Section 1 – Overview and PIA Initiation

Government Institution: Royal Canadian Mint (Mint)

Official Responsible for the PIA:
Simon Kamel, Vice-President
Corporate and Legal Affairs

Head of the government institution or Delegate for section 10 of the Privacy Act
Emily-Brynn Rozitis, Senior Program Manager, Privacy
Corporate and Legal Affairs

Name of Activity:
Access to Information and Privacy (ATIP) Software

Personal Information Bank Descriptions:
Access to Information Act and Privacy Act Requests, PIB #PSU 901

Legal Authority for Activity:
The personal information collected by the ATIP software is collected under the authority of:

- sections 6 and 11 of the *Access to Information Act* (ATIA) and sections 4 and 5 of the ATIA *Regulations*.
- section 13 of the *Privacy Act* and section 8 and 11 of the *Privacy Regulations.*

Description Summary:
As a federal Crown corporation, the Mint is subject to the ATIA*, Privacy Act*, and their Regulations, and all related Treasury Board of Canada Secretariat ("TBS") policy instruments. Both Acts provide for the right of Canadians and, as applicable, other individuals to seek access to information held by federal government institutions, including the requesters' personal information. Historically, the Mint's implementation and management of the above requirements has largely been a manual process. To modernize and streamline its delivery of ATIP services through digitization, the Mint implemented an ATIP software solution that was selected by the Government of Canada following a TBS-led competitive Request for Proposal process.

PIA Scope:
The PIA was scoped based on factors such as the sensitivity of the involved personal information and expected level of risk to individuals and the Mint. The PIA analyzed the personal information practices associated with the new software solution in accordance with legal and policy requirements and ensured that any privacy risks were identified with a related recommendation and mitigation plan. As PIAs are evergreen documents, the Mint commits to revisiting the report's content in the event of future process and system changes.

Section 2 - Risk Area Identification and Categorization

The following section contains standardized risks identified in the PIA report per the TBS requirements for a core PIA. The common, numbered risk scale is utilized where appropriate in ascending order: the first level (1) represents the lowest level of potential risk for the risk area; the fourth level (4) represents the highest level of potential risk for the given area.

A) Type of program or activity

Risk scale – 2: Administration of a program or activity and services.

B) Type of personal information involved and context

Risk scale – 3: Social Insurance Number, medical, financial or other sensitive personal information or the context surrounding the personal information is sensitive; personal information of minors or of legally incompetent individuals or involving a representative acting on behalf of the individual.

C) Program or activity partners and privacy sector involvement

Risk scale – 3: - With other institutions or a combination of federal, provincial or territorial, and municipal governments.

D) Duration of the program or activity

Risk scale – 3: Long-term program or activity.

E) Program population

Risk scale – 3: The program's use of personal information for external administrative purposes affects certain individuals.

F) Technology and privacy

Does the new or substantially modified program or activity involve implementation of a new electronic system or the use of a new application or software, including collaborative software (or groupware), to support the program or activity in terms of the creation, collection or handling of personal information?

Yes

Does the new or substantially modified program or activity require any modifications to information technology (IT) legacy systems?

No

Does the new or substantially modified program or activity involve implementation of new technologies or one or more of the following activities:

Enhanced identification methods?

No

Use of surveillance?

No

Use of automated personal information analysis, personal information matching and knowledge discovery techniques?

No

G) Personal information transmission

Risk scale – 2: The personal information is used in a system that has connections to at least one other system.

H) Privacy breach risk impact

Potential risk that in the event of a privacy breach, there will be an impact on the individual or employee?

Yes. Expected moderate risk impact: Inconvenience, reputational and/or financial harm.

Potential risk that in the event of a privacy breach, there will be an impact on the institution?

Yes. Expected moderate risk impact: Inconvenience and/or reputational harm.