Policy on Privacy Practices

DATE OF ISSUE: September 2017
REVISION DATE: N/A

APPLICATION

1. This is an order that applies to members of the Canadian Armed Forces and a directive that applies to employees of the Department of National Defence (DND) and to the Staff of the Non-Public Funds (NPF), Canadian Forces (CF) involved in the administration and delivery of Non-Public Property (NPP) activities, services and programs.

2. For greater certainty, this includes all non-public property vested in the commanders of units and other elements, and in the Chief of the Defence Staff (CDS) established under sections 38 to 41 of the *National Defence Act*; all activities of the Staff of the NPF, CF; and all non-public property services, programs and operations including the public Alternative Service Delivery functions assigned to be executed under the NPP accountability framework.

APPROVAL AUTHORITY

3. This policy is issued under the authority of the Director General Morale Welfare Services (DGMWS), in his capacity as the Managing Director NPP and Chief Executive Officer (CEO), Staff of the NPF, CF.

ENQUIRIES

4. Enquiries should be directed to the Canadian Forces Morale and Welfare Services (CFMWS) National Manager Access to Information and Privacy Program (NM ATIP).

DEFINITIONS

5. See Annex A: Definitions.

POLICY OBJECTIVE

6. The objective of this policy is to establish consistent practices and procedures to ensure that personal information is protected and effectively managed by identifying and mitigating privacy risks in accordance with the requirements of the *Privacy Act* (the Act), Regulations, and related Treasury Board Secretariat (TBS) policies, directives, standard and guidelines.

7. Non-compliance with the Act may result in complaints and investigations by the Office of the Privacy Commissioner of Canada as well as reviews by the Federal Court. A privacy breach may cause injury or harm to affected individuals and also affect the achievement of the organization's objectives.

AUTHORITIES, ROLES AND RESPONSIBILITIES

8. Pursuant to section 73 of the Act, the Minister of National Defence, as the head of the government institution, has designated the following positions within the CFMWS to exercise all his powers, duties and functions under the Act concerning NPP services, programs and operations:

a. Managing Director NPP/ CEO of the Staff of the NPF, CF;

b. Chief of Staff/Vice-President Corporate Services (COS/ VP CorpSvcs); and

c. NM ATIP.

9. **CFMWS VP CorpSvcs** oversees the administration of the CFMWS ATIP Program and reports on the state of privacy management within NPP entities at the Executive Management Board (ExMB) on an annual basis.

10. **CFMWS NM ATIP** is responsible for:

a. providing privacy advice and guidance as well as training and awareness to the managers and staff involved in NPP programs and services;

b. determining the need and conducting a privacy impact assessment (PIA) when warranted, and creating or modifying a personal information bank (PIB), in collaboration with program managers;

c. ensuring stakeholders review of the PIA in a timely manner, and endorsing and co-signing the completed PIA, as the delegate responsible for section 10 of the Act;

d. submitting to TBS for registration and approval any new or revised PIB, along with the approved PIA that has been sent to the Office of the Privacy Commissioner (OPC), at least 60 days before the implementation of the new or substantially modified NPP program or activity;

e. ensuring that sections I and II of completed PIAs are published on the CFMWS Web site, within three months following the approval of the PIA;

f. working in close collaboration with the offices of primary interest (OPIs), and the CFMWS Unit Security Supervisor as required, in the management and resolution of privacy breaches in accordance with the CFMWS Privacy breach protocol;

g. monitoring the implementation of the action plans developed by CFMWS divisions to address the privacy issues and risks identified in PIAs, or as a result of a privacy breach;

h. making decisions regarding the disclosure of personal information pursuant to subsection 8(2)(e), (j) and (m) of the Act. See Annex B: Guidelines for the disclosure of personal information pursuant to subsection 8(2) of the *Privacy Act*;

i. notifying the OPC in a timely manner of any planned initiative or issue that may relate to the Act or any of its provisions or that may have an impact on the privacy of Canadians (e.g. "material" privacy breaches, completed PIAs, new consistent uses of personal information, and disclosure in the public interest); and

j. maintaining an up-to-date inventory of all current NPP personal information sharing agreements.

