Treasury Board of Canada Secretariat
Secrétariat du Conseil du Trésor du Canada
Canada

Directive on Privacy Impact Assessment

Published: Apr 01, 2010

Published by Treasury Board of Canada, Secretariat
90 Elgin, Ottawa, Ontario, K1A 0R5, Canada

Catalogue Number: BT39-9/2010E-PDF
ISBN: 978-0-660-09671-1

This document is available on the Government of Canada website, Canada.ca

This document is available in alternative formats upon request.

Aussi offert en français sous le titre : Directive sur l'évaluation des facteurs relatifs à la vie privée

Directive on Privacy Impact Assessment

1. Effective date

1.1 This directive takes effect on April 1, 2010.

1.2 This directive replaces the following:

- *Privacy Impact Assessment Policy*, dated May 2, 2002; and
- Data matching components of the *Privacy and Data Protection Policy* (1993).

1.3 Government institutions will have until September 1, 2010, to implement the requirements of this directive except for those described in Subsections 6.3.9, 6.3.10, 6.3.11, 6.3.16, 6.3.17 and Appendix C, which institutions will have until April 1, 2011, to implement.

2. Application

2.1 This directive applies to government institutions as defined in section 3 of the *Privacy Act*, including parent Crown corporations and any wholly owned subsidiary of these corporations.

2.2 This directive does not apply to the Bank of Canada.

2.3 Appendix B contains additional requirements for "departments," as defined in section 2 of the *Financial Administration Act* (FAA) and referenced in subsection 71(5) of the *Privacy Act*.

2.4 The directive does not apply to the development of new legislation.

3. Context

3.1 The Government of Canada is committed to ensuring that privacy protection is a core consideration in the initial framing and subsequent administration of programs and activities involving personal information. In recent years, Canadians and parliamentarians have been concerned with the complex and sensitive privacy issues that stem from proactive anti-terrorism measures, use of surveillance and privacy-intrusive technology, sharing of personal information across borders and threats to privacy posed by security breaches. Canadians want to be informed of how their personal information is handled and assured of its protection.

3.2 Under the *Privacy Act*, a collection or grouping of personal information is referred to as a personal information bank (PIB). Under the *Privacy Act*, heads of government institutions are required to identify, describe and publicly report their PIBs. The President of the Treasury Board, as designated Minister, holds general responsibility for registering all PIBs and reviewing the manner in which they are maintained and managed in all government institutions defined in section 3 of the *Privacy Act*. In addition to this general oversight role, the President of the Treasury Board is responsible for reviewing and approving new or substantially modified PIBs or establishing the terms and conditions for such approval for the departments defined in section 2 of the *Financial Administration Act* (FAA). Under subsection 71(6) of the *Privacy Act*, the President of the Treasury Board may choose to delegate this authority to the departments defined in section 2 of the FAA. In making this determination, the President of the Treasury Board will consider a department's compliance with the *Policy on Privacy Protection*, with this and other directives as well as with any prescribed forms. The delegation for review and approval of PIBs can only be given to the departments defined in section 2 of the FAA. Regardless of any such delegation, the President of the Treasury Board remains responsible for the ongoing review of PIBs for all government institutions that are subject to the *Privacy Act*.

3.3 The *Directive on Privacy Impact Assessment* (PIA) supports the President of the Treasury Board's responsibilities by ensuring that privacy implications will be appropriately identified, assessed and resolved before a new or substantially modified program or activity involving personal information is implemented. Government institutions routinely perform broad risk management activities and develop risk profiles related to their programs and activities. The PIA is the component of risk management that focuses on ensuring compliance with the *Privacy Act* requirements and assessing the privacy implications of new or substantially modified programs and activities involving personal information. However, if not properly framed within an institution's broader risk management framework, conducting a PIA can be a resource-intensive exercise. As such, the government is committed to ensuring that a PIA is conducted in a manner that is commensurate with the privacy risk identified and respects the operating environment of the government institution.

3.4 This directive is issued pursuant to paragraph 71(1)(*d*) and subsections 71(3), 71(4), 71(5) and 71(6) of the *Privacy Act*.

