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

Summary of Privacy Impact Assessment Report and Follow-up Actions

Published: 2006-00-19

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT53-28/2006E-PDF
ISBN: 978-0-660-25386-2

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Sommaire du Rapport d'évaluation des facteurs relatifs à la vie privée (ÉFVP) et des mesures de suivi

1. Purpose

This document is to facilitate the review of the Privacy Impact Assessment (PIA) Update by: providing context; highlighting key points that show how privacy considerations have been factored into the design, development and implementation of the Corporate Business Intelligence Software (CBIS) and reviewing the status of follow up on the three privacy risk areas and recommendations that were made.

2. Description - Corporate Business Intelligence Software

CBIS provides a single window to corporate management information to authorized users within the departments through a web interface. The purpose is to provide a consolidated means of reporting, analyzing and displaying data to improve internal planning and decision-making. CBIS supports a big picture view by providing demographic information at various organizational levels. It also provides data at the level of individuals and transactions.

Currently, the software has the capacity to permit users to access information and create dynamic reports using data that has been extracted from the Human Resources (HRMS), the Financial (SAP) and the Salary Forecasting System (SFS) databases. These databases contain information that has been previously collected from individuals with authority under the Privacy Act. CBIS does not collect information. It delivers information and reports on-line using previously collected data. It is intended to replace a number of stand-alone reporting mechanisms currently in use.

3. Why the PIA was Necessary

Deployment of CBIS will signify changes to business processes and systems that will re-design information delivery within the departments.

4. PIA Objectives

- To assess whether privacy considerations have been adequately factored into the development and delivery of this new internal service delivery initiative.
- To resolve any privacy issues that may be of potential public concern (i.e. employees and individuals performing services for the departments).

5. PIA Findings

Three privacy risks, considered low to moderate in severity, were identified. Recommendations and initiatives that are either planned or underway to address these risks are highlighted in the relevant sections of this summary document.

6. Current BI Tool Reporting Capacity

Four types of reports have been developed - Organization Profile, Leave Profile, Salary Forecasts and Financial Reporting. The following charts summarize data extracted from HRMS, SAP and SFS that is used to prepare these reports. This data will also be used to generate other information and reports to support human resources and financial reporting and decision-making.

Chart 1: Organization Profile, Leave Balance, and Leave Usage Data Summary (Note: Not yet deployed)

Field Name	Field Name	Field Name
Branch	Pension service start date	Years of departmental service
Name	Department start date	Years of position service
Sex	Position start date	Average years of public service
Official language	Leave type	Average years in department
Classification	Leave carry over	Average years in position
Full/part time	Leave entitlements	Retirement eligibility without penalty (0-2 years, 2-5 years, >5 years),
Employment tenure (casual, indeterminate, regular, student, term)	Leave used/paid	Average age (when there are more than 5 employees in an occupational group)
Employee status (active, assignment out, deceased, terminated, leave of absence)	Current leave balance	Age range (up to 29 years, 30-39 years, 40-49 years, 50-54 years, 55 years and over),
Employment type (departmental employee, agency, contractor/consultant, maintenance, messenger, MP staff, other federal department, other government, parliamentary secretary, work experience),	Years of public service	Employee counts
Age		

CHART 2: Salary Forecasting Data Summary

(Note: Deployed September 2004.)

Field Name	Field Name	Field Name
Fiscal year	Pay action/reason	Total forecast
Organization	Start/end date	Year-to-date actual amount

Fund centre	Next increment date	To year-end planned amount
Annual salary budget amount	Annual salary rate	To year-end planned FTE usage
Annual FTE (full-time equivalent) budget	Annual terminable allowance rate	Monthly forecast FTE usage
Reporting object	Annual bilingual bonus rate	Monthly forecast amount
Employee name	Year-to-date FTE usage forecast	Monthly actual amount
Position number	To year-end FTE usage forecast	Monthly planned amount
Classification	Total FTE usage forecast	Monthly planned FTE usage
Employee status (active, leave of absence, etc.)	Year-to-date forecast amount	Head count
Employee tenure (continuing/term)	To year-end forecast amount	

CHART 3: Financial Reporting Data Summary

(Deployed beginning April 2006.)

Field Name	Field Name
Fiscal year	Annual budget amount
Organization	Outstanding commitment amount
Fund centre	Actual expenditure amount
Fiscal period	Vendor name
Reporting object (personnel costs, goods and services)	Description of expenditure/commitment
Fund	Budget free balance

The PIA examined how the software traces, identifies and transforms the above data to produce information and reports. The report concluded that the analysis of this data could possibly generate new facts about employees.

Two recommendations were made:

- *To the extent that it is retained, schedule "new" Personal Information, generated by reason of any analysis conducted, for disposition.*
- *Amend language of PIB PSE 901 to indicate that PIB PSE 901 also holds "derivative" Personal Information*

Follow up:

These recommendations were addressed during the Office of the Privacy Commissioner of Canada's (OPCC) informal review.