11. **CFMWS Division Heads**, in their capacity as NPP functional authorities, are responsible for:

a. ensuring that privacy practices within their areas of responsibilities are consistent with and respect the provisions of the Act, Regulations and other applicable legislation;

b. Approving and co-signing the PIA completed for their division and ensuring that the PIA is provided to the OPC by the NM ATIP, along with any additional documentation that may be required by that office, at least 60 days before the implementation of a new or substantially modified NPP program or activity involving personal information;

c. ensuring that an action plan is developed and implemented in a timely manner to address privacy risks identified in the PIA, or as a result of a privacy breach; and

d. informing employees of the legal and administrative consequences of any inappropriate or unauthorized access to, or use, disclosure, modification, retention and disposal of, personal information related to a particular NPP program or activity.

12. **Managers** and, where applicable, **staff** involved in the management or delivery of programs,

activities and services under the NPP accountability framework are responsible for:

a. complying with the requirements set out in sections 4 to 8 of the *Privacy Act*, the Regulations, and section 6.2 of the TBS Directive on Privacy Practices regarding the creation, collection, notification and consent, accuracy, use and disclosure, safeguards, retention and disposal of personal information, as well as the TBS Directive on Social Insurance Number (SIN) regarding the restrictions limiting the collection and use of this identifying number;

b. prior to disclosing personal information in response to a request from a NPP client, ensuring that the individual has adequately identified himself or herself as the individual to whom the information pertains, or as the person authorized in writing by the individual or authorized by law to administer the affairs of the individual;

   Note: *Where a rigorous verification of identity is necessary, the individual may be required to be present when the information is disclosed. If there is any doubt concerning the identity of the person seeking access, disclosure must not take place;*

c. safeguarding and not disclosing personal information without the consent of the individual to whom it relates, except in accordance with section 8 of the Act and Annex B: Guidelines for the disclosure of personal information pursuant to subsection 8(2) of the *Privacy Act*;

d. promptly reporting and managing any suspected or actual breach of privacy, in accordance with the CFMWS Privacy breach protocol;

e. consulting the CFMWS NM ATIP in the following circumstances:

   i. in the early stages of the planning of any new or substantially modified NPP program or activity involving personal information to determine whether a PIA is warranted;

   ii. when creating or revising a form requiring the collection of personal information, for a compliance review and the inclusion of the appropriate privacy notice and consent statement, as required;

   iii. prior to any new use or disclosure consistent with the purpose for which the personal information was originally obtained or compiled, but is not currently described in a PIB, or for a purpose that was not originally intended;

   iv. when preparing information sharing agreements involving personal information with public sector organizations, to ensure that appropriate privacy protection provisions are included therein, in accordance with the requirements of the Act and the TBS Guidance on Preparing Information Sharing Agreements Involving Personal Information;

f. collaborating with the CFMWS NM ATIP in the development of a PIA and the creation or modification of a PIB, and providing in a timely manner necessary documentation and evidence;

g. developing and implementing an action plan to address any privacy risks identified in the PIA, or as a result of a privacy breach, and providing a status update to the CFMWS NM ATIP, as required; and

h. depositing a copy of all current personal information sharing agreements with the CFMWS NM ATIP.

13. **CFMWS Chief Information Officer** ensures that:

a. as part of any security assessment of IM/IT solutions involving personal information, that the CFMWS NM ATIP has been consulted to determine whether a PIA is warranted. If a PIA is required, and has not been completed prior to granting an Authority to Operate, the corresponding Letter of Authorization must contain a mandatory condition requiring the submission of a completed PIA within acceptable timelines; and

b. the NPPNet is compliant with the requirements of the *Privacy Act* and the related TBS policies and directives, including the *Standard on Privacy and Web Analytics* and also the terms and conditions for privacy notices in Appendix C of the *Standard on Web Usability*.