3.5 This directive is to be read in conjunction with the *Privacy Act*, the *Privacy Regulations*, the *Policy on Privacy Protection*, *Directive on Privacy Practices* and *Directive on Privacy Requests and Correction of Personal Information* and the *Directive on Social Insurance Number*.

4. Definitions

4.1 Definitions to be used in the interpretation of this directive are attached in Appendix A. Additional definitions are provided in Appendix A of the *Policy on Privacy Protection*.

5. Directive statement

5.1 Objectives

5.1.1 To provide direction to government institutions with respect to the administration of PIAs for new or substantially modified programs and activities involving the creation, collection and handling of personal information; and

5.1.2 To ensure, through the conduct of PIAs, sound management and decision making as well as careful consideration of privacy risks with respect to the creation, collection and handling of personal information as part of government programs or activities.

5.2 Expected results

5.2.1 PIAs are conducted in a manner that is commensurate with the level of privacy risk identified prior to establishing any new or substantially modified program or activity involving personal information.

5.2.2 Privacy practices that comply with legal and policy requirements related to the administration of the *Privacy Act* are implemented.

5.2.3 The public reporting of personal information under the control of government institutions is complete, accurate and up to date.

6. Requirements

6.1 Heads of government institutions are responsible for:

6.1.1 Establishing a PIA development and approval process that:

- takes into consideration the responsibility within the institution for establishing PIBs;
- is commensurate with the level of risk related to the privacy invasiveness of the institution's programs or activities; and
- ensures the PIA is completed by the senior official or executive holding responsibility within the institution for new or substantially modified programs or activities.

6.2 Heads of government institutions or the official responsible for section 10 of the *Privacy Act*, are to fulfill the following responsibilities:

6.2.1 Establishing or modifying PIBs in collaboration with the senior official or executive holding functional responsibility for the new or substantially modified program or activity;

6.2.2 Obtaining approval of the designated Minister for any new or substantially modified PIB before implementing the new or modified program or activity, unless otherwise specified in the terms and conditions of a delegation under subsection 71(6) of the *Privacy Act*—this requirement only applies to the departments defined in section 2 of the *FAA*;

6.2.3 Adhering to the specific obligations related to PIAs and the Treasury Board submission process outlined in Appendix B; and

6.2.4 Collaborating with the appropriate senior official or executive to ensure that PIAs are completed and respect the process outlined in section 6.3.

6.3 The appropriate senior officials or executives are responsible for adhering to the following process for the completion of a privacy impact assessment:

A) Initiation of a privacy impact assessment

6.3.1 Initiating a PIA for a program or activity in the following circumstances:

- when personal information is used for or is intended to be used as part of a decision-making process that directly affects the individual;
- upon substantial modifications to existing programs or activities where personal information is used or intended to be used for an administrative purpose; and
- when contracting out or transferring a program or activities to another level of government or the private sector results in substantial modifications to the program or activities.

6.3.2 Determining, in consultation with the official responsible for section 10 of the *Privacy Act*, whether:

- a new or substantially modified program or activity in which no decisions are made about individuals will have an impact on privacy and warrant the conduct of a PIA; or
- the government institution's privacy protocol is adequate to address the potential impact on privacy of such a program or activity.

6.3.3 Documenting decisions adequately with respect to requirement 6.3.2.

B) In cases where more than one institution is involved

6.3.4 Identifying the lead government institution in cases of multi-institutional PIAs. Unless otherwise established by an arrangement or agreement, the lead government institution will be the institution that has primary control over the personal information or holds the authority for initiating the program or activity.

6.3.5 Ensuring, in cases where the above factors are not relevant because the program or activity is common to all government institutions, that the lead will be, unless otherwise established by an arrangement or agreement, the government institution that either:

- is responsible for delivering the program or activity across government;
- is the contracting authority for the program or activity; or
- is the policy authority for the program or activity across government.

6.3.6 Coordinating, as appropriate, an interdepartmental committee made up of key stakeholders, including legal and policy authorities when a new program or activity involves government-wide consideration.

6.3.7 Determining and documenting the most appropriate approach for the completion and approval of the PIA in support of the program or activity. In cases of joint programs or activities, an overarching or a multi-institutional PIA is favoured. At a minimum, the approach will take into consideration the approval process of the institutions involved and will cover the full scope of the program or activity.

