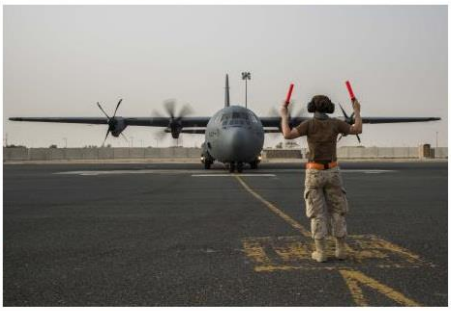
National Defence / Défense nationale

ASSISTANT DEPUTY MINISTER (REVIEW SERVICES)

Audit of Privacy and Protection of Personal Information



1259-5-020 ADM(RS)
978-0-660-45522-8
D2-639/2022E-PDF
September 2022

Canada

Table of Contents

Acronyms and Abbreviations

ADM(RS)	Assistant Deputy Minister (Review Services)
ATIP	Access to Information and Privacy
CAF	Canadian Armed Forces
CCS	Chief Corporate Secretary
CFMWS	Canadian Forces Morale and Welfare Services
CHRO	Chief Human Resources Officer
CIO	Chief Information Officer
COO	Chief Operating Officer
DND	Department of National Defence
IM	Information Management
IS	Information Security
IT	Information Technology
LAC	Library and Archives Canada
MW	Morale and Welfare
NM ATIP	National Manager, Access to Information and Privacy
NPF	Non-Public Funds
NPP	Non-Public Property
OCI	Office of Collateral Interest
OPC	Office of the Privacy Commissioner
OPI	Office of Primary Interest
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
RCMP	Royal Canadian Mounted Police
SISIP	Service Income Security Insurance Plan
SOP	Standard Operating Procedure
TB	Treasury Board
TBS	Treasury Board of Canada Secretariat

Results in Brief

The *Privacy Act* governs the personal information handling practices of federal institutions. The Act, which came into effect on July 1, 1983, governs the collection, use, sharing, disclosure and disposal of individuals' personal information. Under the *Privacy Act*, personal information is defined as information about an identifiable individual that is recorded in any form, and that can be used to identify an individual through its use, either alone or in combination with other information.

The Treasury Board (TB) *Policy on Privacy Protection* and *Directive on Privacy Practices* obligates federal institutions to protect personal information they have collected.

Since its inception in April 2017, Canadian Forces Morale and Welfare Services' (CFMWS) Access to Information and Privacy (ATIP) program has made significant efforts to build a strong privacy management framework. We noted several areas of positive privacy practices. We also identified areas in need of improvement.

We examined the management of privacy practices at CFMWS. All employees are responsible for privacy practices, but the National Manager, Access to Information and Privacy (NM ATIP), located within CFMWS Corporate Services Division, leads the overall privacy efforts for CFMWS. The ATIP program's overall responsibilities include the development of privacy policies, procedure and practices; the delivery of privacy training and awareness programs to staff; assessing and reporting on privacy breaches; coordinating and assessing CFMWS input for *InfoSource*; and providing privacy analysis and advice using a number of tools, such as Privacy Impact Assessments (PIA).

Key Findings and Recommendations

CFMWS is aware of protection of personal information as an important consideration in program delivery and business activities. CFMWS has developed a privacy management framework that establishes accountabilities and policies for the handling of personal information in compliance with the *Privacy Act* and the relevant TB Policies and directives.

Overall Conclusion

- CFMWS has a defined privacy management framework
- Key controls are in place to safeguard personal information

While the authorities delegated under the *Privacy Act* to the NM ATIP as the functional lead are clear, more detailed responsibilities are needed to ensure divisions assess privacy risks within their programs and enact controls such as employee training and oversight of third parties to safeguard personal information in a manner commensurate with its sensitivity.

Opportunities exist to enhance the security of personal information maintained within CFMWS operational databases by enhancing monitoring and compliance activities associated with the

various databases and disposal of personal information from the databases when this information is no longer needed.

Note: Please refer to Annex A—Management Action Plan for the management response to the ADM(RS) recommendations.

1.0 Introduction

1.1 Background

CFMWS is responsible for administering Non-Public Property (NPP) on behalf of the Chief of the Defence Staff, and for delivering selected Morale and Welfare (MW) Services and activities to eligible members and their families. MW programs fall into one of two categories:

a) Public Programs – MW programs that are (with some exceptions) reimbursed 100% by the public and are a public responsibility; or

b) NPP MW Programs – MW programs that may have a public component, but certain cost elements may receive a level of public support less than 100%. These programs are an NPP responsibility.

As a result of its collection, use and disclosure of personal information, CFMWS is subject to the requirements of the *Privacy Act*. It is also subject to the policies and directives issued by the TB which support the Act's administration; mainly, the *Policy on Privacy Protection,* the *Directive on Privacy Practices* and the *Directive on Privacy Impact Assessments*.

The *Privacy Act* provides the legal framework for federal institutions' collection, use, disclosure and disposal of personal information. The Act is founded on the principle that individuals have a right to know what information is being collected about them and how it will be used in the administration of government services or programs.

The *Privacy Act* sets out the rules governing the management of personal information held by federal government institutions. Sections 4 through 8 restrict the collection of personal information and limit how that information, once collected, can be used and disclosed.