- Snapshot reports used to make administrative decisions about employees will be retained on personal files and in accordance with departmental retention schedules.
- PIB PSE 901 will be updated incorporating feedback from the OPPC and in consultation with ATIP Coordinators for the departments. This will be done during the 2005 annual InfoSource review and update. Also, any other data banks that require updating as a result of the addition of Salary Forecasting System data to the Corporate Business Intelligence Software will be done during the 2005 annual InfoSource update.

7. Personal Identifiers

PRI or Departmental ID Numbers: The software users personal identifiers to trace and capture previously collected data. They are neither visible nor accessible to end users through the BI Tool. For example:

Retirement Eligibility - The number of years before an employee can retire without penalty is provided using ranges so that employee age cannot be identified.

Age: Information is provided using ranges and averages so that employee age cannot be identified. Age ranges show the age group of an employee. Average age is provided for organization profile reports when there are more than five employees in an occupational group or work unit.

8. Use of Personal Information

The PIA looked at whether information generated by the tool would be used in a manner consistent with the Privacy Act. Information will be used internally for administration and management of personnel. These uses are consistent with the purpose for which employee information was originally collected.

9. Accuracy of Personal Information

Since the BI tool extracts data that has been previously collected and entered into HRMS, SAP and SFS, corrections must be made at the level of the source databases. These databases already have established procedures to input and log corrections as well as monitor data for quality assurance.

Two recommendations were made:

- *Ensure accuracy errors are corrected as soon as discovered and minimize such errors.*
- *Establish procedures to document and log corrections as necessary.*

Error identification has been identified as a quality assurance requirement to be addressed as part of the deployment of the software. The development of a record with respect to requests has been identified as an outstanding work item. It is anticipated that a process will be developed as an application support unit to log and document corrections as necessary.

10. Access to Information through the BI Tool

An automated access control system,the *Access Manager,* controls who receives access and the ability to "drill down" to less aggregated data at different organizational levels and "drill through" to the lowest level of detail on individuals.

The Corporate Services Branch (CSB), in keeping with its overall responsibility to manage and protect employee privacy, documented the rules governing access to employee information. These rules underpin the CBIS access control system and mirror current business rules and practices that are based on role, function and need to know in accordance with the provisions of the Privacy Act. Within these parameters, five business rules determine who receives access from the Access Manager – Lead of an Organization, Branch Coordinators/Executive Assistants, Non-managing Executives/ Special Project Advisors, Officers and Administrative Staff.

A premise underlying the development and testing of the access rules was that users would not get access to employee information that they would not otherwise have or to less information than they would receive upon request.

Managers of all corporate management systems control access within CSB to the various corporate systems modules containing employee information. CSB staff is granted access only to those modules containing information needed to carry out specific job functions.

11. Changes to Work Processes and Information Delivery – Maintaining Employee Privacy

CBIS will provide a self-service environment for direct access to salary and financial information, employee information and demographic data. CSB will continue to manage and safeguard employee information and make corrections to source data as needed by:

- Providing guidance and support in the development of procedures to validate and correct information and reports that the BI Tool produces.
- Periodic monitoring of information and reports produced to ensure compliance with the principles of the Privacy Act.
- Resolving problems as they arise.
- Consulting with internal Access to Information and Privacy Officers for advice and guidance as needed.

The privacy impact assessment will be maintained throughout the CBIS lifecycle

12. Training, Communications and Information for CBIS Users

Since information will be directly accessible to users through the BI Tool, they will need guidance on their responsibilities to use and protect employee information under the Privacy Act. This will be accomplished through:

- Including information about the Privacy Act in the on-line reference section of the BI Tool and in training materials.
- Requiring individuals to whom the tool is deployed to accept their responsibilities in accordance with the Privacy Act.

- Advising end users of the consequences of non-compliance.

A communications strategy and plan will be developed. Also, the summary of the PIA (this document) is accessible in the on-line reference section of the BI Tool.

13. Security Management

System security was considered satisfactory based on the Threat and Risk Assessment that was previously conducted. All users have the necessary clearance to access Protected B information. IT Security Staff and project team representatives also provided additional information to the OPPC during the informal review process.

Three recommendations were made:

- *Ensure that contingency plans and procedures are in place to respond to security breaches or disclosures of Personal Information in error.*

  The need to document procedures for managing ongoing security and for responding to security breaches or disclosures of information is recognized.

  Individual breaches will be investigated and addressed case-by-case depending on the nature and sensitivity of the information disclosed. Managers will be responsible to handle these situations within their delegated authority in consultation with the Staff Relations Section, HRD, and the Security Services Division (CSB).

- *Identify process to advise the data subjects (i.e. employees where such violations occur).*

  HRD will follow up with the ATIP Coordinator for guidance.

- *Consult with the departmental security officials to establish a "lifecycle" approach to the Tool's security*.

  SSD provided input to the PIA and will follow up accordingly.