

# Directive on Conducting Privacy Impact Assessments

1.1 This directive takes effect on March 6, 2012.

## 2. Application

2.1 This directive applies to all divisions that manage statistical and non-statistical programs that involve the collection, use, or disclosure of personal information.

## 3. Legal Context

3.1 The purpose of the *Privacy Act* is to ensure the protection of the privacy of individuals with respect to personal information about themselves held by a government institution and the provision that individuals have a right of access to that information.

In support of the *Privacy Act*, a Privacy Impact Assessment (PIA) is an evaluation process which allows those involved in the collection, use or disclosure of personal information to assess and evaluate privacy, confidentiality or security risks associated with these activities, and to develop measures intended to mitigate or eliminate identified risks.

The Treasury Board of Canada Secretariat (TBS)'s Directive on Privacy Impact Assessment outlines the required steps for conducting PIAs.

## 4. Definitions

4.1 Definitions to be used to interpret this directive are in Appendix A.

## 5. Directive statement

### 5.1 Objective

5.1.1 Statistics Canada will develop and maintain a generic PIA to assess the privacy risks associated with a standard statistical program.

5.1.2 Statistics Canada will conduct a specific privacy impact assessment for all new and significantly redesigned collections, uses or disclosures of personal information that raise privacy, confidentiality or data security risks if a generic, or already existing, PIA does not adequately address the risks.

### 5.2 Expected results

5.2.1 A generic PIA provides an efficient mechanism to address standard risks associated with statistical programs.

5.2.2 By conducting a privacy impact assessment for all new and significantly redesigned collections, uses or disclosures of personal information that raise privacy, confidentiality or data security risks, Statistics Canada is performing due diligence in the protection of personal information as well as being compliant with the TBS Directive.

5.2.3 In cases where substantially similar collections, uses or disclosures of personal information

occur in statistical programs, the generic Statistics Canada privacy impact assessment will apply so as to ensure compliance with the TBS Directive.

## 6. Requirements

### Director, Information Management Division (IMD)

The Director, Information Management Division (IMD) has been delegated responsibility for ensuring compliance with the Treasury Board Secretariat Directive on Privacy Impact Assessment. The director has responsibility to direct privacy specialists in the division to:

**6.1.1** Provide advice and assistance to program areas on the requirements of the TBS PIA Directive, PIA guidelines and related legislation.

**6.1.2** Provide a copy of PIAs to TBS and the Office of the Privacy Commissioner (OPC) following the approval by the Chief Statistician.

**6.1.3** Post a summary of every approved PIA on the Statistics Canada web site.

**6.1.4** Assist other divisions in reviewing and updating PIAs that have been previously conducted, when and if required.

**6.1.5** Develop and register personal information banks (PIB) with Treasury Board Secretariat and include them in the Statistics Canada chapter of *Info Source* if the PIA is for personal information not linked to a current PIB.

### 6.2 Senior managers (Directors and above)

**In directing managers in a division, the director is responsible for:**

**6.2.1** Reviewing all new and significantly redesigned collections, uses and disclosures of personal information to determine whether the proposed program or system conforms to a generic or already existing PIA;

**6.2.2** Developing, at an early stage in the planning process, a specific privacy impact assessment with support from the privacy specialists in Information Management Division, in cases where a generic PIA does not address all the risks related to privacy, confidentiality and security;

**6.2.3** Inform the privacy officers in the Information Management Division of any new program or activity (or any substantial modification to an existing program or activity) where personal information is being collected or used. This will alert them to the possibility of the requirement for a new or modified PIA or PIB (personal information bank).

**Note: Operational details related to privacy impact assessments are provided in Appendix B.**

### 6.3 Director General, Informatics Branch

The Director General, Informatics Branch is responsible for directing staff to:

**6.3.1.** Assist in the conduct of the IT threat and risk assessment for specific PIAs, if required, and providing advice on mitigation measures related to IT security.

### 6.4 Assistant Chief Statisticians

As advisors to the Chief Statistician, Assistant Chief Statisticians:

**6.4.1** Recommend the approval by the Chief Statistician of specific Privacy Impact Assessments conducted within their fields.

## **6.5 Chief Statistician**

The Chief Statistician:

**6.5.1** Approves the Statistics Canada generic Privacy Impact Assessment, including all modifications to it, and all specific Privacy Impact Assessments conducted in Statistics Canada.

## **6.6 Chief Audit Executive**

As the officer responsible for the internal audit functions in Statistics Canada, the Chief Audit Executive:

**6.6.1** Assures, on a regular and ongoing basis, compliance with this directive through risk-based compliance audits.

## **7. Consequences**

**7.1** Consequences of non-compliance with this directive can include informal follow-up and requests from the Director, Information Management Division, internal audits or formal direction from Statistics Canada senior management on corrective measures.

**7.2** Consequences of non-compliance with the TBS Directive on privacy impact assessment would be reflected in TBS's assessment of Statistics Canada under the Management Accountability Framework program.