The *Privacy Act* also addresses the retention and disposal of personal information. It balances the legitimate collection and use requirements essential to government programs with an individual's right to a reasonable expectation of privacy.

The TB *Policy on Privacy Protection* and *Directive on Privacy Practices* obligate federal institutions to protect personal information they have collected. The TB policy establishes baseline security requirements to protect information holdings, including personal information. However, institutions are responsible for conducting their own assessments to determine whether safeguards above baseline levels are required.

Prior to FY 2017/2018, ATIP activities related to NPP and the Staff of the Non-Public Funds (NPF), Canadian Forces were managed by the Department of National Defence's (DND) ATIP Office.

Following the Minister's approval of the NPP ATIP designation order in February 2017, and since the Staff of the NPF, Canadian Forces is a separate agency, CFMWS established its own ATIP office, which began to operate in April 2017.

The NM ATIP administers the provisions of the *Privacy Act* within the CFMWS for NPP and the Staff of the NPF, Canadian Forces.

The NM ATIP reports to the Director Corporate Services who, in turn, reports to the Vice-President Corporate Services (Chief Corporate Secretary (CCS)).

The NM ATIP is responsible for managing all activities related to the CFMWS ATIP Program, in accordance with the NPP ATIP designation order and the provisions of the *Privacy Act*, and applicable regulations, directives, policies and guidelines.

While ATIP plays a leading role in the development and support of privacy practices across CFMWS, the responsibility for the protection and handling of personal information at CFMWS is a shared responsibility between ATIP and the divisions. While the authorities delegated under the *Privacy Act* are to the NM ATIP, divisions must support the functional lead by ensuring that personal information under divisional control is managed in accordance with the *Privacy Act*. This involves, among other things, assessing privacy risks within their program, safeguarding personal information in a manner commensurate with its sensitivity, initiating a PIA when required, mitigating privacy risks though training, and monitoring and notifying ATIP immediately in the event of a breach.

1.2 Rationale

Individuals are increasingly concerned about the protection and security of their personal information. This concern increases the pressure on organizations to address privacy and data protection issues. The need to protect data from loss, theft or misuse has opened up an entirely new area of risk for organizations. Data-driven new technologies have raised additional new data protection and privacy concerns.

CFMWS collects personal information in the course of administering certain employer-paid benefits for Canadian Armed Forces (CAF) members, and Staff of the NPF, as well as providing services directly to CAF members, veterans and their families, and to employees of other federal institutions such as the Royal Canadian Mounted Police (RCMP) and the Canadian Coast Guard.

As such, CFMWS possesses and relies on the personal information of its members/clients, and protecting this information is vital. Privacy breaches could harm individuals and damage CFMWS' reputation. This audit examined the overall privacy management framework in place to govern CFMWS' personal information data holdings and provides some recommendations on how to better protect personal information under its care and control.

1.3 Objective

The objective of this audit is to assess CFMWS' Privacy Management Framework and determine whether the policies, procedures and practices for managing personal information comply with the *Privacy Act* and its supporting TB policies and directives.

2.0 Findings and Recommendations

2.1 Privacy Management Framework

Key elements of a comprehensive privacy management program are in place.

Under the government's *Policy on Privacy Protection,* heads of institutions are required to establish management practices to administer the *Privacy Act.* Generally, management practices are governed by way of a departmental/organizational privacy management framework. A privacy management framework program refers to the structures, policies, procedures and processes in place to ensure a government institution meets its obligations under the *Privacy Act*. Core elements include effective governance, clear accountabilities, a privacy breach protocol, a process for the identification and management of privacy risks, and awareness training.

Notable Practices

- CFMWS has an overarching privacy management framework to guide privacy activities
- Accountability for privacy compliance is set out in internal policies
- Common standards and practices for the handling of personal information have been established

A privacy management framework can be used as a foundational element in establishing and operating a comprehensive information privacy program that addresses privacy obligations and risks while facilitating current and future business opportunities.

The audit team conducted an assessment of CFMWS' privacy policies, procedures and practices against TB requirements in the TB *Policy on Privacy Protection,* the TB *Directive on Privacy Impact Assessments* and the TB *Directive on Privacy Practices*. Overall, the policies were found to have met the requirements of the *Privacy Act* and supported policies and directives.

The audit evidence indicated that the ATIP Directorate had established a number of policies and procedures to aid in the management and safeguarding of personal information under CFMWS' care and control. Overall, these policies and procedures were found to be concise and easy to understand. These policies and procedures are posted on the organization's intranet and are accessible to all employees. In April 2021, CFMWS' Cyber Security Policy and supporting directives came into effect. These documents set out the requirements for the safeguarding of information held in electronic format throughout its entire lifecycle.

2.2 Roles and Responsibilities

Pursuant to the *Privacy Act*, heads of government institutions may delegate select powers, duties or functions under the Act to one or more officers or employees. Once a delegation order has been signed, the powers, duties and functions delegated may only be exercised or performed by the deputy head, or by the named officers or employees. TB's *Privacy Policy* and

Directive on Privacy Practices set out clear responsibilities for decision making on matters under the Act and accountability for the management of personal information within an institution.

