

Privacy impact assessment summary

Military Family Services Program / Veteran Family Program (MFSP/VFP)

Section I: Overview and privacy impact assessment initiation

Government institution:

Canadian Forces Moral and Welfare Services (CFMWS)¹

Government official responsible for the program or activity:

Colonel C.D. Harris
Director Military Family Services (MFS) Division, CFMWS

Head of the government institution / delegate for section 10 of the *Privacy Act*:

Rachelle Delage
National Manager Access to Information and Privacy (ATIP) Program
Corporate Services Division, CFMWS

Name and description of program or activity:

The Military Personnel and Organization Lifecycle²

Program seeks to enable the production of ready force elements and fulfill obligations of Defence Combat and Support Operations, Defence Services and Contributions to Government, and Defence Capability Development and Research through the provision of the military establishment, personnel, and personnel services. The Program also honours and recognizes the service and unique sacrifices of our military personnel, provides for a safe and secure workplace, and ensures the appropriate conduct of Defence military personnel. It ensures that personnel are available in the quantity, mix of occupations and with the requisite occupational skills that provides for an optimized military establishment that enables the readiness and employment of multi-purpose combat capable forces and other Defence services. The Program oversees the availability of Regular and Reserve Force personnel to fulfill the military establishment, and the delivery of services provided to the personnel, including recruitment services; transition and release services; professional development services, occupation training services; morale and well-being services; health care services; compensation and benefits services, honours and recognition services, security, protection, justice and safety services, and the planning and governance of the Program. The Program coordinates the execution of subordinate programs responsible for promoting a unified Defence culture and a safe and secure workplace and the planning and governance of the Program. The authority for this Program is derived from the *National Defence Act*.

¹ CFMWS is the current operating name of the organization responsible for administering and delivering Non-Public Property (NPP) programs on behalf of the Chief of Defence Staff.

² Program activity and class of record as currently published in the *Info Source* for the National Defence and Canadian Forces.

Description of the class of records associated with the program or activity:

Welfare

Description: Information dealing with the Canadian Forces Welfare Program and Services.

Document Types: Financial counselling, and social work services.

Record Number: DND PSB 405

Personal information bank (PIB):

- Proposal for a new PIB
- Proposal to modify an existing PIB
- No modification required for the existing PIB

Legal authority for the program or activity:

In 1969, TB minute 689194 introduced the concept of delivering Morale and Welfare (MW) programs through a combination of Public and Non-Public Property (NPP) resources.

The *National Defence Act* (NDA), Sections 2 and 38 – 41, vests NPP with the Chief of the Defence Staff (CDS), Base / Wing Commanders and Unit Commanding Officers to be used for the benefit of serving and former Canadian Armed Forces (CAF) personnel and their families.

Canadian Forces Morale and Welfare Services (CFMWS) is the organization responsible for administering NPP programs and activities on behalf of the CDS and for delivering selected public MW programs, services, and activities to eligible members and their families on behalf of the Chief of Military Personnel (CMP).

To recognize the vital role played by the families of Veterans living with physical and mental health issues as a result of their service, Budget 2017 proposed to invest \$147.0 million over six years, starting in 2016–17, and \$15.0 million per year ongoing, to expand access to the Military Family Services Program (MFSP) through Military Family Resource Centres (MFRCs) for the families of Veterans medically released. This would increase the availability of the MFSP for medically released Veterans through all 32 MFRC locations across the country.

Summary of the project, initiative, or change:

The MFSP promotes and facilitates community-based services and programs to enhance the well-being of military families. As such, Military Family Services (MFS), a division of CFMWS, invests in front-line services for families through MFRCs, which are located on bases, wings and units across Canada. In the United States and in Europe, MFS employs staff who offer a host of services and outreach to families who are posted outside of Canada.

In addition to services and support available locally at MFRCs, MFS also connects military families nationally to services and support through the Family Information Line (FIL) and www.CAFconnection.ca. FIL is a 24/7 bilingual, confidential toll-free service at 1-800-866-4546 and email services that provides supportive counselling, useful information and referral to services, and immediate crisis management support to military families. Another access point to services is through www.CAFconnection.ca, a website for and about military families that connects families with their local MFRC in Canada, and MFS staff in the United States and in Europe, and other available services and resources.

The MFSP works to ensure that the Canadian military family community is well supported in order for military families to lead positive and nurturing family lives comparable to other Canadian families while supporting the operational effectiveness of the Canadian Forces (CAF).

In October 2015, a Memorandum of Understanding (MOU) between Veterans Affairs Canada (VAC) and the CDS, in his NPP capacity through CFMWS, launched a trial initiative – the Veteran Family Program (VFP). The VFP offered transition-focused core programming and extended MFSP to medically released Veterans and their families for two years post release at seven (7) pilot MFRC locations. As part of the 2017 Federal Budget, VAC expanded access to the VFP to encompass all 32 MFRCs to the target population, on an unlimited basis post-release.

