PIA Summary for Public Posting

Enterprise Migration to Software as a Service (SaaS) PIA

July 2013

1. About Destination Canada

The Canadian Tourism Commission, operating as Destination Canada (DC), is a Crown Corporation wholly owned by the Government of Canada. Established in 2000, DC was created to lead the Canadian tourism industry in marketing Canada as a four-season tourism destination. DC's legislated mandate is to: sustain a vibrant and profitable Canadian tourism industry; to market Canada as a desirable tourist destination; to support a cooperative relationship between the private sector and the governments of Canada, the provinces, and the territories with respect to Canadian tourism; and to provide information about Canadian tourism to the private sector and to the governments of Canada, the provinces, and the territories. It fulfills its mandate by working with various levels of government to conduct research and to administer marketing initiatives that increase international visits and tourism revenue. DC also works alongside several international partners to help promote Canadian tourism.

2. About the Project

For more than a decade, DC has relied on a patchwork of applications to support its financial, procurement, client relationship, human resources and performance management needs. Notwithstanding itsDespite efforts to prolong the useful life of these applications through product customizations, in time, several systems reached the end of their life-cycle and were no longer supported by their original vendors. In many cases, the applications were failing to meet the operational needs of DC, particularly in regards to core functionality, user-friendliness, data integrity and security, and systems inter-connectivity.

Following an independent assessment of its systems, and an evaluation of enterprise options available in the marketplace, DC decided to adopt a "Software as a Service" (SaaS) model for the renewal of its information management infrastructure. SaaS is a software delivery model in which software and associated data are centrally hosted on an external vendor's servers, an approach to systems management more commonly referred to as "cloud computing".

3. Scope of the Privacy Impact Assessment

Although DC is not itself named in the Schedule to the *Privacy Act*[1], it reports to Parliament through the Minister of Innovation, Science and Economic Development of Canada (previously the Minister of Industry). As such, and in keeping with its designation as a Crown Corporation, DC abides by the Act and its supporting policies and directives, as established by the Treasury Board SecretariatTBS.

Under the TBS *Policy on Privacy Protection*, all federal institutions subject to the *Privacy Act* are required to undertake an assessment of the privacy impacts associated with the development or design of new programs or services involving personal information (or when making significant changes to an existing program or service). This PIA report provides evidence of compliance with those requirements.

In recognition of the potential security and privacy challenges surrounding cloud computing, a privacy impact assessment was conducted so as to inform the program's policy and technical implementation. The PIA also served to proactively manage and mitigate potential risks to personal information under the Commission's control. The PIA was initiated in the early phases of project planning. Critical recommendations emanating from the PIA process were evaluated and addressed by management over the course of the project's development and implementation.

The SaaS PIA covers only those activities relating to the migration of systems and data to the cloud under the SAP Business ByDesign initiative (the "SaaS initiative"). Additional system or service-specific PIAs will be conducted, where appropriate, in support of DC's on-going application modernization efforts. A separate PIA concerning payroll and benefit services was completed in conjunction with the introduction of those services.

4. Privacy Analysis

Based on the findings of the PIA, and consistent with our preliminary evaluation of privacy risks, the SaaS initiative is considered to be of low privacy risk: personal information being transferred to the cloud is limited and non-sensitive in nature; the initiative does not involve the collection of any new personal information; uses of personal information already under DC's control are consistent with those for which the information was collected (and for which consent was obtained); and information safeguards are commensurate withreflect the sensitivity of the information affected.

[1] *Privacy Act* (R.S.C., 1985, c. P-21).

DESTINATION CANADA

5. Risk Area Identification and Categorization

A: Type of Program or Activity	Level of Risk to Privacy
Program or activity that does NOT involve a decision about an identifiable individual. Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual.	☑ 1
Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc…).	☐ 2
Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e., a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).	☐ 3
Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).	☐ 4
B: Type of Personal Information Involved and Context	**Level of risk to privacy**
Only personal information provided by the individual – at the time of collection –- relating to an authorized program & collected directly from the individual or with the consent of the individual for this disclosure / with no contextual sensitivities. The context in which the personal information is collected is not particularly sensitive. For example: general licensing, or renewal of travel documents or identity documents.	☐ 1
Personal information provided by the individual with consent to also use personal information held by another source / with no contextual sensitivities after the time of collection.	☑ 2
Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual.	☐ 3

Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.	☐ 4
C: Program or Activity Partners and Private Sector Involvement	**Level of risk to privacy**
Within the department (amongst one or more programs within the department)	☑ 1
With other federal institutions	☐ 2
With other or a combination of federal/ provincial and/or municipal government(s)	☐ 3
Private sector organizations or international organizations or foreign governments	☑ 4
D: Duration of the Program or Activity	**Level of risk to privacy**
One time program or activity: Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.	☐ 1
Short–term program: A program or an activity that supports a short-term goal with an established “sunset” date.	☐ 2
Long-term program: Existing program that has been modified or is established with no clear “sunset”.	☑ 3
E: Program Population	**Level of risk to privacy**
The program affects certain employees for internal administrative purposes.	☐ 1
The program affects all employees for internal administrative purposes.	☑ 2
The program affects certain individuals for external administrative purposes.	☑ 3
The program affects all individuals for external administrative purposes.	☐ 4
F: Technology and Privacy	**Level of risk to privacy**

Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?	No
Does the new or modified program or activity require substantial modifications to IT legacy systems and / or services?	No
The new or modified program or activity involves the implementation of potentially privacy invasive technologies?	No
G: Personal Information Transmission	**Level of risk to privacy**
The personal information is used within a closed system. No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.	☐ 1
The personal information is used in system that has connections to at least one other system.	☑ 2
The personal information may be printed or transferred to a portable device.	☐ 3
The personal information is transmitted using wireless technologies.	☐ 4
I: Risk Impact to the Individual or Employee	**Level of risk to privacy**
Inconvenience.	☑ 1
Reputation harm, embarrassment.	☑ 2
Financial harm.	☑ 3
Physical harm.	☐ 4
H: Risk Impact to the Department	**Level of risk to privacy**
Managerial harm. Processes must be reviewed, tools must be changed, change in provider / partner.	☑ 1

Organizational harm. Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	☑ 2
Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	☑ 3
Reputation harm, embarrassment, loss of credibility. Decrease confidence by the public, elected officials under the spotlight, departmental strategic outcome compromised, government priority compromised, and impact on the Government of Canada Outcome areas.	☑ 4