Through a Delegation Order, authority for certain statutory and regulatory requirements have been assigned to the NM ATIP. The NM ATIP reports to the Director Corporate Services who, in turn, reports to the Vice-President Corporate Services (within CCS). The one-person ATIP Section is responsible for managing all activities related to the CFMWS ATIP Program, in accordance with the NPP ATIP designation order and the provisions of the *Privacy Act*, Regulations, directives, policies and guidelines. In addition, the administration of the *Privacy Act* is also facilitated at the divisional levels of CFMWS. Each division has an ATIP point of contact who coordinates the collection of information. Liaison Officers provide assistance to the NM ATIP by searching and gathering records related to privacy requests in their respective divisions.

While ATIP plays a leading role in the development and support of privacy practices across CFMWS, the responsibility for the protection and handling of personal information at CFMWS is a shared responsibility between ATIP and the divisions. While the authorities delegated under the *Privacy Act* are to the NM ATIP, divisions must support the functional lead by ensuring that personal information under divisional control is managed in accordance with the *Privacy Act*. This involves, among other things, safeguarding personal information in a manner commensurate with its sensitivity, initiating a Privacy Impact Assessment when required and notifying ATIP immediately in the event of a breach.

Privacy responsibilities at CFMWS are described in several internally available documents, most notably: CFMWS' *Policy on the Access to Information and Privacy Program* and the CFMWS *Policy on Privacy Practices*. However, the documented privacy responsibilities for CFMWS program heads and staff do not take into account the type and sensitivity of the information handled by each role.

Responsibilities of program heads to assess privacy risks of their own programs, and embed privacy controls into program systems, procedures and training is not explicitly defined.

ADM(RS) Recommendation

1. It is recommended that CFMWS establish privacy responsibilities for divisions and program personnel to ensure clear accountabilities for privacy responsibilities.

OPI: CCS
OCI: All Divisions

2.3 Privacy Impact Assessment

CFMWS has a PIA process in place, which includes a policy to inform staff and stakeholders of the PIA directive and its requirements.

Under the Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Impact Assessments* (effective April 1, 2010), federal institutions are required to institute a formal process to identify and mitigate privacy risks when establishing any new or substantially modified program or activity involving personal information. The *Directive on Privacy Impact Assessments* establishes core elements for the conduct of PIAs, which focus on legal obligations related to privacy. Federal institutions must submit final PIA reports to the Office of the Privacy Commissioner (OPC) before they implement programs or services.

The PIA process helps ensure that privacy implications will be appropriately identified, assessed and resolved before a new or substantially modified program or activity involving personal information is implemented. PIA is the component of departmental risk management activities that focuses on developing appropriate privacy protections within new programs or activities.

CFMWS has implemented a formalized process to comply with the TBS *Directive on Privacy Impact Assessments* including roles and responsibilities, and steps to follow in determining the requirement for a PIA and for conducting the assessment.

CFMWS has established procedures to ensure that PIAs are considered for all new program initiatives. NM ATIP works closely with Information Management/Information Technology (IM/IT) to identify and mitigate security risks related to the introduction of new IT systems. Considering the need for a PIA is a specific step in the standard IT project life cycle.

Program managers are responsible for initiating PIAs for all new programs and services under their control, while the one-person ATIP Section is responsible for facilitating the PIA process at CFMWS, for providing privacy tools and approving PIAs prior to review by the OPC. To date, only one formal PIA has been completed by CFMWS.

Privacy risks also arise from ongoing operations. Several CFMWS databases were developed prior to the requirement for a PIA to be conducted. As a result, it is difficult to ascertain whether all privacy implications have been identified and addressed. At present, the NM ATIP is working with the various program areas to help identify and address privacy risks in on-going operations.

ADM(RS) Recommendation

2. It is recommended that CFMWS regularly identify privacy risks to on-going operations and ensure controls are in place to mitigate these risks.

OPI: CCS
OCI: COO

2.4 Training and Awareness

The TB *Policy on Privacy Protection* expects the deputy head or delegates to be responsible for making employees aware of policies, procedures and legal obligations under the *Privacy Act*. It is critical that CFMWS employees understand how to properly safeguard personal information, since a lack of awareness could lead to a major privacy incident and harm CFMWS' reputation. Therefore, implementing a privacy awareness training program to equip all employees to proactively protect personal information is vital. Privacy training helps staff identify and mitigate privacy risks.

It is important to train and promote privacy awareness among all staff, especially those who will handle personal information regularly. A privacy overview can be included in a new hire orientation program. Learning objectives should include understanding their responsibilities as a data steward to identify and safeguard personal information, and when and how to report a privacy incident.

CFMWS' training and awareness program included the delivery of informal briefings to division heads and management teams, as well as a presentation conducted in fiscal year 2017/2018 for the Executive Management Board. Guidance is also provided to managers and employees at all levels on an "as needed" basis. The audit noted a number of examples of program managers seeking guidance and advice from ATIP on the application of the *Privacy Act* and its supporting policies and directives. A number of employees have completed the free online course entitled Access to Information and Privacy Fundamentals that is available on GCCampus.