6.3.8 Overseeing the initial collection as well as any disclosures to government institutions involved in the program or activity.

C) Completion of the privacy impact assessment

6.3.9 Completing the core PIA elements as outlined in Appendix C.

6.3.10 Determining an appropriate format for the PIA based on the government institution's business needs, internal reporting and broader risk management activities.

6.3.11 Determining, in consultation with the official responsible for section 10 of the *Privacy Act* and based on the completed core PIA, if additional documentation or analysis is required and whether further elaboration on specific risk mitigation is warranted. When high level risks are identified, additional documentation, including mitigation plans or strategies, will be required.

D) Internal approval of the privacy impact assessment

6.3.12 Obtaining, prior to seeking formal approval, endorsement or sign-off from:

- the official responsible for section 10 under the *Privacy Act*;
- the appropriate senior officials or executives; and
- the government institution's legal services unit—in cases where the legal authority for the program or activity is unclear or where potential issues with respect to the *Charter of Rights and Freedoms* have been raised.

6.3.13 Obtaining internal approval of the completed core PIA in accordance with the process established within the government institution.

E) Notification and registration

6.3.14 Ensuring that the approved core PIA is provided to Treasury Board Secretariat (TBS) along with the proposed new or substantially modified PIB description, unless otherwise specified in the terms and conditions of a delegation under subsection 71(6) of the *Privacy Act*. TBS will only confirm that mandatory requirements of the core PIA have been completed for the purpose of establishing or revising a PIB. Because no additional documentation will be reviewed, none is to be provided to TBS for the purpose of reviewing and approving PIBs.

6.3.15 Ensuring that the approved core PIA provided to TBS is simultaneously provided to the Office of the Privacy Commissioner, along with any additional documentation that may be requested by that office.

F) Public reporting of the core privacy impact assessment

6.3.16 Making the following sections of the approved core PIA available to the public:

- Overview and PIA Initiation; and
- Risk Area Identification and Categorization—Areas (a) to (h).

6.3.17 Respecting security requirements as well as any other confidentiality or legal consideration when reporting publicly on the sections of the core PIA cited in 6.3.16.

G) Sharing the privacy impact assessment

6.3.18 Sharing copies of the approved PIA and other relevant documentation with partners or other government institutions as required and in a manner that respects security requirements as well as any other confidentiality or legal consideration.

6.4 Monitoring and reporting requirement

6.4.1 The monitoring and reporting requirements of the *Policy on Privacy Protection* apply to this directive.

7. Consequences

7.1 The consequences outlined in the *Policy on Privacy Protection* apply to this directive.

8. Roles and responsibilities of government organizations

8.1 In addition to the roles and responsibilities of government organizations identified in the *Policy on Privacy Protection*, the Treasury Board Secretariat will:

8.1.1 Review the content of the approved core PIA in a timely manner to ensure that the assessment is complete. TBS does not approve PIAs and will only review the core PIA to fulfill its obligation with respect to the review and approval of PIBs.

8.1.2 Review, approve and register PIBs for the departments defined in section 2 of the FAA.

8.1.3 Review and register the PIBs of all government institutions including the Bank of Canada in compliance with the Act;

8.1.4 Review Appendix C—Core privacy impact assessment on an annual basis to ensure that the core PIA remains relevant and propose amendments if required.

8.2 In addition to the roles and responsibilities of government organizations identified in the *Policy on Privacy Protection*, the Office of the Privacy Commissioner can:

8.2.1 Decide whether analysis or additional information is necessary for the purpose of its review or investigation under the *Privacy Act*.

As an Officer of Parliament charged with the oversight of the *Privacy Act*, the Privacy Commissioner has broad powers of investigation and review and can request additional project documentation related to the planning, assessment or implementation of new or substantially modified programs or activities that involve personal information or have an impact on the privacy of Canadians and of those individuals present in Canada.

