Section 1 – Overview and PIA Initiation

Government Institution: Royal Canadian Mint (Mint)

Official Responsible for the PIA:
Francis Mensah
Chief Financial Officer and Vice-President
Finance and Administration

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:
Travel and Expense Software Solution (TESS)

Personal Information Bank Descriptions:
- Travel, PIB #PSU 909
- Hospitality, PIB #PSU 908
- Accounts Payable, PIB #PSU 931
- Members of Boards, Committees and Councils, PIB #PSU 919
- Relocation, PIB #PSU 910

Legal Authority for Activity:
The personal information for TESS is collected under the authority of the *Financial Administration Act* and ss. 4(1) and 19 of the *Royal Canadian Mint Act.*

Description Summary:
Travel, hospitality, conference and event (THCE) expense management forms a critical component of the Mint's business. The procurement of an expense processing software solution was deemed necessary to replace manual processes, mitigate against administrative errors, and ensure heightened THCE policy compliance. Through a request for proposal procurement process, the Mint selected a software solution to be customized to the Mint's THCE needs, and to implement streamlined and modernized paperless processes for approvals, expense submission, reconciliation, and reporting.

PIA Scope:
The PIA was carefully scoped based on factors such as other planned stakeholder reviews and the expected low risk of privacy impact 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 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 – 2: Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.

C) Program or activity partners and privacy sector involvement

Risk scale – 4: Private sector organizations, international organizations or foreign governments.

D) Duration of the program or activity

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

E) Program population

Risk scale – 1: The program's use of personal information for internal administrative purposes affects certain employees.

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.

Risk scale – 4: The personal information is transmitted using wireless technologies.

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 low risk impact: Inconvenience to individuals.

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

Yes. Expected low risk impact: Inconvenience to organization, embarrassment.