EPA Classification No: CIO 2151-P-04.1	CIO Approval Date: 1/5/10
CIO Transmittal No: 10-002	Review Date: 1/13

Issued by the EPA Chief Information Officer,
Pursuant to Delegation 1-19, dated 7/7/05

PROCEDURES FOR PREPARING PRIVACY IMPACT ASSESSMENTS

1. PURPOSE

These procedures provide instructions for determining if personally identifiable information (PII) is collected in electronic systems and ensuring adequate controls are put in place. The Privacy Impact Assessment (PIA) is the tool required by the Office of Management and Budget (OMB) for addressing privacy issues with electronic systems. The PIA evaluation process provides a means to assure Agency compliance with laws and regulations governing the privacy of individuals and helps ensure that the electronic systems developed by the Agency protect individuals' privacy.

2. SCOPE AND APPLICABILITY

These procedures apply to all EPA organizations and its contractors engaged in the design and development of Agency systems, databases or applications (hereafter, systems). A PIA is required for:

a. New Systems: Any new system that collects, maintains, or disseminates personally identifiable information (PII) from or about members of the public as required by the E-Government Act of 2002. (OMB Memorandum M-07-16 recommends that agencies provide the same privacy protections to information about its employees. Accordingly, EPA may require PIAs on certain systems that collect PII on Agency employees.) The PIA should be initiated during the definition phase of the system life cycle phase and updated in each phase of the life cycle until the operation and maintenance. At this time, the final PIA should be submitted reflecting the current state of the system.

b. Existing Systems: Require an updated PIA when there is a significant modification or where changes have been made to the system that may create a new privacy risk. (For a listing of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f)). http://www.whitehouse.gov/omb/circulars/a130/a130appendix_i.aspx

c. Information Collection Requests: When the information collected is both new and an electronic collection for ten or more individuals who are not employees of the Federal government.

d. Capital Planning and Investment Control (CPIC) Systems: EPA requires all CPIC systems (i.e., major and lite) to complete a PIA.

3. AUDIENCE

All Agency system developers, system owners and their contractors.

EPA Classification No: CIO 2151-P-04.1	CIO Approval Date: 1/5/10
CIO Transmittal No: 10-002	Review Date: 1/13

4. BACKGROUND

The E-Government Act of 2002 requires PIAs for electronic systems as well as information collection requests that are electronic. Conducting the PIA is a process for examining the risks and ramifications of collecting, maintaining and disseminating information in an *identifiable form* in an electronic system, and for identifying and evaluating protections and alternative processes to mitigate the impact on privacy of collecting information in identifiable form. *Identifiable form* refers to data within the system or online collection that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. The PIA provides a *framework* for considering the privacy implications of information collected on individuals and where potential disclosure risks may lie. Informed decision-making and the ability to design a system which addresses actual or potential privacy concerns are dependent on early identification of privacy issues. Privacy concerns should always be considered when requirements are being analyzed and decisions are being made about data collection, usage, storage and system design.

The PIA:

- Identifies the type of personal and potentially identifiable information in the system;
- Identifies who has access to that information (whether full access or limited access rights); and
- Describes the administrative controls that ensure that only information that is necessary and relevant to EPA's mission is included in the system and that the PII is accessed only by individuals with a "need to know" in the performance of their official duties.

5. AUTHORITY

E-Government Act of 2002, Section 208, 44 U.S.C. 3501 note.

6. PROCEDURES

A Privacy Threshold Analysis (PTA) should be completed as soon as the system has been categorized in ASSERT (i.e., the Automated System Security Evaluation and Remediation Tracking tool). The Program Office/Region will conduct a PTA prior to initiating a PIA. The PTA will identify if the system will collect any type of PII elements. If so, a PIA will be required to evaluate the privacy risks to the individuals. When required, the PIA should be developed immediately after the PTA finding.

Program Office/Region

- Complete the Privacy Threshold Analysis (PTA) at http://intranet.epa.gov/privacy/guidance_document.htm.
- Complete the PIA form (if required) located at http://intranet.epa.gov/privacy/policies_procedures.htm.
- Submit PTA and/or PIA to Liaison Privacy Official (LPO).

Liaison Privacy Official

- Review PTA and/or PIA for completeness.
- Forward PTA, along with the LPO's findings, to the Privacy Act Officer.
- Inform preparer if PIA is required.
- Forward PIA to Privacy Act Officer for review and approval.