9. References

9.1 Relevant legislation and regulations:

- *Access to Information Act*
- *Access to Information Regulations*
- *Canadian Charter of Rights and Freedoms*
- *Financial Administration Act*
- *Library and Archives of Canada Act*
- *Official Languages Act*
- *Personal Information Protection and Electronic Documents Act*
- *Privacy Act*
- *Privacy Regulations*

9.2 Related policy instruments and publications:

- *Communications Policy of the Government of Canada*
- *Contracting Policy*
- *Directive on Information Management Roles and Responsibilities*
- *Directive on Privacy Practices*
- *Directive on Privacy Requests and Correction of Personal Information*
- *Directive on the Social Insurance Number*
- *Policy on Government Security*
- *Integrated Risk Management Framework*
- *Policy Framework for Information and Technology*
- *Policy on Access to Information*
- *Policy on Information Management*
- *Policy on Learning, Training and Development*
- *Policy on Management of Information Technology*
- *Policy on Management of Projects*
- *Policy on Privacy Protection*

10. Enquiries

10.1 Please direct enquiries about this directive to your institution's access to information and privacy (ATIP) coordinator. For interpretation of this directive, the ATIP coordinator is to contact:

Information and Privacy Policy Division
Chief Information Officer Branch
Treasury Board Secretariat
219 Laurier Avenue West
Ottawa ON K1A 0R5

E-mail: ippd-dpiprp@tbs-sct.gc.ca
Telephone: 613- 946-4945
Fax: 613-952-7287

Appendix A - Definitions

appropriate senior official or executive of the government institution (*agent principal ou cadre approprié de l'institution fédérale*)
: Is the official holding administrative responsibility for the completion of the PIA. Where an official is not specifically assigned, this responsibility will rest with the senior official or executive holding functional responsibility for the program or activity in question.

authentication (*authentification*)
: Is the act of verifying (i) the validity of the identity of an individual or an Entity, or (ii) the integrity of data in electronic form.

automated personal information analysis, personal information matching and knowledge discovery techniques (*recours à des techniques d'analyse automatisée des renseignements personnels, de comparaison des renseignements personnels et de découverte de connaissances*)
: Refer to those activities involving the use of technology to analyze, match, create, compare, cull, identify, define or extract personal information elements.

core privacy impact assessment (*évaluation des facteurs relatifs à la vie privée de base*)
: Consists of those standardized elements of a PIA that are directly linked to policy and legal compliance.

enhanced identification methods (*méthodes d'identification améliorées*)
: Refer to the technological means used to identify or authenticate an identifiable individual.

flow of personal information (*flux des renseignements personnels*)
: Describes the creation, collection, retention, use, disclosure and disposition of personal information. It also includes the identification of partners that handle the personal information during the administration of a program or an activity.

lead government institution (*institution fédérale responsable*)
: Is the government institution that leads the multi-institutional PIA and is responsible for determining the most appropriate approach for the completion and approval of the PIA in support of a multi-institutional program or activity.

official responsible for section 10 of the *Privacy Act* (*agent pour l'article 10 de la Loi sur la protection des renseignements personnels*)
: Is the officer or employee that has been designated through a delegation order with the responsibilities of the head or the officer or employee who is performing those responsibilities in the name of the head with respect to section 10 of the *Privacy Act*, which concerns the establishment of PIBs for the personal information under the control of the government institution.

substantial modification (*modification importante*)
: Refers to a change or an amendment to the privacy practices related to a particular program or activity, which is reflected in a PIB description. This includes any change or amendment to the privacy practices related to activities that use automated or technological means to identify, create, analyze, compare, extract, cull, match or define personal information.

surveillance (*surveillance*)
: Refers to a systematic approach for watching over, tracking or monitoring physical and logical spaces, individuals or individuals' activities, whereabouts, behaviour or interests.

Appendix B—Privacy Impact Assessment requirements related to the preparation of Treasury Board submissions

Government institutions seeking Treasury Board approval for programs or activities that involve personal information are responsible for:

- Making every reasonable effort to initiate the PIA at the earliest possible phase of project planning;
- Identifying whether a PIA has been completed in the body of the submission and, if a PIA was not completed because of the urgency or priority of the initiative, identifying the timelines for the completion of the PIA;
- Identifying in their project brief the measures taken or to be taken to address privacy issues and risks, where relevant, when seeking project approval from Treasury Board; and
- Completing a PIA for the new or substantially modified program or activity that was approved by Treasury Board either before its implementation or within such time and subject to such conditions established by TBS.