## **8. References**

### **8.1 Relevant legislation and regulations for this directive are as follows:**

*Statistics Act*

*Privacy Act*

### **8.2 Related policy instruments and publications are as follows:**

#### **Policy on Government Security (Treasury Board Secretariat)**

Policy on Privacy Protection (Treasury Board Secretariat)

Directive on Privacy Protection (Treasury Board Secretariat)

Directive on Privacy Impact Assessment (Treasury Board Secretariat)

Directive on Privacy Requests and Correction of Personal Information (Treasury Board Secretariat)

Directive on Social Insurance Number (Treasury Board Secretariat)

Directive on Information Management Roles and Responsibilities (Treasury Board Secretariat)

Policy on Confidentiality and Security (Statistics Canada)

Directive on Access to Information and Privacy (Statistics Canada)

Generic Privacy Impact Assessment for Statistics Canada Surveys (Statistics Canada)

## 9. Enquiries

Please direct enquiries about this directive to the Director of Information Management Division.

---

## Appendix A — Definitions

**Privacy Impact Assessment (PIA)** is a comprehensive process for determining the privacy, confidentiality and security risks associated with the collection, use or disclosure of personal information. It also defines the measures used to mitigate and, wherever possible, eliminate the identified risks. The PIA process ensures that measures intended to protect privacy and ensure the confidentiality and security of personal information are considered at the outset of any new program or service delivery initiative. A PIA also communicates to the public how their privacy is protected and how their information is kept confidential and secure from unauthorized access.

**Privacy** is the right to be left alone, to be free from interference, from surveillance and from intrusions. When choosing to “invade” a person’s privacy, governments have obligations with respect to the collection, use, disclosure, and retention of personal information. Privacy generally refers to information about individual persons.

**Confidentiality** refers to a commitment not to release identifiable information about an individual (such as a person, business or organization). It implies a “trust” relationship between the supplier of the information and the organization collecting it; this relationship is built on the assurance that the information will not be disclosed without the individual’s permission or without due legal authority.

**Security** is the arrangements organizations use to prevent confidential information from being obtained or disclosed inappropriately, based on assessed threats and risks. Security measures also protect the integrity, availability and value of the information assets. This includes both physical safeguards, such as restricted access to areas where the information is stored and used, and security clearances for employees, as well as technological safeguards to prevent unauthorized electronic access.

**Personal Information**, as defined by the federal *Privacy Act* (section 3), means information about an identifiable individual that is recorded in any form including age, date of birth, marital status, education, medical information, address, identifying number, symbol or other particular assigned only to that person.

**Personal Information Bank** is a description of personal information that is organized and retrievable by a person’s name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank is under the control of a government institution.

## Appendix B — Procedures for conducting a privacy impact assessment

A privacy impact assessment (PIA) is an evaluation process that allows those responsible for the collection, use and disclosure of personal information to evaluate the privacy, confidentiality and security risks that may be involved and to develop mitigation measures aimed at avoiding or

reducing the identified risks.

The Treasury Board Privacy Impact Assessment (PIA) Directive requires all federal government departments undertaking new or substantially redesigned programs that involve the collection, use or disclosure of personal information to complete a privacy impact assessment of the activity.

Because of the commonalities in procedures among surveys at Statistics Canada, the [Generic Privacy Impact Assessment for Statistics Canada Surveys](#) covers the majority of the Agency's household and business surveys, as well as the receipt and use of administrative information for statistical purposes. This generic PIA describes in detail how the Agency meets the ten privacy principles and includes a threat and risk assessment that focuses on the Agency's major data collection methodologies.

However, in cases where the generic PIA is deemed not applicable to a survey due to special or enhanced privacy risks, a specific privacy impact assessment must be produced. The specific PIA need only address risks not identified in the generic PIA.

According to the TBS PIA Directive, the collection, use and disclosure of personal information in the context of new or redesigned administrative programs and services—for example, human resources and marketing—may require that a privacy impact assessment be conducted.

The following are the procedures that both statistical and non-statistical program managers must follow.

### **Step 1. Determination of the need for a privacy impact assessment**

A program area may contact a privacy specialist in Information Management Division to discuss the program, services or survey. If the Generic Privacy Impact Assessment for Statistics Canada Surveys is deemed to adequately address all known privacy risks, no further action is required. Alternatively an existing specific PIA may address all the known risks.

### **Step 2. When a privacy impact assessment is required**

Using the Treasury Board template for a Core Privacy Impact Assessment, the program manager must complete a first draft of a PIA. This draft will be reviewed by a privacy specialist in Information Management Division. There will likely be various exchanges over the development period of the PIA.

### **Step 3. When a privacy impact assessment is finalized**

Under the Treasury Board directive the head of institution is required to approve the final PIA. Therefore divisions are responsible for creating the memo from their Assistant Chief Statistician to the Chief Statistician requesting approval of the PIA.

Depending on the nature of the program covered by the PIA, the Chief Statistician may grant approval himself or, will decide that review and approval by Policy Committee is required.

### **Step 4. When a privacy impact assessment is approved**

Information Management Division will arrange the following:

- Copies of the approved PIA are sent to Treasury Board and the Office of the Privacy Commissioner.
- A summary of the PIA is prepared and posted on the Statistics Canada web site.

Date Modified: 2012-04-24