PRIVACY IMPACT ASSESSMENTS

Official Guidance

Office of Privacy and Civil Liberties

United States Department of Justice

(Revised March 2012)

Introduction

The Department of Justice (the Department or DOJ) is committed to ensuring the appropriate protection of privacy and civil liberties in the course of fulfilling its missions. Privacy Impact Assessments (PIAs), which are required by Section 208 of the E-Government Act of 2002,[1] are an important tool to assist the Department in achieving this objective. Specifically, Section 208 of the E-Government Act of 2002 requires all federal agencies to conduct a PIA before developing or procuring information technology that collects, maintains, or disseminates information that is in identifiable form or before initiating a new collection of information that will be collected, maintained, or disseminated using information technology and that includes any information in identifiable form in certain circumstances involving the public.

In August 2010, the Department's Office of Privacy and Civil Liberties (OPCL) revised the Department's PIA template to better assist DOJ components in conducting their PIAs. This guidance is designed to supplement the revised DOJ PIA template by providing DOJ personnel with guidance on how to effectively conduct a PIA and how to properly document this assessment.

This guidance is solely for the purpose of setting forth internal Department policy and guidance, and does not create any rights, substantive or procedural, that are enforceable at law by any party in any matter, civil or criminal.

Chief Privacy and Civil Liberties Officer's Authority

The Department's Chief Privacy and Civil Liberties Officer (CPCLO) is primarily responsible for the Department's privacy policy, including advising the Attorney General regarding "appropriate privacy protections, relating to the collection, storage, use, disclosure, and security of personally identifiable information, with respect to the Department's existing or proposed information technology and information systems."[2] Additionally, the CPCLO is responsible for advising the Attorney General concerning the "implementation of policies and procedures, including appropriate training and auditing, to ensure the Department's compliance with privacy-related laws and policies, including section 552a of title 5, United States Code [the Privacy Act of 1974], and Section 208 of the E-Government Act of 2002 (Public Law 107–347)."[3]

The CPCLO's review and approval of Departmental PIAs is one mechanism through which the CPCLO fulfills the above-referenced statutory mandates.[4]

[1] E-Government Act of 2002, Pub. L. 107-347, § 208, 116 Stat. 2899, 2921-23.
[2] Violence Against Women and Department of Justice Reauthorization Act of 2005, Pub. L. 109-162, § 1174, 119 Stat. 2960, 3124 (2006). See also Implementing Recommendations of the 9/11 Commission Act of 2007, Pub. L. 110-53, § 803, 121 Stat. 266, 360-1.
[3] Violence Against Women and Department of Justice Reauthorization Act of 2005 § 1174.
[4] See Attorney General Order No. 2843-2006, dated October 2, 2006 (CPCLO approval for PIAs required).

Office of Privacy and Civil Liberties' Role

OPCL supports the CPCLO through the development and implementation of the Department's privacy compliance program. With regard to PIAs, OPCL provides guidance and training to components on compliance with E-Government Act PIA requirements, reviews PIAs in preparation for signature by the CPCLO, and provides public notice of PIAs as appropriate. Accordingly, OPCL issues this PIA guidance to be followed by all Departmental offices, boards, divisions, components, and bureaus.

What is a PIA?

A PIA is an analysis required by the E-Government Act of how information in identifiable form[5] is handled to ensure compliance with applicable legal, regulatory, and policy requirements regarding privacy, to determine the risks and effects of collecting, maintaining, and disseminating such information in an electronic information system, and to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.[6] The PIA demonstrates that the Department considers privacy from the beginning stages of a system's development and throughout the system's life cycle (i.e., collection, use, retention, processing, disclosure, and destruction). This ensures that privacy protections are built into the system from the start – not after the fact – when they can be far more costly or could affect the viability of the project. Additionally, the PIA demonstrates that the system developers and owners have made technology choices that reflect the incorporation of privacy into the fundamental system architecture.

The PIA also gives the public notice of this analysis and helps promote trust between the public and the Department by increasing transparency of the Department's systems and missions.

When Should a PIA be Completed?