Although, CFMWS has developed mandatory Security Awareness training, its focus is on the confidential handling of personal information and not on the broader responsibilities under the *Privacy Act*. Security and privacy are not synonymous. Without a CFMWS specific privacy awareness training, the likelihood that employees are unaware of their responsibilities and what to do in the event of a privacy breach increases.

Going forward, CFMWS intends to make the Access to Information and Privacy Fundamentals course mandatory for all its employees. Given that ATIP training is no longer available to all CFMWS staff from GCCampus, CFMWS will develop its own ATIP fundamentals training course for all employees. While this initiative is important and commendable, CFMWS' ATIP awareness program, as currently designed, falls short of providing employees with a general awareness of core privacy principles so that they may fully consider privacy impacts when providing specific

services. CFMWS would benefit from a comprehensive privacy awareness strategy designed specifically for employees handling personal information on a day-to-day basis.

Guidance on how to apply privacy principles in day to day program operations is also important. The audit found that standard operating procedures (SOP) exist for some CFMWS programs. These SOPs govern the collection and use of personal information and provide direction to front line staff on how to best exercise their obligations under the *Privacy Act*. However, additional work is required to ensure that SOPs are in place for all of CFMWS' personal information data holdings.

ADM(RS) Recommendation

3. It is recommended that CFMWS expand its current privacy awareness and training program with specific training requirements for employees most actively involved in the handling of personal information and ensure that SOPs are in place for all CFMWS' personal information data holdings.

OPI: CCS
OCI: CHRO

2.5 Notice/Identifying Purpose

CFMWS is compliant with the notification provisions under the *Privacy Act*.

Pursuant to subsection 5(2) of the *Privacy Act*, a federal institution must inform individuals from whom it collects personal information of the purpose for which personal information is collected. At the time of collection, the individual who is providing the personal information must be informed of the purpose for which the information is being collected unless doing so would result in inaccurate information being collected or would defeat the purpose or prejudice the use for which the information is collected.

Notable Practices

- Collection practices do not extend beyond legislative mandate
- CFMWS limits its collection and use of personal information to that which is directly related to its operational activities

Under paragraph 6.2.9 of the *Directive on Privacy Practices*, institutions must notify the individual whose information is collected directly of the following:

1. The purpose and the authority for the collection
2. Uses or disclosures that are consistent with the original purpose
3. Uses or disclosures that are not related to the original purpose
4. Legal or administrative consequences for refusing to provide the personal information
5. Rights of access to, correction of and protection of personal information under the Act

The CFMWS Privacy Notice and application/enrollment forms, which are posted on the internet, summarize the CFMWS privacy practices. They advise that CFMWS collects personal information under the authority of the *National Defence Act* and the purpose for which the information is collected. The Notice also includes a reference to how the information may be used and how to withdraw consent.

When creating a form involving the collection of personal information, the CFMWS *Policy on Privacy Practices* requires that managers consult with NM ATIP for a compliance review and the inclusion of the appropriate privacy notice and consent statement. Interviews with senior management and a review of correspondence between NM ATIP and the divisions show there was consultation with the NM ATIP when developing new forms. The NM ATIP has also taken the initiative to review current forms and to challenge the collection of various data elements.

2.6 Limiting Collection and Use

A sound privacy management framework includes ensuring that an institution only collects the information that it currently needs and has the authority to collect. CFMWS' authority to collect personal information falls under the *National Defence Act*.

Pursuant to section 4 of the *Privacy Act*, personal information can only be collected by a federal institution if it relates directly to an operating program or activity of the institution. The institution must have legislative authority for the particular program or activity and also have a demonstrable need for each element of personal information collected. Personal information can only be used for the purposes for which it was collected or for a purpose consistent with that purpose.

CFMWS collects personal information required to administer various programs and services. In addition to biographical data (e.g., names, addresses, dates of birth, marital status, military service numbers), financial, medical and military service information is collected.

CFMWS recognizes the importance of ensuring that its data holdings only contain information that it has the legislative authority to receive. CFMWS has taken a number of concrete steps in recent years to limit their collection of personal information to that which is required to deliver its programs. Personal information is generally collected from the person to whom it relates, with some exceptions that are currently under review.

Personal Information Banks (PIB) are descriptions of personal information under the control of a government institution that are organized and retrievable by an individual's name or by a number, symbol or other element that identifies that individual. Under the *Privacy Act,* heads of government institutions are required to identify, describe and publicly report their PIBs. PIBs are the vehicles through which a government organization informs the public about the personal information it collects. Through these descriptions, individuals can also learn how their personal information is used, and for how long the information is being retained.

The audit team examined a sample of application/enrollment forms used to collect personal information along with the information listed in the corresponding CFMWS institution specific PIBs to confirm the personal information collected by the forms was consistent with the information identified in the PIBs.

For the two programs examined, the audit found that PIBs had been established to define and approve the collection of information consistent with the program, and that application/enrollment forms were collecting information consistent with the PIBs.

2.7 Limiting Disclosure

As per Section 8(1) of the *Privacy Act*, personal information under the control of a government institution shall not be disclosed by the institution, without the consent of the individual to whom it relates, obtained at the time the information is first collected.

Section 8(2) of the *Privacy Act* identifies 13 authorized grounds for disclosure without consent.

CFMWS' general Privacy Notice, program-specific PIBs and the notice on program-specific forms describe the manner in which personal information gathered may be shared.