14. **CFMWS Unit Security Supervisor** works in close collaboration with the CFMWS NM ATIP to ensure the timely reporting of, intervention in, and investigation into suspected or actual breaches of privacy related to NPP activities, in accordance with the CFMWS Privacy breach protocol.
15. **NPP Contracting authorities** must consult the CFMWS NM ATIP when a proposed NPP procurement involves personal information, to ensure that appropriate privacy protection clauses are included in contracting documents, in accordance with the requirements of the Act and the TBS Guidance Document: Taking Privacy into Account Before Making Contracting Decisions.

MONITORING AND CONSEQUENCES

16. The CFMWS NM ATIP monitors compliance with the Treasury Board Secretariat (TBS) policies, directives, standard and guidelines related to the administration of the *Privacy Act* within NPP organizations.
17. Privacy breaches caused by the culmination of inappropriate information-management practices may result in disciplinary action, up to and including termination of employment.

REFERENCES

Acts and regulations:

a. Access to Information Act

b. Privacy Act

c. Access to Information Regulations

d. Privacy Regulations

Treasury Board publications:

a. Policy on Privacy Protection
b. Directive on Privacy Impact Assessment
c. Directive on Privacy Practices
d. Directive on Social Insurance Number
e. Guidance Document: Taking Privacy into Account Before Making Contracting Decisions
f. Guidance on Preparing Information Sharing Agreements Involving Personal Information
g. Guidelines for Privacy Breaches
h. Info Source
i. Standard on Privacy and Web Analytics

CFMWS policies:

a. Policy on the Access to Information and Privacy (ATIP) Program

b. Privacy Breach Protocol
c. Protocol for non-administrative uses of personal information (*under development*)
d. CFMWS Non-Public Property Functional Authority Policy
e. Non-Public Property (NPP) Network (NPP Net) Privacy Policy

ANNEXES

Annex A: Definitions

Annex B: Guidelines for the disclosure of personal information pursuant to subsection 8(2) of the *Privacy Act*

ANNEX A: DEFINITIONS

Administrative purpose: Use of personal information about an individual in a decision-making process that directly affects that individual. This includes all uses of personal information for confirming identity (i.e., authentication and verification purposes) and for determining eligibility of individuals for government programs.

Consistent use: Use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.

Data matching: An activity that involves comparing personal data obtained from a different source within the same government institution, for administrative or non-administrative purposes. The data-matching activity that is established can be systematic or recurring. The data-matching activity can also be conducted on a periodic basis when deemed necessary. Under the TBS Policy on Privacy Protection, data matching includes the disclosure or sharing of personal information with another organization for data-matching purposes.

Delegate: An officer or employee of a government institution who has been delegated to exercise or perform the powers, duties and functions of the head of the institution under the Act.

Disclosure: Release of personal information by any method (e.g., transmission, provision of a copy, examination of a record) to any body or person.

Government institution: For the purposes of the *Access to Information Act* and the *Privacy Act*, any department, ministry of state, body, or office listed in Schedule I of the Acts as well as any parent Crown corporation and wholly-owned subsidiary of a Crown corporation within the meaning of section 83 of the *Financial Administration Act*. These institutions must respect and fulfill all responsibilities provided for in the Acts.

Head of government institution: For the purpose of the *Access to Information Act* and the *Privacy Act*, in the case of a department or ministry of state, the head of the government institution is the minister. In other cases, the head of the institution is the person designated by an Order in Council or, if no such person is designated, the chief executive officer of the institution, whatever their specific title. The head, or their delegate(s), is responsible for exercising all powers, duties and functions related to the application of the *Access to Information Act* and the *Privacy Act* within their institution. For NPP entities, the Minister of National Defence is the head of the institution.

Info Source: A series of annual TBS publications aimed at the public that contain clear and detailed information on government institutions, their program responsibilities and their information holdings, for the purpose of assisting members of the public in exercising their right of access under the Act. *Info Source* publications also provide contact information for government institutions as well as summaries of court cases and statistics on access to information and privacy requests.

Need-to-know: The restriction of access to protected or classified information to individuals who need to access and know the information in order to perform their duties.

New consistent use: Consistent use that was not originally identified in the appropriate personal information bank (PIB) described in the *Info Source*.

