sale or purchase of securities or of foreign or Canadian currency, or

(vi) a contemplated sale or acquisition of land or property.

R.S., 1985, c. A-1, s. 18; 2006, c. 9, s. 146.

Personal Information

Personal information

19. (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any record requested under this Act that contains personal information as defined in section 3 of the *Privacy Act*.

Where disclosure authorized

(2) The head of a government institution may disclose any record requested under this Act that contains personal information if

(a) the individual to whom it relates consents to the disclosure;

(b) the information is publicly available; or

(c) the disclosure is in accordance with section 8 of the *Privacy Act*.

1980-81-82-83, c. 111, Sch. I "19".

Third Party Information

Third party information

20. (1) Subject to this section, the head of a government institution shall refuse to disclose any record requested under this Act that contains

(a) trade secrets of a third party;

(b) financial, commercial, scientific or technical information that is confidential information supplied to a government institution by a third party and is treated consistently in a confidential manner by the third party;

(c) information the disclosure of which could reasonably be expected to result in material financial loss or gain to, or could reasonably be expected to prejudice the competitive position of, a third party; or

(d) information the disclosure of which could reasonably be expected to interfere with contractual or other negotiations of a third party.

Product or environmental testing

(2) The head of a government institution shall not, pursuant to subsection (1), refuse to disclose a part of a record if that part contains the results of product or environmental testing carried out by or on behalf of a government institution unless the testing was done as a service to a person, a group of persons or an organization other than a government institution and for a fee.

Methods used in testing

(3) Where the head of a government institution discloses a record requested under this Act, or a part thereof, that contains the results of product or environmental testing, the head of the institution shall at the same time as the record or part thereof is disclosed provide the person who requested the record with a written explanation of the methods used in conducting the tests.

Preliminary testing

(4) For the purposes of this section, the results of product or environmental testing do not include the results of preliminary testing conducted for the purpose of developing methods of testing.

Disclosure if a supplier consents

(5) The head of a government institution may disclose any record that contains information described in subsection (1) with the consent of the third party to whom the information relates.

Disclosure authorized if in public interest

(6) The head of a government institution may disclose any record requested under this Act, or any part thereof, that contains information described in paragraph (1)(b), (c) or (d) if that disclosure would be in the public interest as it relates to public health, public safety or protection of the environment and, if the public interest in disclosure clearly outweighs in importance any financial loss or gain to, prejudice to the competitive position of or interference with contractual or other negotiations of a third party.

1980-81-82-83, c. 111, Sch. I “20”.

Operations of Government

Advice, etc.

21. (1) The head of a government institution may refuse to disclose any record requested under this Act that contains

(a) advice or recommendations developed by or for a government institution or a minister of the Crown,

(b) an account of consultations or deliberations in which directors, officers or employees of a government institution, a minister of the Crown or the staff of a minister participate,

(c) positions or plans developed for the purpose of negotiations carried on or to be carried on by or on behalf of the Government of Canada and considerations relating thereto, or

(d) plans relating to the management of personnel or the administration of a government institution that have not yet been put into operation,

if the record came into existence less than twenty years prior to the request.

Exercise of a discretionary power or an adjudicative function

(2) Subsection (1) does not apply in respect of a record that contains

(a) an account of, or a statement of reasons for, a decision that is made in the exercise of a discretionary power or an adjudicative function and that affects the rights of a person; or

(b) a report prepared by a consultant or an adviser who was not a director, an officer or an employee of a government institution or a member of the staff of a minister of the Crown at the time the report was prepared.

R.S., 1985, c. A-1, s. 21; 2006, c. 9, s. 149.

Testing procedures, tests and audits

22. The head of a government institution may refuse to disclose any record requested under this Act that contains information relating to testing or auditing procedures or techniques or details of specific tests to be given or audits to be conducted if the disclosure would prejudice the use or results of particular tests or audits.

1980-81-82-83, c. 111, Sch. I "22".

Internal audits

22.1 (1) The head of a government institution may refuse to disclose any record requested under this Act that contains a draft report of an internal audit of a government institution or any related audit working paper if the record came into existence less than fifteen years before the request was made.