The audit team reviewed a sample of application/enrollment forms used by CFMWS and found that the information disclosure notices on the forms used by individuals to provide their information and to provide their consent to disclosure of this information corresponded with PIBs and CFMWS' Privacy Notice. Therefore, the individuals providing consent were well informed of the potential circumstances in which their personal information may be disclosed.

2.8 Information-Sharing Agreements with Third Party Service Providers

The TB *Directive on Privacy Practices* requires that contracts that are established with private-sector entities outline measures and provisions to address the following:

- Control over the personal information;
- Limitations on collection and handling as well as any prohibitions regarding the personal information for the purposes of the contract;
- Disposition of the personal information, where relevant;
- Administrative, technical and physical safeguards; and
- Obligations of other parties acting on behalf of a government institution.

Institutions subject to the *Privacy Act* are accountable for personal information under their control. Contracting out a program or service does not relieve an institution of its privacy obligations. A lack of controls or weaknesses in the third parties' control design, operation or effectiveness could result in a privacy breach. Therefore, contracts with third parties should

contain appropriate provisions for controls for protection of personal information and privacy. They should also contain the requirement for monitoring or auditing to ensure that information collected or transferred to third parties is secure throughout its lifecycle.

CFMWS has entered into contracts with third parties in various sectors, including banking and insurance industries, as well as commercial businesses, to facilitate the delivery of programs and services. Given the sensitivity and volume of data being disclosed by CFMWS to third parties and the consequences associated with potential data breaches, appropriate information-sharing agreements are an important means of mitigating some of the risks associated with data transfers.

A review of several internal policy instruments found that the policies and guidance in place for entering into third-party contracts are quite prescriptive. We reviewed CFMWS' General Conditions for engaging in contracts with third-party service providers. It stipulates that the contractor shall keep private and confidential any personal information collected, created or handled by the contractor under the contract and shall not use, copy, disclose, dispose of or destroy except in accordance with the provisions of the contract. We also reviewed the CFMWS *Directive on Cybersecurity and People,* which requires that information-sharing agreements with external providers identify the requirements for the protection of confidential information. The CFMWS guidance is consistent with the requirements of the *Privacy Act* and policy guidance of the TBS on protection of privacy clauses in contracts.

CFMWS' guidance requiring specific clauses on privacy within formal contracts with third parties is commendable. The audit also noted that the NM ATIP regularly consults with program managers on aspects of privacy that should be included in agreements with third parties. However, we were unable to confirm the number of information-sharing agreements in effect at the time of this audit. Without an up-to-date inventory of the third parties and the nature of the transfer of private information, it is not possible to confirm that appropriate clauses have been used in formal contracts.

As acknowledged through interviews, CFMWS does not have a formal process in place to monitor the compliance of third parties with privacy protection clauses in agreements. Instead, CFMWS programs rely on the heightened focus and regulations imposed in the financial services and insurance sectors. This practice may not be sufficient to provide assurance that data handling practices are consistent with the terms of the agreements and effective in providing protection of personal information.

ADM(RS) Recommendation

4. It is recommended that CFMWS maintain an up-to-date inventory of business arrangements where personal information is transferred to a third party, and obtain assurances that the data handling practices of their partners are consistent with the terms of its information-sharing agreements.

OPI: COO, CCS
OCI: CIO, Division Heads

2.9 Limiting Retention

Under subsection 6(1) of the *Privacy Act*, institutions must retain personal information used for an administrative purpose in order to ensure the individual to whom it relates has a reasonable opportunity to access the information if desired. Section 6(3) goes on to say that the ultimate disposal of personal information under the control of an institution should be performed securely, and in accordance with record disposition authorities of Library and Archives Canada (LAC).

Federal institutions are expected to develop retention and disposal schedules to manage their records. These schedules establish how long records will be kept before they are destroyed or transferred to LAC. The Library and Archivist of Canada issues Records Disposition Authorities for this purpose.

A records retention and disposal schedule is important from a privacy perspective, as retention past the period it is used in program, exposes the information to potential misuse with no benefit to the program.

CFMWS has documented retention periods for most of its data holdings as disclosed in *Info Source*. While these retention periods were developed in cooperation with LAC, CFMWS is still waiting for LAC to provide Record Disposition Authority Numbers for some of these data holdings.

2.10 Disposal

Some information may be retained longer than the required retention period because IT systems lack mechanisms to dispose of personal information that is no longer needed.

CFMWS has an obligation to protect the personal information it collects from the time it is obtained until it is disposed of by an approved method. Properly disposing of personal information is consistent with retaining only the necessary information. Records should be disposed of in a manner that does not pose a privacy risk.

We examined CFMWS' disposal practices and found that CFMWS has developed policies and SOPs for the disposal of both paper and electronic media, such as CDs and USBs. Classified, designated or sensitive material is to be destroyed through the use of burn bags or by an approved shredder. This is done by CFMWS Administrative Services and is recorded. Classified/designated Information Security (IS) awaiting destruction is stored in a secure container until it is properly disposed of.

Although we found that CFMWS has schedules that set out how long personal information may be retained before it is destroyed, we noted that some of the primary electronic repositories for client information do not have the technical capability to dispose of records. Instead, the records are segregated from the active files into a repository with highly restricted access. As a result of this limitation, personal information is not being disposed of at the end of the retention period.