Non-administrative purpose: Use of personal information for a purpose that is not related to any decision-making process that directly affects the individual. This includes the use of personal information for research, statistic analysis, audit, and evaluation purposes.

Non-Public Property: NPP is defined in section 2 of the *National Defence Act* (NDA) and includes all money and property received for or administered by or through NPP organizations, and all money and property contributed to or by CAF members for their collective benefit and welfare.

NPP Functional Authorities: Subject matter experts who are responsible for the various CFMWS NPP functions.

Original purpose: Purpose that was first identified when initiating the collection of personal information and that is directly related to an operating program or activity of the institution. A purpose that is not consistent with the original purpose is considered to be a secondary purpose.

Personal Information: Information that is about an identifiable individual and recorded in any form, as defined in section 3 of the *Privacy Act*. Examples include information relating to race, nationality, ethnic origin, religion, age, marital status, address, education as well as the medical, criminal, financial or employment histories of an individual. Personal information also includes any identifying number or symbol, such as the social insurance number, assigned to an individual.

Personal information Bank (PIB): Description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the PIB has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.

Privacy: An individual's right to be left alone and to be free of unwarranted intrusions. It is also the right of an individual to retain control over his or her personal information and to know the uses, disclosures and whereabouts of that information.

Privacy breach: The improper or unauthorized creation, collection, access, use, disclosure, retention and/or disposal of personal information. A privacy breach may occur within an institution or off-site and may be the result of inadvertent errors or malicious actions by employees, third parties, partners in information-sharing agreements or intruders.

Privacy Commissioner of Canada: An Officer of Parliament who investigates complaints from individuals regarding the handling of personal information by federal government institutions. In addition, the Commissioner has the authority to conduct compliance reviews of the privacy practices of government institutions as the practices relate to the collection, retention, accuracy, use, disclosure and disposal of personal information by government institutions subject to the Act. The Commissioner has the powers of an ombudsman and can make recommendations with respect to any matter which has been investigated or reviewed. In addition, the Commissioner can report on institutional activities in annual or special reports to Parliament.

Privacy impact assessment (PIA): Policy process for identifying, assessing, and mitigating privacy risks. Government institutions are required to develop and maintain PIAs for all new or modified programs and activities that involve the use of personal information for an administrative purpose.

Privacy notice: Verbal or written notice informing an individual of the purpose of a collection of personal information and of the government institution's authority for collecting it, including creating, using and disclosing information. The notice, which must reference the PIB described in *Info Source*, also informs the individual of his or her right to access, and request the correction of, the personal information and of the consequences of refusing to provide the information requested.

Privacy practices: All practices related to the creation, collection, retention, accuracy, correction, use, disclosure, retention and disposal of personal information.

Privacy protocol: Set of documented procedures to be followed when using personal information for non-administrative purposes, including research, statistics, audit, and evaluation. These procedures ensure that the individual's personal information is handled in a manner that is consistent with the principles of the Act.

Web analytics: The collection, analysis, measurement and reporting of data about Web traffic and use visits for the purpose of understanding and optimizing Web usage.

ANNEX B: GUIDELINES FOR THE DISCLOSURE OF PERSONAL INFORMATION PURSUANT TO SUBSECTION 8(2) OF THE *PRIVACY ACT*

These guidelines identify the authorities to make discretionary disclosure decisions, clarify the circumstances under which personal information managed under the NPP accountability framework may be disclosed, without the consent of the individual to whom it relates, pursuant to subsection 8(2) of the *Privacy Act* and also clarify the retention requirements in this regard.

1. GUIDELINES

Subsection 8(2) of the Act describes the different circumstances under which personal information under the control of a government institution may be disclosed without the consent of the individual to whom the information pertains. Such disclosures are discretionary and are subject to the provisions of any other Act of Parliament.

Subsection 8(2) does not take precedence over specific statutory prohibitions, and **only applies where no other statutory provision exists**. Therefore, where another federal statute forbids the disclosure of personal information (e.g., section 241 of the *Income Tax Act*), the personal information cannot be disclosed by the institution.