Exception

(2) However, the head of a government institution shall not refuse under subsection (1) to disclose a draft report of an internal audit of a government institution if a final report of the audit has been published or if a final report of the audit is not delivered to the institution within two years after the day on which the audit was first commenced.

2006, c. 9, s. 150.

Solicitor-client privilege

23. The head of a government institution may refuse to disclose any record requested under this Act that contains information that is subject to solicitor-client privilege.

1980-81-82-83, c. 111, Sch. I "23".

Statutory Prohibitions

Statutory prohibitions against disclosure

24. (1) The head of a government institution shall refuse to disclose any record requested under this Act that contains information the disclosure of which is restricted by or pursuant to any provision set out in Schedule II.

Review of statutory prohibitions by Parliamentary committee

(2) Such committee as may be designated or established under section 75 shall review every provision set out in Schedule II and shall, not later than July 1, 1986 or, if Parliament is not then sitting, on any of the first fifteen days next thereafter that Parliament is sitting, cause a report to be laid before Parliament on whether and to what extent the provisions are necessary.

1980-81-82-83, c. 111, Sch. I "24".

Severability

25. Notwithstanding any other provision of this Act, where a request is made to a government institution for access to a record that the head of the institution is authorized to refuse to disclose under this Act by reason of information or other material contained in the record, the head of the institution shall disclose any part of the record that does not contain, and can reasonably be severed from any part that contains, any such information or material.

1980-81-82-83, c. 111, Sch. I "25".

Refusal of Access

Refusal of access where information to be published

26. The head of a government institution may refuse to disclose any record requested under this Act or any part thereof if the head of the institution believes on reasonable grounds that the material in the record or part thereof will be published by a government institution, agent of the Government of Canada or minister of the Crown within ninety days after the request is made or within such further period of time as may be necessary for printing or translating the material for the purpose of printing it.

1980-81-82-83, c. 111, Sch. I "26".

Act does not apply to certain materials

68. This Act does not apply to

(a) published material or material available for purchase by the public;

(b) library or museum material preserved solely for public reference or exhibition purposes; or

(c) material placed in the Library and Archives of Canada, the National Gallery of Canada, the Canadian Museum of Civilization, the Canadian Museum of Nature or the National Museum of Science and Technology by or on behalf of persons or organizations other than government institutions.

R.S., 1985, c. A-1, s. 68; R.S., 1985, c. 1 (3rd Supp.), s. 12; 1990, c. 3, s. 32; 1992, c. 1, s. 143(E); 2004, c. 11, s. 22.

Confidences of the Queen's Privy Council for Canada

69. (1) This Act does not apply to confidences of the Queen's Privy Council for Canada, including, without restricting the generality of the foregoing,

(a) memoranda the purpose of which is to present proposals or recommendations to Council;

(b) discussion papers the purpose of which is to present background explanations, analyses of problems or policy options to Council for consideration by Council in making decisions;

(c) agenda of Council or records recording deliberations or decisions of Council;

(d) records used for or reflecting communications or discussions between ministers of the Crown on matters relating to the making of government decisions or the formulation of government policy;

(e) records the purpose of which is to brief ministers of the Crown in relation to matters that are before, or are proposed to be brought before, Council or that are the subject of communications or discussions referred to in paragraph (d);

(f) draft legislation; and

(g) records that contain information about the contents of any record within a class of records referred to in paragraphs (a) to (f).

Definition of "Council"

(2) For the purposes of subsection (1), "Council" means the Queen's Privy Council for Canada, committees of the Queen's Privy Council for Canada, Cabinet and committees of Cabinet.

Exception

(3) Subsection (1) does not apply to

(a) confidences of the Queen's Privy Council for Canada that have been in existence for more than twenty years; or

(b) discussion papers described in paragraph (1)(b)

(i) if the decisions to which the discussion papers relate have been made public, or

(ii) where the decisions have not been made public, if four years have passed since the decisions were made.