ADM(RS) Recommendation

5. It is recommended that CFMWS dispose of the required data from its databases so that it follows best *Privacy Act* practices.

Functional OPI: COO
Technical OPI: CIO;
Database OPIs: SISIP and CFOne

2.11 Safeguarding of Personal Information

CFMWS has implemented administrative, physical and technical safeguards to protect its personal information holdings.

Sound security practices are an essential component for meeting the protection requirements established under the *Privacy Act*. Appropriate measures and controls must be present to ensure personal information is not subject to unauthorized access, use, disclosure, alteration or destruction.

Provisions governing the safeguarding of personal information are set out in the TBS *Directive on Privacy Practices*. TB policy establishes baseline security requirements to protect information holdings, including personal information. However, institutions are responsible for conducting their own assessments to determine whether safeguards above baseline levels are required.

Security safeguards must protect personal information from loss or theft as well as unauthorized access, disclosure, copying, use or modification. Access to information should only be provided on a 'need to know' basis, and only once staff have obtained an appropriate security clearance.

A review of the CFMWS' *Security Orders and Policy on Cyber Security* and its accompanying directives, issued on April 1, 2021, noted policies and procedures were in place to govern the safeguarding of personal information throughout its entire lifecycle. These documents set out internal security practices and procedures and the responsibility of each member of the CFMWS to abide by all security regulations and maintain proper security practices.

While security protocols surrounding personal information vary depending on the sensitivity of the information collected, personal information under the care and control of CFMWS is generally safeguarded by way of physical measures (e.g., restricted access to operational areas and document storage, locked workstations when not attended); organizational measures (e.g., security clearances); and technological measures such as access controls, intrusion detection systems, passwords and encryption.

2.12 Access Controls

CFMWS has a formal user provisioning process to manage (assign, modify, revoke) access for all user types to all systems and services.

Where personal information or client data is collected, stored or maintained electronically, information must be protected through the use of adequate access controls. The term *access controls* is used to describe both the physical and technical solutions to allow access only to authorized individuals and to restrict the functions they are able to perform. Generally, the principle of *least privilege* should be applied, limiting each authorized user's access to the minimum information and resources needed to perform their legitimate duties and functions.

Automated role-based access within a system facilitates the ongoing management of access rights. It grants access permissions to roles and assigns employees to those roles. Changes made to the access level of a role are automatically assigned to all employees with that roll. Access controls should be managed to define authorized individuals or groups, their roles and their associated privileges. Processes are also required to remove access rights when individuals no longer require access.

We looked at how CFMWS determines who needs access to its various databases and to what specific information within those systems. We also examined the administrative processes and procedures in place for ongoing management of this access.

The audit found that CFMWS has processes and procedures to grant, remove and manage access to their systems and that both the *need-to-know* and *least privilege* principles are enforced. As per CFMWS IS Security Orders, it is expected that a person is granted access to only that information for which appropriate access authorization(s) and an established *need-to-know* are approved. Access is to be only granted to those resources necessary to perform the assigned task. Controlled access is normally achieved through a combination of technical, physical and/or procedural means. Employees are granted access based on their position.

Should the employee change position, the access level is modified to reflect the requirements of the new position or removed in the event that the individual leaves or goes on extended leave.

The audit team was informed that managers determine appropriate access controls, rules, access rights and restrictions for specific user roles and conduct periodic reviews of all access rights to confirm that these rights are still appropriate. The scope of this audit did not include the testing of manager review and approval of access rights.

2.13 Monitoring

Section 6.2.21 of the TBS *Directive on Privacy Practices* requires government institutions to adopt appropriate measures to ensure that access, use and disclosure of personal information are monitored and documented, so that inappropriate or unauthorized activity in this regard can be identified and rectified in a timely fashion.

Logging and monitoring user activity is crucial to determining whether access rights have been appropriately exercised. Without full activity logging of access and changes to data residing in the various CFMWS databases, personal information may be inappropriately accessed, used or disclosed with no means of detection.

Overall, CFMWS has controls in place to safeguard personal information under its control from unauthorized use and disclosure by external forces. IT monitors the network 24/7 to detect any unauthorized access to its IT systems. Cybersecurity events or incidents are identified and dealt with promptly so as to minimize the impact, and corrective measures are implemented to minimize the probability and impact of similar events and incidents.

User activity on CFMWS' systems is recorded. A record is created and logged when users log in, create, modify or delete files in any of the networks. However, not all logs are actively monitored to ensure the timely identification of inappropriate or unauthorized access to or disclosure of, personal information that is accessible to internal users. CFMWS would benefit from monitoring internal audit logs and records on a regular basis to identify any indications of possible inappropriate access, use or disclosure and for attempts to defeat security protocols.

ADM(RS) Recommendation

6. It is recommended that CFMWS implement an audit log review tool to aid in the investigation of unauthorized access, use or disclosure by internal users.

Functional OPI: CCS
Technical OPI: CIO
Action OPIs: All Divisions

2.14 Privacy Breach Protocol

TBS has issued *Guidelines for Privacy Breaches* to help institutions avoid instances of improper or unauthorized access to or disclosure of personal information, and to mitigate the consequences of a breach should one occur.