Privacy Act Officer

- Review the PTA and/or PIA upon receipt.
- Confirm the records control schedule referenced in the PIA with Agency Records Office.
- Provide final determination concerning PIA requirements.
- Post PIAs subject to E-Government Act requirements to the Privacy Web site.

7. RELATED DOCUMENTS

- Privacy Act of 1974 (5 USC 552a) (http://archives.gov/about/laws/privacy-act-1974.html)
- E-Government Act of 2002, 44 U.S.C. 3501 et seq.
- http://www.whitehouse.gov/omb/memoranda_fy2005_m05-15/, 44 USC 3541
- OMB Circular A-130, Management of Federal Information Resources, Appendix I
- M-99-18, Privacy Policies of Federal Web Sites (June 2, 1999) (June 2, 1999)
- M-03-18, Implementation Guidance for the E-Government Act of 2002 (August 1, 2003)
- M-05-15, FY 2005 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (June 13, 2005)
- M-06-15, Safeguarding Personally Identifiable Information (May 22, 2006)
- M-06-20, FY 2006 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 17, 2006)
- M-06-25, FY 2006 E-Government Act Reporting Instructions (August 25, 2006)
- M-07-19, FY 2007 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management (July 25, 2007)
- M-07-20, FY 2007 E-Government Act Reporting Instructions (August 14, 2007)
- M-04-25, FY 2004 Reporting Instructions for the Federal Information Security Management Act (August 23, 2004)
- Section E- FY04 FISMA Reporting Template (Excel)

8. ROLES AND RESPONSIBILITIES

Agency Privacy Act Officer – Reviews PTAs to determine if correct determination has been made by the LPO. Reviews PIAs to ensure compliance with E-Government Act and Privacy Act requirements. Approves PIAs in accordance with provisions of Section 208 of the E-Government Act of 2002, 44 U.S.C. 3501 note. Posts applicable PIAs to Agency Privacy Web site.

Agency Records Officer – Reviews record control schedules to ensure that applicable schedules are applied.

Liaison Privacy Officials – Provide assistance, guidance and feedback to PIA preparers. Review PTA and PIA for completeness. Forward the paperwork to the Privacy Act Officer for review and approval.

Personally Identifiable Information (PII) - Any information about an individual maintained by an agency, which can be used to distinguish, trace, or identify an individual's identity, including personal information which is linked or linkable to an individual.

Program Offices/Regions – Conduct a Privacy Threshold Analysis for newly developed systems and systems that undergo substantial revision and complete PIAs for any system that collects Privacy Act information.

9. DEFINITIONS

Identifiable Form. Information in an Information Technology (IT) system or online collection that: (1) directly identifies an individual (e.g. name, Social Security Number [SSN], date of birth) or (2) in conjunction with other data elements allows for indirect identification (race, gender, demographic indicator).
Personal Identifier. A name, SSN, or other identifying number, symbol, or other identifying particular assigned to an individual.
Privacy Act Information. Data about an individual that is maintained in a system of records and retrieved by name or other personal identifier assigned to the individual.
Privacy Impact Assessment (PIA). An analysis of how privacy information is handled: (i) to ensure that handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.
Privacy Threshold Analysis (PTA). A survey of questions that is prepared for all new systems and any other systems that undergo substantial modifications. The PTA determines if the system will be collecting any PII data elements and if a full PIA is required to evaluate privacy risks from the collection. Review of survey responses will allow the Privacy Act Officer to determine whether any personally identifiable data elements will be collected and whether a full PIA is required.
System of Records (SOR). A group of any records under the control of the Agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual.

10. WAIVERS

There are no waivers to this procedure.

11. RELATED PROCEDURES AND GUIDELINES

- EPA's Privacy Policy http://www.epa.gov/privacy/policy/index.htm
- Privacy Act Manual http://www.epa.gov/privacy/policy/2190/index.htm
- System of Record Notice http://intranet.epa.gov/privacy/policies_procedures.htm

12. MATERIAL SUPERSEDED

These procedures update and replace CIO 2151-P-04.

13. ADDITIONAL INFORMATION

For further information, please contact the Records, FOIA and Privacy Branch, Collection Strategies Division, Office of Information Collection, Office of Environmental Information.

Linda A. Travers
Principal Deputy Assistant Administrator
Office of Environmental Information