R.S., 1985, c. A-1, s. 69; 1992, c. 1, s. 144(F).

Privacy Act P-21

Here are the relevant provisions applicable for the current policy.

Definitions

3. In this Act,

"administrative purpose"
«*fins administratives* »

"administrative purpose" , in relation to the use of personal information about an individual, means the use of that information in a decision making process that directly affects that individual;

"alternative format"
«*support de substitution* »

"alternative format" , with respect to personal information, means a format that allows a person with a sensory disability to read or listen to the personal information;

"Court"
«*Cour* »

"Court" means the Federal Court;

"designated Minister"
«*ministre désigné* »

"designated Minister" means a person who is designated as the Minister under subsection 3.1(1);

"government institution"
«*institution fédérale* »

"government institution" means any department or ministry of state of the Government of Canada listed in the schedule or any body or office listed in the schedule;

"head"
«*responsable d'institution fédérale* »

"head" , in respect of a government institution, means

(a) in the case of a department or ministry of state, the member of the Queen's Privy Council for Canada who presides over the department or ministry, or

(b) in any other case, either the person designated under subsection 3.1(2) to be the head of the institution for the purposes of this Act or, if no such person is designated, the chief executive officer of the institution, whatever their title;

"personal information"
«*renseignements personnels* »

"personal information" means information about an identifiable individual that is recorded in any form including, without restricting the generality of the foregoing,

(a) information relating to the race, national or ethnic origin, colour, religion, age or marital status of the individual,

(b) information relating to the education or the medical, criminal or employment history of the individual or information relating to financial transactions in which the individual has been involved,

(c) any identifying number, symbol or other particular assigned to the individual,

(d) the address, fingerprints or blood type of the individual,

(e) the personal opinions or views of the individual except where they are about another individual or about a proposal for a grant, an award or a prize to be made to another individual by a government institution or a part of a government institution specified in the regulations,

(f) correspondence sent to a government institution by the individual that is implicitly or explicitly of a private or confidential nature, and replies to such correspondence that would reveal the contents of the original correspondence,

(g) the views or opinions of another individual about the individual,

(h) the views or opinions of another individual about a proposal for a grant, an award or a prize to be made to the individual by an institution or a part of an institution referred to in paragraph (e), but excluding the name of the other individual where it appears with the views or opinions of the other individual, and

(i) the name of the individual where it appears with other personal information relating to the individual or where the disclosure of the name itself would reveal information about the individual,

but, for the purposes of sections 7, 8 and 26 and section 19 of the *Access to Information Act*, does not include

(j) information about an individual who is or was an officer or employee of a government institution that relates to the position or functions of the individual including,

(i) the fact that the individual is or was an officer or employee of the government institution,

(ii) the title, business address and telephone number of the individual,

(iii) the classification, salary range and responsibilities of the position held by the individual,

(iv) the name of the individual on a document prepared by the individual in the course of employment, and

(v) the personal opinions or views of the individual given in the course of employment,

(k) information about an individual who is or was performing services under contract for a government institution that relates to the services performed, including the terms of the contract, the name of the individual and the opinions or views of the individual given in the course of the performance of those services,

(l) information relating to any discretionary benefit of a financial nature, including the granting of a licence or permit, conferred on an individual, including the name of the individual and the exact nature of the benefit, and

(m) information about an individual who has been dead for more than twenty years;

"personal information bank"
«*fichier de renseignements personnels* »

"personal information bank" means a collection or grouping of personal information described in section 10;

"Privacy Commissioner"
«*Commissaire à la protection de la vie privée* »

"Privacy Commissioner" means the Commissioner appointed under section 53;

"sensory disability"
«*déficience sensorielle* »

"sensory disability" means a disability that relates to sight or hearing.

R.S., 1985, c. P-21, s. 3; 1992, c. 1, s. 144(F), c. 21, s. 34; 2002, c. 8, s. 183; 2006, c. 9, s. 181.

Use of personal information

7. Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be used by the institution except

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose; or

(b) for a purpose for which the information may be disclosed to the institution under subsection 8(2).

