PIA Summary for Public Posting

Applicant Tracking System (ATS) PIA

December 2016

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

DC's ability to fulfill its mandate in an effective and efficient manner depends, in part, on its ability to attract and maintain a highly motivated, knowledgeable and innovative workforce. Despite its significant mandate and international presence, DC employs only 93 permanent full-time employees and 23 term employees.[1] Although the corporation has added several new staff members over the past few years (and attracted many new members to its management team), its ongoing success depends on its ability to augment the skills of its permanent workforce. It also depends on having effective systems in place to support key human resource functions – systems that enable DC to undertake human resource planning, training and development, compensation, and performance management activities in line with the corporation's long-term strategic direction.

In keeping with its strategic interest in investing in corporate initiatives that provide employees with the necessary tools to maximize their performance, DC has elected to implement and operate an implemented an ATS for corporate recruiting. In time, the ATS is expected to automate portions of its the recruitment process, and to help in the application of more modern leverage data-intelligence techniques to modernize its hiring campaigns. By investing in an ATS, DC expects to be able to improve the efficiency

[1] A 2016 internal audit of corporate efficiency by Ernst & Young LLP found that DC's corporate functions were very efficiently resourced, and that its corporate expenditures per capital were markedly lower in comparison to other Canadian federal Crown corporations.

of its recruiting efforts, and to better reach hard-to-find talent. The ATS is also expected to assist in building better talent pools, and in hiring the right people in the right positions so that new recruits become long-term and productive employees of the organization.

The use of an ATS for recruitment purposes is not uncommon in industrythe private sector. More than 86% of Fortune 500 companies employ applicant tracking or management systems for staffing.[2] Its principal function will be to automate DC's recruitment process using a defined workflowthe process, and to provide a centralized database of information relating tofor DC's recruitment efforts. Once implemented, the ATS is expected to assist DC's Human Resources Group (HR) in the processing and analysis of resumes and applicant information, and to help manage the corporation's broader recruitment efforts.

For the most part, data will be collected directly from applicants via the ATS (as located on the corporation's website); in some cases, data may also be sourced or parsed from job and resume boards such as LinkedIn.com (with the individual's consent). In all cases, personal information to be collected through the ATS will be limited to that which is needed for recruitment and hiring purposes. Information will not be used for secondary purposes, nor to make decisions about individuals outside of hiring activities.

3. Scope of the Privacy Impact Assessment

Although DC is not itself named in the Schedule to the *Privacy Act*[3], 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 TBS.

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.

The ATS PIA was completed under the direction of the DC's Executive Director for Human Resources. Consultations with DC's Information Technology and Facilities Management group, along with its Access to Information and Privacy unit and Legal Services group were undertaken as needed.

[2] See Talemetry, ATS Market Share for Fortune 500, February 2017.

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

4. Privacy Analysis

Based on the results of the PIA, inherent risks arising from the implementation of DC's ATS are considered to be moderate to low. Recommendations from the ATS PIA, as adopted, are expected to reduce those risks to a negligible level.

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?	Yes
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