
SUMMARY OF RESULTS

Privacy Impact Assessment Report

Performance Measurement Framework: Immigration – Contribution Accountability Measurement System

Citizenship and Immigration Canada

OVERVIEW

Citizenship and Immigration Canada's Contribution Accountability Framework will allow the department to demonstrate responsible stewardship of the funds it supplies to contribution programs for immigrants and refugees and to more effectively evaluate the success of those programs.

The framework comprises five components – performance measurement, evaluation, contribution agreement process, management control framework, and provincial/territorial accountability.

To support the performance measurement and evaluation components of the Framework, Citizenship and Immigration Canada (CIC) has developed the Immigration – Contribution Accountability Measurement System – iCAMS.

iCAMS is an Internet-based data collection system for settlement and resettlement contribution programs. Using iCAMS, CIC will gather information about clients and the services they receive.

Because there could be privacy issues associated with collecting personal client information, CIC carried out a privacy impact assessment for iCAMS.

The privacy impact assessment reflects the state of the iCAMS project as it existed on 19 November 2001. It looks at how clients' personal information is collected, why this information is collected, how it is used and how clients' personal privacy is protected. This document is a summary of the results of the privacy impact assessment.

THE PRIVACY IMPACT ASSESSMENT AND ICAMS

■ What is a privacy impact assessment?

A privacy impact assessment is a process required by federal law to ensure that privacy is considered throughout the development of a project in which a government agency collects personal information.

The assessment includes:

- analyzing what information is collected and how that information is used
- determining privacy concerns associated with collecting and using the information
- recommending ways to avoid or mitigate any potential problems

The result of a privacy impact assessment is documented assurance that privacy issues have been identified and adequately addressed.

■ What is iCAMS?

iCAMS is an Internet-based computer system that CIC has developed to collect information on the settlement and resettlement contribution programs it funds. These programs include the Resettlement Assistance Program (RAP), the Language Instruction for Newcomers to Canada (LINC) program, the Immigrant Settlement and Adaptation Program (ISAP) and the Host program (Host).

■ Why was a privacy impact assessment required for iCAMS?

While the information gathered using iCAMS is protected by several laws (including the *Privacy Act* – a law that obliges government departments and agencies to respect the privacy rights of Canadians), a privacy impact assessment ensures that privacy has been considered at all stages of the project's development.

The privacy impact assessment determines whether introducing and using iCAMS will pose any privacy risks. If any privacy risks are discovered, the assessment provides recommendations on ways to avoid or mitigate those problems.

■ **How was the privacy impact assessment carried out?**

In late 2001, an independent privacy consultant reviewed project documentation and met with program, project, privacy and other departmental staff to identify and analyze privacy implications associated with introducing and using iCAMS.

Input from Canada's Privacy Commissioner was also considered. The Privacy Commissioner, an advocate for the privacy rights of Canadians, provides guidance and advice on how best to protect personal information. Further information on the office of the Privacy Commissioner can be obtained at www.privcom.gc.ca.

INFORMATION COLLECTION, USE AND PROTECTION

■ How will information be collected using iCAMS?

CIC funds service provider organizations, to deliver settlement contribution programs to newcomers. The organizations will collect client information and enter it into secure iCAMS computers. The data will then pass directly, in a secure manner, to CIC's national headquarters through the Internet.

■ What personal information will be collected using iCAMS?

Some personal information collected in iCAMS will be provided by the client to the service provider organization while some will already have been provided by the client to CIC. The following lists the personal information collected:

- an immigration identifier number, e.g., IMM1000 (record of landing)
- name
- address
- date of birth
- gender
- country of birth, citizenship and country of last permanent residence
- educational and language background
- marital and family status
- date of arrival and landing

■ What other information will be collected using iCAMS?

iCAMS will also collect information on the services and programs that service provider organizations deliver to clients. Service provider organizations will enter service data into iCAMS on an individual client basis for LINC and RAP, and on an aggregate basis for ISAP and Host.

■ How is this information protected?

The following laws and policies were reviewed as part of the privacy impact assessment to determine how client information is being protected in iCAMS:

- Privacy Act and Regulations

The Privacy Act obliges government departments and agencies to respect the privacy rights of Canadians by placing limits on collecting, using and disclosing personal information

- Access to Information Act and Regulations

The Access to Information Act gives individuals the right to have access to information in federal government records (as long as it is not exempted or excluded in the legislation)

- Personal Information Protection and the Electronic Documents Act

This Act sets out ground rules for how private-sector organizations may collect, use and disclose personal information

- Several Treasury Board of Canada policies

These policies cover how information is to be used, displayed, managed and protected in the federal government

Beyond these laws and policies, personal information will also be protected and kept confidential through a variety of CIC procedures:

- Personal information collected in iCAMS will not be used to make administrative decisions about individual clients.
- Reports generated for evaluation purposes will show only aggregate data – data that does not identify individuals.
- The service provider organizations that collect information using iCAMS will only be able to view the information they enter for their own clients and their organizations. They will not be able to access information entered by any other service provider organizations (except in the case of LINC training centres that will view assessment centre information).
- Access to information will also be limited within service provider organizations. Access will be controlled by passwords and user accounts issued by CIC in consultation with service provider organizations. Reliability checks will be required for employees before user accounts and passwords are issued.