A PIA should be conducted before developing or procuring IT systems or projects that collect, maintain, or disseminate information in identifiable form, or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for ten or more persons (excluding agencies, instrumentalities or employees of the federal government).[7]

---

[5] The E-Government Act of 2002 applies to "information in identifiable form." We note that the National Institute of Standards and Technology (NIST) has stated that the term "information in identifiable form" is "[o]ften considered to have been replaced by the term PII [personally identifiable information]." NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), Appendix C (April 2010). However, NIST also notes that terms such as "information in identifiable form" are similar to NIST's definition of PII and "organizations should not use the term PII (as defined in this document) interchangeably with these terms and definitions because they are specific to their particular context." Id.

[6] See OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A, Section II.A.6, dated Sept. 26, 2003.

[7] See id. at Section II.B.1.

OPCL assists components by assessing the need to conduct a PIA through the Initial Privacy Assessment (IPA) process.[8] Once OPCL provides a component with a determination that a PIA is required, a PIA should be conducted. The PIA should be drafted and issued during system development, with sufficient lead time to permit final Departmental approval and public website posting on or before the commencement of any system operation (including before any testing or piloting).

Section 208 of the E-Government Act does not apply to national security systems.[9] Nevertheless, it is the Department's policy that PIAs must also be conducted for national security systems and submitted to OPCL for review and approval by the CPCLO.

Who Should Prepare the PIA?

The PIA process requires that candid and forthcoming communications occur among the system manager/owner, component privacy officials, and OPCL, to make the PIA comprehensive and meaningful and to ensure appropriate and timely handling of privacy concerns. With this in mind, the PIA should be written and reviewed by a combination of the component's privacy officials, IT security staff, and the program personnel responsible for the system.

Preparing a PIA

The E-Government Act requires, where practicable, that agencies make PIAs publicly available. Therefore, PIAs should be clear, unambiguous, and understandable to the general public. The length and breadth of a PIA will vary according to the size and complexity of the system.

To ensure consistency within the Department in the preparation of PIAs, all components must utilize and fully complete the most recent Department PIA template, as posted on the OPCL website at http://www.justice.gov/opcl.htm, or on the DOJnet.

Please adhere to the following guidelines when drafting responses to the questions posed in the PIA template:

- Use plain language and take into account the perspective of a member of the public who is unfamiliar with the system or technology.
- Spell out each acronym the first instance it is used it in the document (e.g., Office of Management and Budget (OMB)).
- Use words, phrases, or names in the PIA that are readily known to the public.
- Define technical terms or references.
- Clearly reference projects and systems and provide explanations, if needed, to aid the general public.
- Include the complete name of the reference when first referencing National

[8] More information about the IPA process can be found in the DOJ's IPA Instructions and Template at http://www.justice.gov/opcl/pia.htm.

[9] See E-Government Act of 2002, § 202(i) (stating that most provisions of Title II (including Section 208) do not apply to national security systems).

Institute of Science and Technology (NIST) publications and other documents (e.g., NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)). The abbreviated format may be used for subsequent references. Full names for NIST documents can be found at NIST's website http://csrc.nist.gov/publications/nistpubs.

It is imperative that in preparing a PIA the component also review other privacy and security documentation relevant to the system, such as any Privacy Act System of Records Notice (SORN) and/or System Security Plan (SSP), to ensure consistency among all privacy/security documentation and the PIA.

A component privacy office with concerns regarding the sufficiency of a proposed answer, or with questions about the PIA template, is welcome to consult informally with OPCL before submitting the response or PIA for final review and approval. Similarly, component IT security staff with concerns or questions regarding the sufficiency of a proposed response to questions concerning the technical or security aspects of the system, should feel free to consult with the Department's Office of the Chief Information Officer (OCIO).

Obtaining Approval and Signatures

The component is responsible for preparing the PIA, including the completion of all internal component reviews, and obtaining the signature of the appropriate component Security Review Official. For Department Components with an appointed Chief Information Officer (CIO), the Security Review Official shall be the Component CIO. For offices within JMD, the Security Review Official shall be the JMD Staff Director. For Offices, Boards and Divisions (OBDs) without an appointed CIO, the Security Review Official shall be the OBD Executive Officer, if the system is owned by the OBD, or the OCIO Staff Director, if the system is owned by the OCIO. In each case, the appropriate Security Review Official shall review all PIAs, assessing whether the system controls meet the security requirements, and shall indicate his/her approval of the system's technical description and security by signing the PIA.