A comprehensive approach to privacy breach reporting can help institutions better manage privacy risks, allowing them to adjust their business operations based on lessons learned. The TBS-issued *Guidelines for Privacy Breaches* require institutions to establish plans and procedures for addressing privacy breaches.

CFMWS' *Guidelines for Privacy Breaches* set out the process by which it responds to breaches of personal information. The document provides measures to guide staff in their responsibilities and appropriate action in case of a breach. The ATIP section is responsible for investigating and managing the life cycle of a privacy breach and notifying TBS and the OPC when required.

The audit team reviewed documentation from the NM ATIP on their response to several privacy breaches in recent years. The audit found that the TBS and the CFMWS *Guidelines for Privacy Breach*es had been followed by the NM ATIP in documenting the nature of the breach and in notifying TBS and the OPC, when required.

3.0 General Conclusion

A privacy breach, whether intentional or inadvertent, can be devastating to an organization and its victims. Risks to an individual in the event of a breach may include reputational harm, financial harm and, in some cases, personal prejudice or prosecution. For an organization, a breach may result in embarrassment, loss of credibility and a decrease in public confidence.

The audit found that CFMWS is aware of protection of personal information as an important consideration in program delivery and business activities. Since its inception in April 2017, CFMWS' ATIP program has developed a Privacy Management Framework that establishes accountabilities and policies for the handling of personal information in compliance with the *Privacy Act* and the relevant TB policies and directives.

The audit noted a number of examples of positive privacy practices. These include a comprehensive privacy management program; established standards and practice for the handling of personal information; incident response procedures to address privacy breaches; and a process to ensure that a PIA is conducted for any new or substantially modified programs that involve the collection and retention or personal information. The responsibilities and accountabilities of ATIP and security staff are coordinated and collaborative. CFMWS has developed administrative, physical and technical safeguards to limit inappropriate access to personal information.

However, more work is needed to ensure that divisions have assessed privacy risks within their programs to ensure the safeguarding of personal information in a manner commensurate with its sensitivity. Improvements to controls, procedures and practices such as privacy awareness training, developing SOPs, oversight when personal information is transferred to third parties, monitoring internal access to CFMWS databases for inappropriate activities and disposing of outdated information from databases would improve the security of personal information under CFMWS's control.

Annex A — Management Action Plan

Roles and Responsibilities

ADM(RS) Recommendation

1. It is recommended that CFMWS establish privacy responsibilities for divisions and program personnel to ensure clear accountabilities for privacy responsibilities.

Management Action

Action 1.1: CFMWS will develop privacy responsibilities and accountabilities for divisions and program personnel.

OPI: CCS

OCI: All Divisions

Target Date: April 2023

Action 1.2: The ATIP Section is established with one person. With the growing privacy risk, and the large number of CFMWS initiatives and programs, the demand for Privacy services has exceeded the capacity of one individual. CFMWS will request Pubic funding for additional ATIP resources as required.

OPI: CCS

Target Date: April 2023

Risk Assessment

ADM(RS) Recommendation

2. It is recommended that CFMWS regularly identify privacy risks to on-going operations and ensure controls are in place to mitigate these risks.

Management Action

Action 2.1 CFMWS will establish procedures for business lines to review ongoing operations to identify privacy risks.

OPI: CCS

OCI: COO

Target Date: N/A – Ongoing process.

Action 2.2 CFMWS will implement reviews of privacy risk in ongoing operations and implement risk mitigation controls, as required.

OPI: CCS

OCI: COO, All Divisions

Target Date: N/A – Ongoing process.

Training and Awareness

ADM(RS) Recommendation

3. It is recommended that CFMWS expand its current privacy awareness and training program with specific training requirements for employees most actively involved in the handling of personal information and ensure that SOPs are in place for all CFMWS' personal information data holdings.

Action 3.1 CFMWS will initiate development of a CFMWS/NPP-specific training course for the employees most actively involved in personal information handling, and issue direction to all units to ensure that they autonomously develop SOPs for all CFMWS' personal information data holdings. Incremental public funding will likely be required for course development

OPI: CCS

OCI: CHRO, All Divisions

Target Date: April 2024

Information-Sharing Agreements with Third Party Service Providers

ADM(RS) Recommendation

4. It is recommended that CFMWS maintain an up-to-date inventory of business arrangements where personal information is transferred to a third party, and obtain

assurances that the data handling practices of their partners are consistent with the terms of its information-sharing agreements.

Action 4.1 CFMWS will create and maintain an inventory of business arrangements where personal information is transferred to a third party.

OPI: COO, CCS

OCI: CIO, Division Heads

Target Date: October 2023

Action 4.2 CFMWS will investigate methods of obtaining assurances in future contracts involving 3rd party data handling practices, and implement those that are the most reasonable and appropriate.

OPI: CCS

Target Date: April 2024

Limiting Disposal

ADM(RS) Recommendation

5. It is recommended that CFMWS dispose of the required data from its databases so that it follows best *Privacy Act* practices.

Action 5.1 CFMWS will investigate and implement changes to IT systems to add the capability to dispose of personal data that is no longer required from its databases.