Disclosures under subsection 8(2) should be limited to the information requested and no more than is necessary to fulfill the purpose for which it will be used. Moreover, only relevant information pertaining to the individual identified in the request may be released; **any information about other individuals should be severed from the record prior to disclosure**.

Pursuant to subsection 9(1) of the Act, when personal information is disclosed for a use or purpose not included in the relevant Personal Information Bank (PIB), a record of the use or disclosure shall be attached to the personal information and should include the following:

- the name and title of the person authorizing the use or disclosure;
- the name of the institution, person, organization or body receiving the information;
- a description of the use or purpose of disclosure; and,
- a copy of the information disclosed, or a description in sufficient detail to allow a determination of exactly what information was used or disclosed.

Additional guidelines concerning the disclosure of personal information pursuant to specific paragraphs of subsection 8(2) of the Act follow. Managers should consult with the CFMWS NM ATIP for guidance, or if they would like an informal review of the records prior to making a disclosure.

***Note**: These guidelines do not apply to routine disclosures made under subsection 8(2) of the Act, as these should be governed by personal information sharing agreements and also described in the relevant PIBs. Consult the CFMWS NM ATIP if these instruments are not already in place.*

2. APPLICATION

Paragraph 8(2)(*a*) - Original purpose or consistent use

Managers and designated staff may disclose personal information for the purpose for which the information was obtained or compiled by the program, or for a use consistent with that purpose, as described in the relevant personal information bank (PIB) described in the Info Source.

If the relevant PIB does not clearly describe the original purpose or consistent uses, or if no PIB exists, employees should consult the CFMWS NM ATIP prior to disclosing personal information.

Paragraph 8(2)(*b*) - Act of Parliament or Regulation

Managers and designated staff may disclose personal information for any purpose, in accordance with any *Act* of Parliament or any regulations made there under that authorizes its disclosure. For example, the *Auditor General Act* specifically authorizes departments to disclose information to the Auditor General or a member of his or her office.

If the legal authority to disclosure personal information is not clearly identified, or for any request received under the *Security of Canada Information Sharing Act* (SCISA), managers must consult the CFMWS NM ATIP prior to responding. It is possible that the legal authority of another organization to request information or require the production of information may not constitute an authority to disclose personal information under this provision.

Paragraph 8(2)(*c*) - Subpoenas, Warrants, Court orders and Rules of court

Warrants or subpoenas are usually served in the location where the records are held or on persons who are thought to hold the requested records. Sometimes parties to a civil proceeding will serve a notice to produce, a similar order or summons on a public servant, requiring him/her to appear at a pre-trial examination and to bring certain documents. These documents should be carefully scrutinized by the Legal Services, to verify the validity of the warrants, subpoenas, court orders and notices for the production of information, and to determine the proper form of compliance.

In some cases, it may be appropriate to ask the courts for permission to sever from the records, certain sensitive information that is not relevant to the issue before the court. In exceptional circumstances, section 37 of the *Canada Evidence Act* allows a government official to ask the court not to disclose even relevant information.

Paragraph 8(2)(*d*) - Attorney General

Managers and designated staff may disclose personal information to the Attorney General for use in legal proceedings involving the Crown, in consultation with Legal Services.

Paragraph 8(2)(*e*) - Federal investigative bodies

Requests from federal investigative bodies (specified in Schedule II of the *Privacy Regulations*) for personal information, along with the responsive records and/or recommendations, if applicable, must be immediately forwarded to the CFMWS NM ATIP who is responsible for making decisions under this provision.

Personal information may only be disclosed to aid in a specific, lawful enforcement or investigative activity and should not be disclosed in relation to a vague inquiry.

Pursuant to subsection 8(4) of the *Privacy Act* and section 7 of the *Privacy Regulations*, the CFMWS NM ATIP shall retain these records for a minimum of two years, and make them available to the Privacy Commissioner, upon request.

Paragraph 8(2)(*f*) - Provinces, foreign states and international bodies

Paragraph 8(2)(*f*) of the Act allows for the disclosure of personal information to a province or foreign state for purposes of administering or enforcing any law or carrying out a lawful investigation as long as there is an agreement or arrangement in place.