The Senior Component Official for Privacy (if designated; otherwise privacy point of contact) should then sign the PIA, indicating official issuance by the component, and then forward the PIA to OPCL for Departmental review and final approval. [10] (Please email the PIA to OPCL at privacy@usdoj.gov; if a PIA is classified, please contact OPCL to coordinate delivery.) PIAs should not be sent to OPCL until all required component signatures have been obtained.

Upon receipt of the PIA, OPCL will review the PIA for legal sufficiency and compliance with the E-Government Act of 2002, as well as further advise the CPCLO of privacy policy issues. Part of that review will include ensuring that there is consistency with related materials (such as SORNs and SSPs). OPCL will coordinate with the

[10] If a PIA contains information that the component wishes to redact prior to publication due to its sensitive or protected nature, the PIA should be appropriately marked to indicate the proposed redactions and the component must provide an explanation, as discussed below, under "Publishing the PIA."

Department's OCIO to obtain a technical and system security review of the PIA. The OCIO will provide OPCL and the CPCLO with a recommendation for approval once the PIA satisfies the OCIO's requirements. If warranted, OPCL and/or the CPCLO may return the PIA to the component for revision or may disapprove it in accordance with the CPCLO's authority.[11] The CPCLO will approve and sign the PIA once the CPCLO determines that the PIA satisfies the applicable requirements. An approved PIA will then be returned to the component for information and publication.

Publishing the PIA

The PIA should not be published until the PIA has been approved and signed by the CPCLO, and OPCL has so advised the component. Approved PIAs will be available to the general public. However, the Department, in its discretion, is not required to make a PIA (or portions thereof) publicly available if such publication would raise security concerns, or would reveal classified, sensitive, or otherwise protected information (e.g., potentially damaging to a national interest, law enforcement effort, or competitive business interest) that is contained in the assessment. If a component submits a PIA to OPCL that contains information that the component wishes to redact prior to publication due to its sensitive nature, the PIA should be appropriately marked to indicate the portions that the component proposes to redact, and the component must attach a separate explanation for the proposed redaction(s).

Publication normally should be accomplished by placing the PIA on the Justice.gov/opcl website. OPCL has a dedicated web page where Department PIAs are posted. Components may also post their PIAs on a component-specific PIA web page.

For PIAs that are completed for systems in development, the PIA does not need to be published until the design and construction of the system have been completed, and the PIA reflects the system as it will operate. However, a component may exercise its discretion and publish a PIA for a system still in development, if it so chooses.

Updating PIAs

Recognizing that information systems may undergo changes throughout their life cycle, it is important that any changes to the system be evaluated with regard to their effect on individuals' privacy. Components must update their PIAs to reflect significant changes to information collection authorities, business processes, or other factors affecting the collection and handling of information in identifiable form.[12] Components should use the IPA process to ascertain whether or not such changes would require a modification to an existing PIA or would require a new PIA.

[11] See Violence Against Women and Department of Justice Reauthorization Act of 2005 § 1174.
[12] See OMB Memorandum, M-03-22, Attachment A, Section II.B.2.

Questions? Contact the Office of Privacy and Civil Liberties

Email: privacy@usdoj.gov
Phone: 202-514-0208
Web Site Link: www.justice.gov/opcl

Definitions

Individual – For purposes of conducting PIAs, it is the Department's policy to define "individual" in this context as any natural person regardless of citizenship status.

Information in Identifiable Form – is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicators, and other descriptors). OMB Memorandum, M-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, Attachment A, Section II.A.2., dated September 26, 2003.

Information Technology – means, as defined in the Clinger-Cohen Act, any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. Id. at Section II.A.3.

National Security System – means, as defined in the Clinger-Cohen Act, an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management. Id. at Section II.A.5.

Personally Identifiable Information – is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII) (April 2010).