The CNSC's Financial Guarantees Program

Privacy Impact Assessment summary

Canadian Nuclear Safety Commission

Government Official Responsible for Privacy Impact Assessment

Colin Moses
Director General
Directorate of Nuclear Substance Regulation

Daniel Schnob
Director General
Finance and Administration Directorate

Head of the Government Institution / Delegate for section 10 of the *Privacy Act*

Nicholle Holbrook
Senior ATIP Advisor

Description of program or activity

The Canadian Nuclear Safety Commission (CNSC) regulates the use of nuclear energy and materials to protect health, safety, security and the environment; to implement Canada's international commitments on the peaceful use of nuclear energy; and to disseminate objective scientific, technical and regulatory information to the public. CNSC licensees are responsible for ensuring that their nuclear facilities and activities are designed, constructed, operated, decommissioned and abandoned in a manner that protects health, safety, security and the environment, while respecting Canada's international obligations. This responsibility includes making appropriate arrangements, as part of corporate business planning, for the termination of licensed activities, including the cessation of operations, short- and long-term management of radioactive waste and the disposition of all nuclear substances and prescribed equipment.

The CNSC requires financial guarantees to ensure that, in the event of bankruptcy, licensees have funds available to terminate licensed activities.

Section 24(5) of the Nuclear Safety and Control Act (NSCA) provides the legal authority for the financial guarantee requirement. This privacy impact assessment reflects the use of personal identity and contact information to impose a financial guarantee on Directorate of Nuclear Substance Regulation licensees (approximately 1,400 licensees that are generally smaller and more independent than Class I facility operators). A very small percentage of these licensees are individuals, not corporations.

The personal information collected is limited to name, contact information and licence details. The payment portion of program delivery has been outsourced to a third-party insurance brokerage, Aon Reed Stenhouse. The broker will manage licensee payments, refunds, issuance of receipts, premium payments to the insurer and CNSC insurance claims. The CNSC does not receive any financial information from the broker.

The CNSC receives a report of licensees who do not pay on time from the broker, and will follow up with these licensees to ensure compliance with licence condition 2020. As a last resort, non-compliant licensees will be subject to CNSC enforcement action. Licensee compliance reports will be monitored to check licensee inventory, to establish financial guarantee requirements.

Licensees can use an online portal, hosted by Trisura, to make payments. Payments can also be made over the phone or by mail.

Description of the Class of Record and Personal Information Bank associated with the program or activity

This collection of personal information is related to multiple Classes of Records for the CNSC:

Medical sector	Record number 1.3.1
Industrial sector	Record number 1.3.2
Commercial sector	Record number 1.3.3
Academic and research sector	Record number 1.3.4

Personal information collected in support of the CNSC's financial guarantees initiative will not be used to make an administrative decision that directly affects the individual, and will not be retrievable by knowing the individual's identity. As such, this collection of personal information is represented in a Class of Personal Information, not a Personal Information Bank.

Licensee contact information

For the process of licensing facilities and activities, licensee organizations are required to provide personal information about designated, identifiable individuals authorized to act on their behalf in dealings with the Commission. Personal information is generally limited to name and contact information.

Legal authority for program or activity

Legal authority for the requirement of financial guarantees, and the collection of associated personal information is derived from section 24(5) of the Nuclear Safety and Control Act, which states:

> "Terms and conditions of licences
>
> (5) A licence may contain any term or condition that the Commission considers necessary for the purposes of this Act, including a condition that the applicant provide a financial guarantee in a form that is acceptable to the Commission."

Type of personal information involved and context

1. **Type of program or activity**
   The personal information collected in support of the financial guarantees initiative is not used to make a decision that directly affects the individual.
   Level of risk to privacy – 1

2. **Type of personal information involved and context**
   Personal information is limited to name and contact information, collected directly from the individual, with no contextual sensitivities.
   Level of risk to privacy – 1

3. **Program partners and private sector involvement**
   The financial guarantees initiative is delivered with the assistance of private-sector partners. The only personal information disclosed to the private sector is the licensee name, licensee number (used as the login ID for the portal), and an eight-digit password used to log in to the portal.
   Level of risk to privacy – 4

4. **Duration of the program or activity**
   The financial guarantees initiative is intended to be a long-term initiative, without an established sunset date.
   Level of risk to privacy – 4

5. Program population

The financial guarantees initiative affects individuals who act as contacts for licensees, under the *Nuclear Safety and Control Act*.
Level of risk to privacy – 3

6. Technology and 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 – No

b. Is the new or modified program or activity a modification of an IT legacy system and/or service?
Risk to privacy – No

c. Enhanced identification methods: This includes biometric technology (e.g., facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID)) as well as easy pass technology, new identification cards including magnetic stripe cards, smart cards (i.e., identification cards 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, or satellite surveillance.
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 Privacy Impact Assessment*, government institutions 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 behaviour.
Risk to privacy – No

7. Personal information transmission

Licensee information is held within LOUIS, an internal CNSC database. Information is provided to program partners via secure transmission methods.
Level of risk to privacy – 3

8. Risk impact in the event of a breach

In the event of a breach of personal information associated with the financial guarantees initiative, 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