The CNSC's Participant Funding Program

Privacy Impact Assessment summary

Canadian Nuclear Safety Commission

Government Official Responsible for Privacy Impact Assessment

Liane Sauer
Director General
Strategic Planning 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 Participant Funding Program (PFP) was enabled through changes to the *Nuclear Safety and Control Act* in 2010 under the *Jobs and Economic Growth Act*, and has been in operation at the CNSC since 2011, with the first contributions paid to participants that same year.

The program objective for the PFP is to provide funding to eligible applications in order to:

- enhance Aboriginal, public and stakeholder participation in the CNSC's environmental assessment (EA) and licensing process
- assist stakeholders in bringing valuable information to the Commission through informed and topic-specific interventions related to aspects of environmental assessment and licensing

Eligible applications include individuals, Aboriginal groups, not-for-profit corporations and other stakeholders that meet specific criteria that include a direct local interest in the project, Aboriginal traditional knowledge or local community insight, and can bring valuable topic-specific information to the Commission. Funding award decisions are made by an appointed independent Funding Review Committee, which includes up to three individuals external to the CNSC and selected based on their knowledge and background in nuclear, regulatory and environmental matters.

Personal information is collected during the application process from individuals applying for funding under the PFP. Personal information is also collected from individuals participating as members of the Funding Review Committee. Personal information, such as knowledge expertise, location and interest in the project, is used to determine eligibility for participation as a committee member and eligibility for participant funding.

The personal information collected may include: name, contact information (title, mailing address, email, telephone number, fax number), preferred language of correspondence, category of applicant (individual/organization/etc.), biographical information, personal opinions and views, signature, as well as financial information such as per diems and salaries.

Application forms and supporting documentation will be held securely in e-Docs, the CNSC's electronic document management system.

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

Operational information collected in support of the PFP is reflected in the following Class of Record:

Public engagement and outreach

Description: This class includes records related to public engagement and outreach, which develop and implement strategies that identify existing and emerging key stakeholder groups, and then develop tools and tactics to reach these specific stakeholders (including the formal duty to consult with Aboriginal groups). The information provided is credible, easily understood and tailored to stakeholder information needs. Stakeholders include the Canadian public, Canadian nuclear licensees, vendors, the academic community, special interest groups, other government departments, other jurisdictions, international organizations, and Aboriginal groups. This program administers funding in accordance with the CNSC Grants and Contributions Program.

Document types: correspondence, strategies, plans, briefing materials, grant and contribution applications, stakeholder lists, presentations, datasheets, research results, historical data, discussion papers, travel and engagement plans, lists of attendees, minutes, agendas, records of decision.

Record number: CNSC 1.5.4

The institution-specific PIB related to this initiative follows:

Participant Funding Program
Description: This bank describes information that is related to the Participant Funding Program, which was established to give the public, Aboriginal groups and other stakeholders the opportunity to request funding from the CNSC to participate in its regulatory processes. The personal information collected may include: name, contact information (title, mailing address, email, telephone number, fax number), preferred language of correspondence, category of applicant (individual/organization/etc.), biographical information, personal opinions and views, signature, as well as financial information such as per diems and salaries.
Class of individuals: individuals, Aboriginal groups, and other stakeholders in the general public who have a direct, local interest in the project; external Independent Funding Review Committee Members.
Purpose: Personal information is collected under the authority of paragraph 21(1)(b.1) of the *Nuclear Safety and Control Act* for the assessment of applications for funding under the PFP and the disbursement of funds to successful applicants.
Consistent uses: Information, including the identities of individuals and the amount of funding received, will be posted on the PFP section of the CNSC's website, as well as the proactive disclosure section of the CNSC's website for contributions over $25,000. Funding applications are reviewed by the Funding Review Committee, which may include individuals external to the CNSC and selected based on their knowledge and background in nuclear regulatory and environmental matters. Information may be used for reporting to senior management, program evaluation, audit and evaluation. Some personal information may be disclosed to Public Services and Procurement (Receiver General Payments PWGSC PCU 712) in order to facilitate payment to successful applicants.
Retention and disposal standards: Records will be retained for six complete years following the conclusion of the hearing for which the funding was received.
RDA number: 2015/009
Related Class of Record number: CNSC 1.5.4
TBS registration number:
Bank number: CNSC PPU 030

Legal authority for program or activity

Nuclear Safety and Control Act, section 21(1)(b.1)

Risk area identification and categorization

1. **Type of program or activity**
   Personal information collected in support of the PFP may be used to make decisions that directly affect the individual (i.e., determining eligibility for funding, administering program payments, overpayments, processing appeals).

   Level of risk to privacy – 2

2. **Type of personal information involved and context**

   The PFP requires the collection of some sensitive personal information. For example, financial information, education, credentials, personal opinions and views about applicants.

   Level of risk to privacy – 3

3. **Program partners and private sector involvement**

   Delivery of the PFP involves the sharing of application information, including the financial banking details of applicants, with Public Services and Procurement Canada, in order to facilitate payment. In addition, applications are reviewed by a Funding Review Committee that includes private sector evaluators with knowledge of the project.

   Level of risk to privacy – 4

4. **Duration of the program or activity**

   The PFP is intended to be a long-term initiative, without an established sunset date.

   Level of risk to privacy – 4

5. **Program population**

   The PFP affects individuals who apply to receive funding under the initiative.

   Level of risk to privacy – 1

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 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, 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

The electronic document management system in use at the CNSC allows individual users with access to documents to be able to print the documents. If exported from the electronic document management system, the records could be saved to a portable device; however, there are system-wide security restrictions on the use of portable devices at the CNSC. Information is transmitted electronically to members of the Funding Review Committee.

Level of risk to privacy – 4

8. Risk impact in the event of a breach

In the event of a breach of personal information associated with the PFP, the CNSC would likely need to change procedures; in addition, public confidence would decrease with respect to how personal information is safeguarded.

Level of risk to privacy - 4