The Minister of Justice and Attorney General of Canada entered into umbrella agreements with all of the provinces and the Yukon, with the exception of the North West Territories, when the *Privacy Act* was proclaimed in force in 1983. It should be noted that these 8(2)(*f*) umbrella agreements only authorize federal institutions to disclose personal information in response to one-time or infrequent requests for disclosure from a provincial institution (defined in each of the said agreements).

There are a number of requirements to be considered in allowing paragraph 8(2)(*f*) disclosures:

- disclosure may only be done at the written request of the other jurisdiction;
- the request must specify the personal information being requested and the purpose for which it will be used, and the purpose must relate to the administration of an act or for law enforcement (not in relation to a vague inquiry);
- these are one-way disclosures from the federal institution to the other jurisdiction and the agreements do not encompass exchanges of information from the other jurisdictions back to the federal institution; and,
- the institution may, but is not obliged to disclose the requested information, as paragraph 8(2)(*f*) is discretionary.

Furthermore, as some Charter issues may arise from the use of this section, a subpoena, warrant or Court order may be required prior to disclosing personal information to a provincial organisation.

Managers should therefore consult the CFMWS NM ATIP prior to disclosing personal information to a province, foreign state or international body under this paragraph.

Paragraph 8(2)(*g*) - Member of Parliament

Managers and designated staff may disclose personal information to a Member of Parliament (MP - includes both members of the House of Commons and the Senate) for the purpose of assisting the individual to whom the information relates in resolving a problem. Only the specific information required for the resolution of the problem may be disclosed under this provision.

It should be noted that once Parliament has been dissolved prior to an election, and until a new MP is sworn in, this provision may not be applied. Once an MP has resigned, personal information may be provided to the former MP only with the express consent of the individual.

Paragraph 8(2)(*h*) - Audit purposes

Managers and designated staff may disclose personal information to officers or employees of the National Defence Assistant Deputy Minister (Review Services) and CFMWS Compliance and Assurance Section for internal audit purposes only and not as part of any decision-making process concerning the individual to whom the information relates.

Paragraph 8(2)(*i*) - Archival purposes

Staff responsible for the retention and disposal of files are authorized to forward files that contain personal information to the Library and Archives Canada and Federal Records Centres located across the country for storage and disposal, in accordance with the retention and disposal schedules.

Paragraphs 8(2)(*j*) - Research or statistical purposes

Requests for the disclosure of personal information for research or statistical purposes should be forwarded to the CFMWS NM ATIP, as only a delegate under the *Privacy Act* can make decisions under this provision.

Paragraph 8(2)(k) - Native claims research

Managers should consult the CFMWS NM ATIP for an invasion-of-privacy test prior to disclosing personal information for the purpose of researching or validating the claims, disputes or grievances of any of the aboriginal peoples of Canada.

Paragraph 8(2)(*l*) - Payment of a benefit and collection of a debt

Managers and designated staff may disclose personal information to any government institution for the purpose of locating an individual in order to collect a debt owing to the Crown or to make a payment owing to the individual by the Crown.

The scope of this provision is rather limited. It aims to more easily find individuals who have a debt to the Crown and to more easily disburse federal benefits. It is important to understand that it does not permit the disclosure of personal information to determine if the individual is a debtor or not, nor does it authorize the disclosure of more information than is necessary to recover money from the individual. Thus, only the information necessary to locate the individual may be communicated under this provision.

Paragraph 8(2)(*m*) - Public interest

Requests for the disclosure of personal information in the public interest should be forwarded to the CFMWS NM ATIP, as only a delegate under the *Privacy Act* may make a discretionary decision under this provision, for any purpose where (i) the public interest in disclosure clearly outweighs any invasion of privacy that could result from the disclosure, or (ii) disclosure would clearly benefit the individual to whom the information relates:

The CFMWS NM ATIP will conduct an invasion-of-privacy test, prior to making a disclosure of personal information in the public interest