Section 1 – Overview and PIA Initiation

Government Institution: Royal Canadian Mint (Mint)

Official Responsible for the PIA:
Michel Boucher
Vice-President Human Resources

Head of the government institution or Delegate for section 10 of the Privacy Act
Andrea Kniewasser
Director, Regulatory Affairs (Compliance)
Corporate and Legal Affairs

Name of Activity:
Mental Health Peer Support Program (MHPSP)

Personal Information Bank Descriptions:
- Institution-specific: Mental Health Peer Support Program PPU 018 (under TBS review)
- Standard: Occupational Health and Safety, PSE 907
- Standard: Training and Development. PSE 905

Legal Authority for Activity:
The personal information required for the MHPSP is collected under the authority of the *Canada Labour Code* Part II: subsections 122.1 and 122.2; and 125(1), as well as subsections 17 and 19 of the *Royal Canadian Mint Act*.

Description Summary:
The MHPSP falls under the Mint's overall mental health strategy and is offered to Mint employees as a separate but complementary option to the Mint's Employee Assistance Program. The overall objective of the program is to promote and enable a healthy and psychologically safe work environment by supporting employees with their mental health. The peer support approach leverages a trusting relationship between someone who has been living with a mental health problem/issue, directly or indirectly, and a co-worker with a similar experience. Peer Supporters will receive training in first aid mental health as well as how to provide comfort, empathy, share lessons learned and direct individuals to other resources.

PIA Objective and Scope:
The purpose of this PIA is a fulsome assessment of the privacy risks associated with the business processes involving the personal information required for the administration of the MHPSP (collection, use, disclosure, retention and disposal), as well as to ensure overall compliance with the *Privacy Act* and related TBS privacy policy suite. The delivery of required training courses for the MHPSP, including the mental health first aid, are out of scope (save for the records required by the program to confirm participant completion).

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; and

Risk scale – 4: Sensitive personal information, including detailed profiles, allegations or suspicions and bodily samples, or the context surrounding the personal information is particularly sensitive.

C) Program or activity partners and privacy sector involvement

Risk scale – 1: Within the institution (among one or more programs within the same institution).

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?

No

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 moderate-high risk impact: breach of sensitive personal information could result in impact to reputation, mental health and wellbeing.

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

Yes. Expected moderate risk impact: reputational harm and embarrassment, loss of employee trust.