Unless otherwise specified in the terms and conditions of a delegation under subsection 71(6) of the *Privacy Act*, government institutions defined as departments in section 2 of the FAA and referenced in subsection 71(5) of the *Privacy Act* are responsible for:

- Obtaining approval of any new or substantially modified PIB before implementing the new or substantially modified program or activity that is related to the PIB; and

- Abiding by any terms and conditions related to the approval of PIBs by the designated Minister in accordance with subsections 71(3) and 71(4) of the *Privacy Act*.

Note: Under the *Policy on Privacy Protection*, heads of government institutions are required to notify the Privacy Commissioner of any planned initiatives (legislation, regulations, policies, programs) that could relate to the *Privacy Act* or to any of its provisions or that could have an impact on the privacy of Canadians. This notification is to take place at a sufficiently early stage to permit the Commissioner to review and discuss the issues involved.

Appendix C—Core privacy impact assessment

The following sections and their information requirements make up the minimum content of the core PIA. In the case of a multi-institutional PIA, each government institution involved will be responsible for contributing to or completing the core PIA in a manner that is consistent with the approach outlined by the lead government institution.

Section I—Overview and PIA Initiation

a. The government institution or, in the case of a multi-institutional PIA, the lead government institution.
b. The head of the government institution or delegate for section 10 of the *Privacy Act* or, in the case of a multi-institutional PIA, the head or delegate of each government institution involved in the program or activity.
c. The appropriate senior official or executive for the new or substantially modified program or activity.
d. Name and description of the program or activity of the government institution or, in the case of a multi-institutional PIA, of the lead government institution.
e. Legal authority for the program or activity or, in the case of a multi-institutional PIA, the legal authority for each government institution involved in the program or activity.
f. Identification of whether the proposal is related to a new PIB or will substantially modify an existing PIB. Existing PIBs are to be identified by their title, registration number and bank number.
g. Short description of the project, initiative or change.
h. In the case of a multi-institutional PIA, the lead government institution will describe the approach for the completion and approval of the PIA in support of the program or activity. At a minimum, a multi-institutional PIA will identify the government institutions involved and ensure that the role of each institution with respect to the program or activity is adequately documented, unless otherwise determined by the approach.

Section II—Risk Area Identification and Categorization

The core PIA must include a completed risk identification and categorization section as outlined below. To have consistent risk categories and risk measurement across government institutions, standardized risk areas (itemized below) and a common risk scale are to be maintained as the basis for risk analysis.

The numbered risk scale is presented in an ascending order: the first level (1) represents the lowest level of potential risk for the risk area; the fourth level (4) represents the highest level of potential risk for the given risk area.

The initial step of the analysis consists of evaluating each risk area independently. The second step consists of grouping the individual results to determine if a more in depth analysis is required. 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	1
- Administration of program or activity and services	2
- Compliance or regulatory investigations and enforcement	3
- Criminal investigation and enforcement or national security	4

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.	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.	2
- Social Insurance Number, medical, financial or other sensitive personal information or the context surrounding the personal information is sensitive; personal information of minors or of legally incompetent individuals or involving a representative acting on behalf of the individual.	3
- Sensitive personal information, including detailed profiles, allegations or suspicions and bodily samples, or the context surrounding the personal information is particularly sensitive.	4

c) Program or activity partners and private sector involvement	Risk scale
- Within the institution (among one or more programs within the same institution)	1
- With other government institutions	2
- With other institutions or a combination of federal, provincial or territorial, and municipal governments	3

- Private sector organizations, international organizations or foreign governments	4

d) Duration of the program or activity	Risk scale
- One-time program or activity	1
- Short–term program or activity	2
- Long-term program or activity	3

e) Program population	Risk scale
- The program's use of personal information for internal administrative purposes affects certain employees.	1
- The program's use of personal information for internal administrative purposes affects all employees.	2
- The program's use of personal information for external administrative purposes affects certain individuals.	3
- The program's use of personal information for external administrative purposes affects all individuals.	4

f) Technology and privacy
- Does the new or substantially modified program or activity involve implementation of a new electronic system or the use of a new application or software, including collaborative software (or groupware), to support the program or activity in terms of the creation, collection or handling of personal information?
- Does the new or substantially modified program or activity require any modifications to information technology (IT) legacy systems?
Specific technological issues and privacy - Does the new or substantially modified program or activity involve implementation of new technologies or one or more of the following activities: • enhanced identification methods; • surveillance; or • automated personal information analysis, personal information matching and knowledge discovery techniques?
A **YES** response indicates the potential for privacy concerns and risks, which will require consideration and, if necessary, mitigation.