1980-81-82-83, c. 111, Sch. II “7”.

Disclosure of personal information

8. (1) Personal information under the control of a government institution shall not, without the consent of the individual to whom it relates, be disclosed by the institution except in accordance with this section.

Where personal information may be disclosed

(2) Subject to any other Act of Parliament, personal information under the control of a government institution may be disclosed

(a) for the purpose for which the information was obtained or compiled by the institution or for a use consistent with that purpose;

(b) for any purpose in accordance with any Act of Parliament or any regulation made thereunder that authorizes its disclosure;

(c) for the purpose of complying with a subpoena or warrant issued or order made by a court, person or body with jurisdiction to compel the production of information or for the purpose of complying with rules of court relating to the production of information;

(d) to the Attorney General of Canada for use in legal proceedings involving the Crown in right of Canada or the Government of Canada;

(e) to an investigative body specified in the regulations, on the written request of the body, for the purpose of enforcing any law of Canada or a province or carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed;

(f) under an agreement or arrangement between the Government of Canada or an institution thereof and the government of a province, the council of the Westbank First Nation, the government of a foreign state, an international organization of states or an international organization established by the governments of states, or any institution of any such government or organization, for the purpose of administering or enforcing any law or carrying out a lawful investigation;

(g) to a member of Parliament for the purpose of assisting the individual to whom the information relates in resolving a problem;

(h) to officers or employees of the institution for internal audit purposes, or to the office of the Comptroller General or any other person or body specified in the regulations for audit purposes;

(i) to the Library and Archives of Canada for archival purposes;

(j) to any person or body for research or statistical purposes if the head of the government institution

(i) is satisfied that the purpose for which the information is disclosed cannot reasonably be accomplished unless the information is provided in a form that would identify the individual to whom it relates, and

(ii) obtains from the person or body a written undertaking that no subsequent disclosure of the information will be made in a form that could reasonably be expected to identify the individual to whom it relates;

(k) to any aboriginal government, association of aboriginal people, Indian band, government institution or part thereof, or to any person acting on behalf of such government, association, band, institution or part thereof, for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada;

(l) to any government institution for the purpose of locating an individual in order to collect a debt owing to Her Majesty in right of Canada by that individual or make a payment owing to that individual by Her Majesty in right of Canada; and

(m) for any purpose where, in the opinion of the head of the institution,

(i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or

(ii) disclosure would clearly benefit the individual to whom the information relates.

Personal information disclosed by Library and Archives of Canada

(3) Subject to any other Act of Parliament, personal information under the custody or control of the Library and Archives of Canada that has been transferred there by a government institution for historical or archival purposes may be disclosed in accordance with the regulations to any person or body for research or statistical purposes.

Copies of requests under paragraph (2)(e) to be retained

(4) The head of a government institution shall retain a copy of every request received by the government institution under paragraph (2)(e) for such period of time as may be prescribed by regulation, shall keep a record of any information disclosed pursuant to the request for such period of time as may be prescribed by regulation and shall, on the request of the Privacy Commissioner, make those copies and records available to the Privacy Commissioner.

Notice of disclosure under paragraph (2)(m)

(5) The head of a government institution shall notify the Privacy Commissioner in writing of any disclosure of personal information under paragraph (2)(m) prior to the disclosure where reasonably practicable or in any other case forthwith on the disclosure, and the Privacy Commissioner may, if the Commissioner deems it appropriate, notify the individual to whom the information relates of the disclosure.

Definition of “Indian band”

(6) In paragraph (2)(k), "Indian band" means

(a) a band, as defined in the *Indian Act*;

(b) a band, as defined in the *Cree-Naskapi (of Quebec) Act*, chapter 18 of the Statutes of Canada, 1984;

(c) the Band, as defined in the *Sechelt Indian Band Self-Government Act*, chapter 27 of the Statutes of Canada, 1986; or

(d) a first nation named in Schedule II to the *Yukon First Nations Self-Government Act*.

