External Reference Checking Process
Using Garda Background Screening Solutions

Privacy Impact Assessment (PIA) Summary

Canadian Nuclear Safety Commission

Government Official Responsible for the Privacy Impact Assessment

Louise Youdale
Director General
Human Resources Directorate

Daniel Schnob
Director General
Finance and Administration Directorate

Head of the government institution / Delegate for section 10 of the *Privacy Act*

Nicholle Holbrook
A/Senior ATIP Advisor

Description of Program or Activity:

The Canadian Nuclear Safety Commission has outsourced a portion of the staffing process, related to the verification of education, credentials, work history and the personal references provided by the applicant. The initial contract winner was First Advantage however, in 2016, the CNSC was required to re-compete the contract and the service provider has changed. In response, the CNSC has chosen to complete a Privacy Impact Assessment to document and assess the collection and disclosure of applicants' personal information.

It is anticipated that the new vendor, Garda Background Screening Solutions, will be in place in early 2017.

For the staffing process, the CNSC collects a variety of personal information however, this assessment will focus on the personal information collected, used and disclosed for the reference checking process. This includes the individual's name, contact information, date of birth, work history, education and credentials, personal opinions / views about the individual and their signature. In addition, this process requires the collection of information about the individuals who will serve as references for the candidate, including the name, contact information and relationship to the candidate. This information will be disclosed to Garda for validation / verification.

In addition, it is anticipated that CNSC's corporate security office will use the services to facilitate the individual security clearance assessment in some circumstances.

Description of the class of records associated with the program or activity

This activity is referenced in standard Classes of Records – Recruitment and Staffing (PRN 920); and Security (PRN 931)

Description of the personal information banks associated with the program or activity

This activity is referenced in standard Classes of Records – Recruitment and Staffing (PRN 920); and Security (PRN 931)

Legal Authority for Program or Activity

As a separate agency, the CNSC is not subject to the *Public Service Employment Act* and has the authority to establish its staffing policy framework and recruitment strategies pursuant to Section 16.(1) of the *Nuclear Safety and Control Act* (NSCA). The President may delegate the power to appoint employees to managers of the CNSC pursuant to Section 12.(3) of the NSCA.

Additional authority can be derived from Order in Council P.C. 2000-1135, an Order (a) authorizing the President of the Canadian Nuclear Safety Commission to exercise and perform the powers and functions of the Treasury Board in the field of personnel management with respect to employees of the Commission, and (b) repealing Order in Council P.C. 1968-26/230 of February 8, 1968.

For completing security clearances on contractors, where required, CNSC's security division relies on the legal authority imparted to the CNSC under section 8(1) and (2) of the *Nuclear Safety and Control Act* as well as the Policy on Government Security.

Risk Area Identification & Categorization

1) **Type of Program or Activity**
   The personal information collected in support of the reference checking process is used to make an administrative decision that directly affects the individual.
   Level of risk to privacy – 2

2) **Type of Personal Information Involved and Context**
   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.
   Level of risk to privacy – 2

3) **Program or Activity Partners and Private Sector Involvement**
   This program involves the outsourcing of services to the private sector.
   Level of risk to privacy – 4

4) **Duration of the Program or Activity**
   This is a long term initiative, without an established sunset date.
   Level of risk to privacy – 4

5) Program Population

The program affects certain individuals for external administrative purposes.
Level of risk to privacy – 3

6) Technology & Privacy

a) 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?
Risk to privacy – Yes

b) Does the new or modified program or activity require any modifications to IT legacy systems and / or services?
Risk to privacy – No

c) Enhanced identification methods - This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc…) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic).
Risk to privacy – No

d) Use of Surveillance - This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.
Risk to privacy – No

e) Use of automated personal information analysis, personal information matching and knowledge discovery techniques - For the purposes of the Directive on PIA, government institution are to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behavior.
Risk to privacy – No

7) Personal Information Transmission

The personal information is used in system that has connections to at least one other system.
The personal information is transferred to a portable device or is printed.
Level of risk to privacy – 3

8) **Risk Impact to the Institution**
In the event of a breach of the personal information related to the external reference check process, the CNSC would likely need to change procedures; in addition, there would be a decrease in public confidence in how personal information is safeguarded.
Level of risk to privacy – 4

9) **Risk Impact to the Individual or Employee**
In the event of a breach of the personal information, there is the potential for reputation harm / embarrassment for the individual.
Level of risk to privacy – 2