Functional OPI: COO

Technical OPI: CIO

Database OPIs: SISIP and CFOne

Target Date: April 2023

Action 5.2 CFMWS will establish and implement procedures to routinely dispose of personal data that is no longer required from its databases.

Functional OPI: COO

Technical OPI: CIO

Database OPIs: SISIP and CFOne

Target Date: April 2023

Monitoring

ADM(RS) Recommendation

6. It is recommended that CFMWS implement an audit log review tool to aid in the investigation of unauthorized access, use or disclosure by internal users.

Action 6.1 CFMWS will investigate audit log review tools and implement based on affordability and effectiveness.

Functional OPI: CCS

Technical OPI: CIO

Action OPIs: All Divisions to utilize

Target Date: October 2023

Action 6.2 CFMWS will develop and implement procedures for regular review of access logs.

Functional OPI: CCS

Technical OPI: CIO

Action OPIs: All Divisions to utilize

Target Date: October 2023

Annex B — About the Audit

Objective

The objective of this audit is to assess CFMWS' Privacy Management Framework and determine whether the policies, procedures and practices for managing personal information comply with the *Privacy Act* and its supporting TB policies and directives.

Audit Criteria[1]

Governance: To provide reasonable assurance that policies, practices and procedures are in place to effectively manage and protect personal information in accordance with the requirements of the *Privacy Act* and its supporting policies and directives, and that privacy roles are clearly defined, formally approved and communicated.

Risk Management: To provide reasonable assurance that CFMWS identifies and analyzes privacy risks as a basis for determining how the risks should be managed to ensure compliance with the *Privacy Act* and its supporting policies and directives and includes a robust training and awareness program.

Controls: To provide reasonable assurance that CFMWS has implemented control activities to help ensure compliance with the *Privacy Act* and its supporting policies and directives.

Scope

The scope of this audit included the privacy management responsibilities of the Corporate Services Division/NM ATIP and the privacy practices in place to govern the collection of personal information collected through the CFOne Membership Program and the Service Income Security Insurance Plan (SISIP).

The audit examined the design of CFMWS' privacy management practices, as measured against the requirements of the *Privacy Act* and its supporting policy and directives. The focus was on the documented policies, procedures and standards in place for collecting, using, disclosing, storing and disposing of personal information. The audit also looked at how the information is safeguarded.

The scope included activities carried out from April 1, 2017 to December 31, 2021 but focused on current practices.

The audit work was conducted between October 2020 and January 2022.

[1]**Sources of Criteria.** *Privacy Act, TB Policy on Privacy Protection, TB Directive on Privacy Practices, TB Directive on Privacy Impact Assessments, Policy on Governance Security.*

The scope did not include an assessment of the accuracy and completeness of data collected, nor did it include the design and effectiveness of key control areas of the existing IT security environment, as this was looked at as part of the April 2019 Audit of IT Security.

Due to restrictions imposed by the current pandemic, the audit team was unable to examine the day-to-day operations of staff most actively engaged in the handling of personal information, nor was the team able to conduct physical inspections.

Methodology

The audit approach included a review of applicable legislation and policy documents; a review of key supporting documents and relevant background documentation; and interviews with key CFMWS personnel in Ottawa.

Statement of Conformance

The findings and conclusions contained in this report are based on sufficient and appropriate evidence gathered in accordance with procedures that meet the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing*. The audit thus conforms to the Institute of Internal Auditors' *International Standards for the Professional Practice of Internal Auditing* as supported by the results of the quality assurance and improvement program. The opinions expressed in this report are based on conditions as they existed at the time of the audit and apply only to the entities examined.

Annex C— SISIP and CFOne Membership Program

SISIP

In 1969, SISIP was established to manage the Service Income Security Insurance Plan that provided government-paid coverage under group life and disability policies to CAF and DND members.

Over time, SISIP has expanded its range of services and products offered through 24 offices across the country to address the financial needs of members, reservists, retirees and their families. With the vision that "[e]very member of the CAF community and their families has financial health and security," the expanded offerings include access to:

- Government and member-paid group life and group disability policies
- Home, Auto, Travel and Critical Illness insurance
- Personal and Business Banking
- Investments held through RRSP, TFSA, RESP, Non-registered accounts, CAF Savings Plans and Registered Disability Savings Plans

Services include:

- Financial Advice
- Financial Counselling and Debt Counselling

CFOne membership

CFOne membership provides access to a variety of programs and services administered through CFMWS. The card easily and accurately confirms membership within the Canadian military community.

The CFOne membership provides access to the CANEX rewards/loyalty program, CANEX Members Only pricing, the CF Appreciation Program, and financial affinity programs including BMO Defence Banking and The Personal Insurance. Targeted programs for members include the Vacations for Veterans Program, the Support Our Troops Summer Camp Program and the Support Our Troops Scholarship Program.

The CFOne membership card is used to validate eligibility for various programs such as SISIP, PSP recreation, messes and military family access to MAPLE virtual doctors.

Eligibility for CFOne membership is open to CAF members (Regular and Reserve Force), RCMP, Coast Guard, veterans, retirees of these organizations and members of foreign military

currently serving with the CAF and their families. Staff of DND and many organizations affiliated with DND are eligible for membership along with their families.