Definition of "aboriginal government"

(7) The expression "aboriginal government" in paragraph (2)(k) means

(a) Nisga’a Government, as defined in the Nisga’a Final Agreement given effect by the *Nisga’a Final Agreement Act*;

(b) the council of the Westbank First Nation;

(c) the Tlicho Government, as defined in section 2 of the *Tlicho Land Claims and Self-Government Act*; or

(d) the Nunatsiavut Government, as defined in section 2 of the *Labrador Inuit Land Claims Agreement Act*.

Definition of "council of the Westbank First Nation"

(8) The expression "council of the Westbank First Nation" in paragraphs (2)(f) and (7)(b) means the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the *Westbank First Nation Self-Government Act*.

R.S., 1985, c. P-21, s. 8; R.S., 1985, c. 20 (2nd Supp.), s. 13, c. 1 (3rd Supp.), s. 12; 1994, c. 35, s. 39; 2000, c. 7, s. 26; 2004, c. 11, s. 37, c. 17, s. 18; 2005, c. 1, ss. 106, 109, c. 27, ss. 21, 25.

Governor in Council may designate exempt banks

18. (1) The Governor in Council may, by order, designate as exempt banks certain personal information banks that contain files all of which consist predominantly of personal information described in section 2l or 22.

Disclosure may be refused

(2) The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that is contained in a personal information bank designated as an exempt bank under subsection (1).

Contents of order

(3) An order made under subsection (1) shall specify

(a) the section on the basis of which the order is made; and

(b) where a personal information bank is designated that contains files that consist predominantly of personal information described in subparagraph 22(1)(a)(ii), the law concerned.

1980-81-82-83, c. 111, Sch. II “18”.

Responsibilities of Government

Personal information obtained in confidence

19. (1) Subject to subsection (2), the head of a government institution shall refuse to disclose any personal information requested under subsection 12(1) that was obtained in confidence from

(a) the government of a foreign state or an institution thereof;

(b) an international organization of states or an institution thereof;

(c) the government of a province or an institution thereof;

(d) a municipal or regional government established by or pursuant to an Act of the legislature of a province or an institution of such a government; or

(e) the council, as defined in the Westbank First Nation Self-Government Agreement given effect by the *Westbank First Nation Self-Government Act*.

Where disclosure authorized

(2) The head of a government institution may disclose any personal information requested under subsection 12(1) that was obtained from any government, organization or institution described in subsection (1) if the government, organization or institution from which the information was obtained

(a) consents to the disclosure; or

(b) makes the information public.

R.S., 1985, c. P-21, s. 19; 2004, c. 17, s. 19.

Federal-provincial affairs

20. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) the disclosure of which could reasonably be expected to be injurious to the conduct by the Government of Canada of federal-provincial affairs.

1980-81-82-83, c. 111, Sch. II "20".

International affairs and defence

21. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) the disclosure of which could reasonably be expected to be injurious to the conduct of international affairs, the defence of Canada or any state allied or associated with Canada, as defined in subsection 15(2) of the *Access to Information Act*, or the efforts of Canada toward detecting, preventing or suppressing subversive or hostile activities, as defined in subsection 15(2) of the *Access to Information Act*, including, without restricting the generality of the foregoing, any such information listed in paragraphs 15(1)(a) to (i) of the *Access to Information Act*.

1980-81-82-83, c. 111, Sch. II "21".

Law enforcement and investigation

22. (1) The head of a government institution may refuse to disclose any personal information requested under subsection 12(1)

(a) that was obtained or prepared by any government institution, or part of any government institution, that is an investigative body specified in the regulations in the course of lawful investigations pertaining to

(i) the detection, prevention or suppression of crime,

(ii) the enforcement of any law of Canada or a province, or

(iii) activities suspected of constituting threats to the security of Canada within the meaning of the *Canadian Security Intelligence Service Act*,

if the information came into existence less than twenty years prior to the request;

(b) the disclosure of which could reasonably be expected to be injurious to the enforcement of any law of Canada or a province or the conduct of lawful investigations, including, without restricting the generality of the foregoing, any such information

(i) relating to the existence or nature of a particular investigation,

(ii) that would reveal the identity of a confidential source of information, or

(iii) that was obtained or prepared in the course of an investigation; or

(c) the disclosure of which could reasonably be expected to be injurious to the security of penal institutions.