Local MFRC services available to medically released CAF Veterans and their families will include, but are not limited to the following:

- Welcome and community orientation (e.g., assistance finding a doctor)
- Workshops for children and teens
- Parenting workshops
- Emergency child care
- Outreach/information and referral
- Employment and education assistance
- Personnel growth and development programming (includes self-help groups, short-term interventions and crisis support and family liaison including support for parents)
- Second language services

MFRCs as well as MFS staff in Europe and US receive personal information from the Department of National Defence (DND) regarding CAF personnel, including name, home address and telephone number, and reason for notification, in accordance with CANFORGEN 164 ADM(HR-MIL) 068 2411213Z OCT 05, as updated from time to time. They also receive further personal information directly from families they serve. As such, the MOU between DND and the MFRC states that they must comply with the Privacy Code for Military Services Program and the Application Guide to the Privacy Code for Military Services Program.

MFS commissions a Compliance and Assurance Review of the MFRC, once every three years, to monitor the activities under the MOU and to ensure that personal information collected by the MFRCs is handled in accordance with the provision of the "MFSP Privacy Code" as published by MFS, and updated from time to time (available at www.CFMWS.com). For greater certainty, it is understood that the MFRCs hold personal information in confidence, within legal bounds.

To date, MFRCs report program and service usage data to MFS. As each MFRC has their own methodology for collecting data, this has resulted in challenges related to reliability, comparability and the ability to capture unique families served. In the one-year review of the VFP pilot, VAC raised concerns that they required the unique families served data for their reporting requirements to Treasury Board. In addition, MFRCs noted that the collection process took an unreasonable amount of time, time that could have been used supporting families.

In order to support consistent and reliable case management and data collection across MFRCs and FIL, CFMWS has selected the Penelope Case Management Software, a business solution provided by Athena Software, to be implemented with trained users, by April 1, 2018, concurrent with the launch of the expanded VFP. The system is already in use at two (2) MFRCs (Trenton and Petawawa). Data conversion/migration from former/current systems, if required, will be manually uploaded to the Penelope application, if necessary.

For improvement of operational efficiencies, the Penelope system will be a centrally controlled client relationship management (CRM) system to be used by 32 MFRCs, MFS, and FIL. Security settings such as role-based accounts will facilitate and control appropriate levels of access to data. Rather than the MFRCs sending their data, MFS will be able to extract the figures needed to report to VAC. The Penelope system will be used to capture data for the 2018-2019 fiscal year, beginning April 1, 2018.

Previously the risk of a breach of confidentiality rested with the MFRCs, as (federally/provincially/territorially) incorporated, not-for-profit organizations. Now that the system will be centralized under CFMWS, a PIA has been undertaken to demonstrate due diligence and support informed decision-making during the development and future development of the project.

Initially, the data collected will be to support the VFP. Once established, the intention is to access the value of including all MFSP program and service data.

Section II: Risk area identification and categorization

The tables below provide privacy risks associated with the program or activity. The numbered risk scale is presented in an ascending order: level 1 represents the lowest level of potential risk for the risk area; level 4 represents the highest level of potential risk for the given risk area. The greater the number of risk areas identified as level 3 or 4, the more likely it is that specific risk areas will need to be addressed in a more comprehensive manner.

A: Type of program or activity	Risk scale
Program or activity that does not involve a decision about an identifiable individual	<input type="checkbox"/> 1
Administration of programs / activity and services	<input checked="" type="checkbox"/> 2
Compliance / regulatory investigations and enforcement	<input type="checkbox"/> 3
Criminal investigation and enforcement / national security	<input type="checkbox"/> 4
Personal information is used to administer the MFSP/VFP in order to identify programs and services to which clients may be referred for assistance, and for case management and documentation of assistance provided.	

B: Type of personal information involved and context	Risk scale
Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.	<input type="checkbox"/> 1
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.	<input type="checkbox"/> 2
Social insurance number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual.	<input checked="" type="checkbox"/> 3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.	<input type="checkbox"/> 4
The activities involve sensitive information about the client including psychosocial functioning, mental health, intervention, recommendations, referrals, etc.	

C: Program or activity partners and private sector involvement	Risk scale
Within CFMWS (amongst one or more programs within CFMWS)	<input checked="" type="checkbox"/> 1
With other federal institutions	<input checked="" type="checkbox"/> 2
With other or a combination of federal/ provincial and/or municipal government(s)	<input type="checkbox"/> 3
Private sector organizations or international organizations or foreign governments	<input checked="" type="checkbox"/> 4
<p>VAC will be providing funding, advice, functional guidance, and training on VAC services to CFMWS and MFRC staff. There will be no sharing of personal information of medically released CAF Veterans or their families between the MFRC/FIL and VAC.</p> <p>CFMWS will be responsible for program development, management, oversight, evaluation and funding allocation to each MFRC, FIL and CAFconnection.ca for service delivery.</p> <p>MFRCs are Canadian not-for-profit organizations with charitable status that are family governed, legally independent, provincially or federally incorporated, and federally funded to deliver the MFSP/VFP.</p> <p>Athena Software is the contactor selected to provide the Penelope Case Management Software as a hosted Software as a Service (SAAS) solution.</p>	

D: Duration of the program or activity	Risk scale
One time program or activity	<input type="checkbox"/> 1
Short-term program	<input type="checkbox"/> 2
Long-term program	<input checked="" type="checkbox"/> 3
MFSP and VFP are long-term programs with no established end date.	