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).	1
- The personal information is used in a system that has connections to at least one other system.	2
- The personal information is transferred to a portable device (i.e., USB key, diskette, laptop computer), transferred to a different medium or is printed.	3
- The personal information is transmitted using wireless technologies.	4

h) Potential risk that in the event of a privacy breach, there will be an impact on the individual or employee.

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

Note: For additional guidance on items h) and i), government institutions can refer to the Guidelines for Privacy Breaches.

In the case of a multi-institutional PIA, each government institution involved is, at a minimum, responsible for completing items b), c), f), g), h) and i), whereas the lead government institution is responsible for completing items a), d) and e).

Section III—Analysis of Personal Information Elements for the Program or Activity

a. Identify each element of personal information collected (for example: 1) name, 2) address).
b. Identify sub-elements associated with each element of personal information collected (for example: 1) first name / middle initial / last name, 2) street name / street number / city / province /postal code).
c. Identify how the personal information will be recorded: on paper, electronically, audio recordings, visual image recordings, human biological samples or other (specify).

In the case of a multi-institutional PIA, each government institution involved is, at a minimum, responsible for identifying the elements of personal information collected or disclosed in relation to their involvement in the multi-institutional program or activity.

Section IV—Flow of Personal Information for the Program or Activity

a. Identify the source(s) of the personal information collected and / or how the personal information will be created.
b. Identify both internal and external sources for the personal information's use and disclosure, that is, identify the areas, groups and individuals who have access to or handle the personal information and to whom it is provided or disclosed. Where relevant, include the following information:
    - Government institution responsible for the program or activity (provide PIB title and number);
    - Other government institution responsible for the program or activity (provide PIB title and number); or
    - Non-federal government institution (e.g., provincial or territorial, municipal, or Aboriginal governments or councils,

organization of a foreign state, international organization) or private sector.

c. Identify where the personal information will transit and will be stored or retained.
d. Identify where areas, groups and individuals can access the personal information.

The government institution is to determine the format for representing the flow of personal information.

In the case of a multi-institutional PIA, each government institution involved is, at a minimum, responsible for outlining the flow of personal information under its control. The lead government institution will be responsible for outlining the flow of personal information between or among government institutions.

Section V—Privacy Compliance Analysis

a. At a minimum, the privacy compliance analysis must cover the following areas and identify specific compliance actions taken or to be taken to meet with each area's requirements:
    - Collection authority (section 4 of the *Privacy Act*)
    - Direct collection, notification and consent, as appropriate (section 5 of the *Privacy Act*)
    - Retention (section 6 of the *Privacy Act*)
    - Accuracy (section 6(2) of the *Privacy Act*)
    - Use (section 7 of the *Privacy Act*)
    - Disclosure (section 8 of the *Privacy Act*)
    - Administrative, physical and technical safeguards
    - Technology and privacy issues
        - Indicate any changes to the business requirements that have an impact on the system, software or program application and, consequently, may affect the current access controls and privacy practices related to the creation, collection, retention, use, disclosure and disposition of personal information.
        - Determine whether the current IT legacy systems and services that will be retained or those that will be substantially modified are compliant with privacy requirements.
        - Identify any awareness activities related to protection of privacy requirements in the new electronic environment.

In the case of a multi-institutional PIA, each government institution involved is, at a minimum, responsible for outlining the privacy practices for the personal information under its control.

Section VI—Summary of Analysis and Recommendations (as applicable)

a. Document the conclusion drawn or recommendations resulting from the risk identification and categorization in a manner that is commensurate with the risk identified.

Section VII—Supplementary Documents List

a. List any additional documents that were used or are related to the core PIA; these documents do not need to be appended to the core PIA.

Section VIII—Formal Approval

a. Indicate that the PIA was formally approved in accordance with the government institution's approval process.
b. In the case of a multi-institutional PIA, indicate that the lead government institution determined the PIA was formally approved.

Completion of the above sections with the information requested fulfills the minimum content requirements of the core PIA.