Policing services for provinces or municipalities

(2) The head of a government institution shall refuse to disclose any personal information requested under subsection 12(1) that was obtained or prepared by the Royal Canadian Mounted Police while performing policing services for a province or municipality pursuant to an arrangement made under section 20 of the *Royal Canadian Mounted Police Act*, where the Government of Canada has, on the request of the province or municipality, agreed not to disclose such information.

Definition of "investigation"

(3) For the purposes of paragraph (1)(b), "investigation" means an investigation that

(a) pertains to the administration or enforcement of an Act of Parliament;

(b) is authorized by or pursuant to an Act of Parliament; or

(c) is within a class of investigations specified in the regulations.

1980-81-82-83, c. 111, Sch. II "22"; 1984, c. 21, s. 90, c. 40, s. 79.

Information obtained by Privacy Commissioner

22.1 (1) The Privacy Commissioner shall refuse to disclose any personal information requested under this Act that was obtained or created by the Commissioner or on the Commissioner's behalf in the course of an investigation conducted by, or under the authority of, the Commissioner.

Exception

(2) However, the Commissioner shall not refuse under subsection (1) to disclose any personal information that was created by the Commissioner or on the Commissioner's behalf in the course of an investigation conducted by, or under the authority of, the Commissioner once the investigation and all related proceedings, if any, are finally concluded.

2006, c. 9, s. 183.

Public Sector Integrity Commissioner

22.2 The Public Sector Integrity Commissioner shall refuse to disclose any personal information requested under subsection 12(1) that was obtained or created by him or her or on his or her behalf in the course of an investigation into a disclosure made under the *Public Servants Disclosure Protection Act* or an investigation commenced under section 33 of that Act.

2005, c. 46, s. 58.

Public Servants Disclosure Protection Act

22.3 The head of a government institution shall refuse to disclose personal information requested under subsection 12(1) that was created for the purpose of making a disclosure under the *Public Servants Disclosure Protection Act* or in the course of an investigation into a disclosure under that Act.

2005, c. 46, s. 58.

Security clearances

23. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that was obtained or prepared by an investigative body specified in the regulations for the purpose of determining whether to grant security clearances

(a) required by the Government of Canada or a government institution in respect of individuals employed by or performing services for the Government of Canada or a government institution, individuals employed by or performing services for a person or body performing services for the Government of Canada or a government institution, individuals seeking to be so employed or seeking to perform those services, or

(b) required by the government of a province or a foreign state or an institution thereof,

if disclosure of the information could reasonably be expected to reveal the identity of the individual who furnished the investigative body with the information.

1980-81-82-83, c. 111, Sch. II "23".

Individuals sentenced for an offence

24. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that was collected or obtained by the Correctional Service of Canada or the National Parole Board while the individual who made the request was under sentence for an offence against any Act of Parliament, if the disclosure could reasonably be expected to

(a) lead to a serious disruption of the individual's institutional, parole or statutory release program; or

(b) reveal information about the individual originally obtained on a promise of confidentiality, express or implied.

R.S., 1985, c. P-21, s. 24; 1994, c. 26, s. 56.

Safety of individuals

25. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) the disclosure of which could reasonably be expected to threaten the safety of individuals.

1980-81-82-83, c. 111, Sch. II "25".

Information about another individual

26. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) about an individual other than the individual who made the request, and shall refuse to disclose such information where the disclosure is prohibited under section 8.

1980-81-82-83, c. 111, Sch. II "26".

Solicitor-client privilege

27. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that is subject to solicitor-client privilege.

1980-81-82-83, c. 111, Sch. II "27".

Medical record

28. The head of a government institution may refuse to disclose any personal information requested under subsection 12(1) that relates to the physical or mental health of the individual who requested it where the examination of the information by the individual would be contrary to the best interests of the individual.

1980-81-82-83, c. 111, Sch. II “28”.