E: Program population	Risk scale
The program affects certain employees for internal administrative purposes.	<input type="checkbox"/> 1
The program affects all employees for internal administrative purposes.	<input type="checkbox"/> 2
The program affects certain individuals for external administrative purposes.	<input checked="" type="checkbox"/> 3
The program affects all individuals for external administrative purposes.	<input type="checkbox"/> 4
The target population for MFSP/VFP includes all CAF serving members and all personnel medically released from service, as well as their parents, spouse/common law partner, children up to and	

including those 18 years of age (including step-children), and/or other dependent relative(s) of the individual.

While not a target population, MFSP/VFP may gather information for Veterans and their families who request services but do not fit eligibility requirements of the VFP program. This is captured to report to VAC the number of individuals and families seeking support that fall outside the current mandate of the program. This is necessary for considering whether to expand the VFP to all Veterans regardless of whether they are medically released or when they were released. These interactions are captured so that the associated costs can be charged back to VAC.

F: Technology and privacy	Yes / No
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?	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
Does the new or modified program or activity require any modifications to IT legacy systems and / or services?	<input type="checkbox"/> Yes <input checked="" type="checkbox"/> No
Does the new or modified program or activity involve the implementation of one or more of the following technologies? <ul style="list-style-type: none"> - Enhanced identification methods - Surveillance - Automated personal information analysis, personal information matching and knowledge discovery techniques 	<input checked="" type="checkbox"/> Yes <input type="checkbox"/> No
A “ yes ” response to any of the above indicates potential privacy concerns and risks that will need to be considered and, if necessary, mitigated.	
<p>The Penelope Case Management Software system is to provide an automatic audit trail and monitoring controls of all system activity by user, date and time in order to be able to detect unauthorized user activity.</p> <p>Through information provided by the presenting client, individual profiles of the primary member and family will be linked to a case file representing the family.</p> <p>An automated email communication system will be used to send periodic service performance questionnaires to service users at specific time increments. This feature will be used to track degree of impact. Clients will provide data used to analyze the results.</p>	

G: Personal information transmission	Risk scale
The personal information is used within a closed system (i.e., no connections to the Internet, Intranet or any other system and the circulation of hardcopy documents is controlled).	<input type="checkbox"/> 1
The personal information is used in system that has connections to at least one other system.	<input checked="" type="checkbox"/> 2
The personal information is transferred to a portable device or is printed (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed.	<input checked="" type="checkbox"/> 3
The personal information is transmitted using wireless technologies.	<input checked="" type="checkbox"/> 4
<p>The CFMWS project team and MFRC/FIL end users will access the Penelope Case Management Software using one of the supported browsers.</p> <p>MFRCs have either Defence Wide Area Network (DWAN) computer or Internet access computer networks that they will use in a secure DND provided environment with some exceptions. They will conduct outreach services and therefore could access the cloud-based Penelope system through iPad, smart phone, or other Internet capable computer.</p> <p>Athena has implemented technical security measures to guard against unauthorized access to personal information transmitted over an electronic communications network. A security certificate from a valid signing authority verifies the connection to the appropriate server. All data is encrypted in transit and at rest on servers.</p>	

H: Potential risk impact to the individual in the event of a privacy breach
<p>Some MFSP/VFP services fall in to the category of psychosocial support. A breach could result in embarrassment or client physiological impact. The risk to the individual is considered to be LOW as there are limited number of services, i.e. short-term counselling, that would involve this level of sensitive data. This information is further protected by the Ethics and Conduct Code for the registered professional collecting the details. Penelope is designed not to allow users other than those authorized or whose case it is to view service notes. To further minimize the risk, guidelines allow for the professional not enter particular sensitive information directly into the Penelope system, but rather into a password-protected file that could be attached to the case file.</p>

I: Potential risk impact to the institution in the event of a privacy breach

A breach could have an impact on organizational credibility and reputation of the MFRCs, MFS, and CFMWS. The risk is LOW with the Penelope Case Management Software. The system runs as a complete SAAS solution on a Tier 3 Datacenter infrastructure. Athena Software has considerable experience in providing their solution to youth services organizations, parenting and teaching organizations as well as many community health organizations and organizations providing services for the deaf, the mentally ill and others. The solutions offers a high level of protection of the data they will hold on our behalf. Their datacenters are certified to a high degree and considerable resources have been expended in perfecting the security posture of their organization. They have a robust ongoing assessment of their product by third party assessors.