FINDINGS AND RECOMMENDATIONS

The privacy impact assessment identified a number of specific privacy issues and recommended measures to deal with them.

■ Service provider privacy responsibilities

Through their agreements with CIC, service provider organizations are required to treat personal client information as subject to the provisions of the *Privacy Act*. There is, however, no documentation available to determine their responsibilities for implementing the provisions of the *Privacy Act*.

Recommend: Develop documentation that identifies the responsibilities service provider organizations have for treating information in accordance with the provisions of the *Privacy Act*, as stated in the contribution agreement.

■ Data custodian responsibilities

The responsibilities of the data custodian – the individual with overall program responsibility for iCAMS – are not documented.

Recommend: Develop documentation that specifies the data custodian's responsibilities and performance measures.

■ Notice of purpose of collection

Under the *Privacy Act*, when a government agency collects personal information, it must tell the individual why the information is being collected and how it will be used.

Recommend: Develop documentation that details the content and delivery method for the Notice of the Purpose of Collection that is required by the *Privacy Act*.

■ CIC access to personal information

CIC will use the information gathered by iCAMS to help demonstrate responsible stewardship of the funds it supplies for contribution programs and to evaluate the success of those programs.

As part of this process, some CIC staff will need access to the information gathered using iCAMS.

For most their work in evaluating programs, CIC staff can work with reports that use aggregate data – data that has been combined and does not identify individuals.

If there is a need for access to individual records to help with program evaluation and measurement, personal identifiers can be masked to create an anonymous record.

Recommend: CIC should document any program measurement and evaluation requirements that create a need for access privileges to personal information in iCAMS where the requirements cannot be accomplished through access to combined or anonymous data.

■ **Client satisfaction survey**

CIC plans to conduct client surveys. Some of these surveys will be conducted anonymously. Others, however, may be conducted using specific clients. If this sort of survey is done, CIC will need to obtain personal information from iCAMS, such as a client's name, address and the service he or she has received.

Recommend: If CIC decides to conduct a survey using specific clients, it should make sure the client's consent to participate is clear and that there are standards to make sure the individual can give consent.

■ **Schedules for records retention and disposal**

Government policy requires that all information that is held be subject to a schedule or timetable for how long it will be retained and how it will be disposed.

Recommend: Develop schedules that detail how long personal information collected using iCAMS will be retained and how it will be disposed.

■ **Service provider security guidelines**

The iCAMS draft user manual describes security guidelines for iCAMS. These guidelines are presented as “best practices” for service providers, but there is no assurance that service provider employees will review this material.

Recommend: Service provider employees should sign an acknowledgement of iCAMS security requirements (not guidelines) as part of the process of obtaining user accounts and passwords.

■ **Data matching**

Matching, comparing or linking data from separate databases to help make decisions about individuals is a privacy concern.

Data matching will not occur in iCAMS. CIC will not use any of the personal information gathered using iCAMS to make decisions about individuals.

Recommend: When personal information is used to evaluate programs, personal identifiers will be masked to protect the identity of individuals.

OTHER RECOMMENDATIONS

■ Canada's Privacy Commissioner

Canada's Privacy Commissioner is an advocate for the privacy rights of Canadians. The Privacy Commissioner provides guidance and advice on how best to protect personal information.

In a letter to CIC, the Privacy Commissioner raised the issue of collecting personal information using iCAMS.

The Privacy Commissioner made a number of recommendations, including:

- Service providers should tell clients why their personal information is being collected and how it will be used.
- Clients must consent when the information requested exceeds what is technically required to deliver the service.
- Access to personal information should be restricted.
- When the information gathered is used to evaluate programs, personal identifiers for personal information should be masked.
- Personal information compiled to help evaluate programs should only be kept in an identifiable format for the time required to perform the analysis and be disposed of according to a pre-determined schedule.

RESPONSE TO RECOMMENDATIONS

■ CIC's Response

CIC is responding to the privacy impact assessment and Privacy Commissioner's recommendations as follows:

- Security (technical, user and physical security) requirements for iCAMS are being developed to protect personal information, which will support the privacy clause in the contribution agreement.
- Data custodian responsibilities are being documented as part of the system development process.
- A pamphlet is being provided to service provider organizations for distribution to settlement clients, outlining the purpose for which their personal information is being collected and how it will be used.
- Aggregate reports that do not identify individuals will primarily be used to evaluate settlement programs and requirements for access to reports with personal identifiers will be limited and documented.
- Any client satisfaction survey implemented as part of program evaluation and performance measurement will be completed on a voluntary basis.
- An appropriate retention and disposal schedule for iCAMS data is being developed.
- Training material is being developed to ensure that service provider organization employees are aware of the privacy and security requirements of accessing iCAMS. In addition, applicants applying for passwords will be required to sign a form indicating that they are aware of these requirements.
- The information being requested relates directly to the delivery of services.
- Access to iCAMS is restricted, as users are assessed for reliability and their need to use the system, prior to being provided with a password.

FOR MORE INFORMATION

If you would like to obtain a copy of the complete iCAMS privacy impact assessment, please make a request in writing under the *Access to Information Act* to:

Diane Burrows
Public Rights Administration
Citizenship and Immigration Canada
360 Laurier Avenue West, 10th Floor
Ottawa, Ontario
K1A 1L1