United States Department of Justice
Office of Privacy and Civil Liberties (OPCL)

Initial Privacy Assessment (IPA) Instructions & Template

(Revised May 2015)

What is an Initial Privacy Assessment? An Initial Privacy Assessment (IPA) is the first step in a process developed by OPCL to assist DOJ components in the development and use of information systems. Specifically, the IPA is a tool used to facilitate the identification of potential privacy issues; assess whether additional privacy documentation is required; and ultimately, to ensure the Department's compliance with applicable privacy laws and policies.

The IPA asks a series of basic questions, the responses to which are reviewed and assessed by the component to identify privacy concerns that may necessitate changes to the system and to determine whether additional privacy analysis and documentation are required, such as a system of records notice (SORN), a collection notice under the Privacy Act, or a Privacy Impact Assessment (PIA) under the E-Government Act. Once the component has completed and reviewed its responses and made its recommendation[1], the completed IPA shall be sent to OPCL, recommending whether a PIA and/or SORN is required. Once OPCL has received the completed IPA, it will make a final determination whether additional privacy documentation is required. OPCL's final determination will be completed as part of section IV of this template.

When should an IPA be completed? An IPA should be completed at the beginning of development of an information system, before commencement of any testing or piloting. (This applies regardless of whether the system is electronic or contains only records in paper form.) Additionally, an IPA should be completed any time there is a significant change to the information system to determine whether there are any resulting privacy issues.

[1] Please reference the following materials to help you in recommending whether a PIA, SORN, and/or Privacy Act (e)(3) notice is required: DOJ PIA Guidance; OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002" (Sept. 26, 2003), Attachment A, II.B; OMB Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications" (June 25, 2010); Privacy Act of 1974, 5 U.S.C. § 552a(a)(4), definition of "system of records", and 552a(e)(3), Privacy Act notice requirements; and DOJ Overview of the Privacy Act of 1974, available on OPCL's website.

The IPA is designed to be a cross-cutting tool to address the requirements of several different privacy laws and policies. These laws and policies have different scopes of coverage, and each has specific terms and definitions to describe that coverage. In order to ensure the IPA's utility as a cross-cutting tool, especially since it is not limited to the terms or definitions of just one law or policy, the term **information system** as used in the IPA instructions and template refers to: any process of collection, maintenance, use, or dissemination of information, whether performed manually with paper records or electronically through the use of information technology (IT) products or design.

Who should prepare the IPA? The IPA should be written and reviewed at the component level through the coordinated effort by the component's privacy officials (e.g., Senior Component Official for Privacy (SCOP), Privacy Act Officer, and/or Office of General Counsel), IT security staff, and the program-specific office responsible for the system.

Where should the prepared IPA be sent? A copy of the completed IPA should be sent to OPCL via email to ***privacy@usdoj.gov***. (For classified IPAs, please call 202-514-0208 to coordinate delivery to Suite 1000, National Place Bldg., 1331 Pennsylvania Ave., N.W., Washington, DC 20530.)

How is the IPA related to the Certification and Accreditation (C&A) process? If an IT system requires C&A from the Office of the Chief Information Officer, the completed IPA must be uploaded into the C&A Web tool as part of the C&A process, along with any communication of approval (e.g., email, letter) by OPCL. For a system that does not require C&A (such as a minor application running on an already certified and accredited IT system, or a paper-based non-IT system), an IPA still should be completed to determine if a PIA, a SORN, or other related privacy documents are required for the system.

Please prepare the IPA per the guidance provided in the questions on the template below.
(These instructions may be detached before submitting the IPA.)

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

Department of Justice
Initial Privacy Assessment (IPA)

DOJ/OPCL (Rev. 05/2015)

NAME OF INFORMATION SYSTEM:

COMPONENT:

COMPONENT PRIVACY POINT OF CONTACT (POC) Name: Office: Phone: Bldg./Room Number: Email:	**IPA AUTHOR** (if different from POC) Name: Office: Phone: Bldg./Room Number: Email:
SYSTEM MANAGER/OWNER Name: Office: Phone: Bldg./Room Number: Email:	**SENIOR COMPONENT OFFICIAL FOR PRIVACY** (if applicable, or if different from POC) Name: Office: Phone: Bldg./Room Number: Email:

IPA REVIEW SIGNATURES	
SYSTEM MANAGER/OWNER Signature: _____ Date signed: _____ (If signed by System Manager's/Owner's delegate, please identify delegate): Delegate's Name: Office: Phone: Bldg./Room Number: Email:	**SENIOR COMPONENT OFFICIAL FOR PRIVACY (where applicable) OR COMPONENT PRIVACY POINT OF CONTACT** Signature: _____ Date signed: _____ (If signed by SCOP's delegate, please identify delegate): SCOP Delegate's Name: Office: Phone: Bldg./Room Number: Email:

After obtaining all review signatures, please forward the IPA to OPCL and indicate the date forwarded. Unclassified IPAs should be emailed to the OPCL mailbox: privacy@usdoj.gov. (For classified IPAs, please call 202-514-0208 to coordinate delivery to Suite 1000, National Place Bldg., 1331 Pennsylvania Ave., N.W., Washington, DC 20530.)

DATE FORWARDED TO OPCL: _____

Note: Completion of an IPA marks the beginning of DOJ's privacy compliance processes. The IPA process is not finished until the component completes the IPA and OPCL has reviewed it as to the necessity for any further privacy documentation. The component shall upload the completed IPA template, with section IV completed indicating OPCL's review and approval, into CSAM if necessary.

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

I. DESCRIPTION OF THE INFORMATION SYSTEM

1. Provide a description of the information system that details: (a) the purpose that the records and/or system are designed to serve; (b) the way the system operates to achieve the purpose(s); (c) the type of information collected, maintained, used, or disseminated by the system; (d) who has access to information in the system; (e) how information in the system is retrieved by the user; (f) how information is transmitted to and from the system; (g) the size of the system (e.g., major, minor, parent, child) and any interconnections with other systems; (h) is this system a third-party system or social media web service (provide details).

   (A COMPREHENSIVE RESPONSE TO THIS QUESTION IS IMPERATIVE; PLEASE USE AS MUCH SPACE AS IS NEEDED TO PROVIDE A CLEAR AND FULL RESPONSE.)

2. Which of the following describes the type of information in the system:

   ___ Electronic only. ___ Combination paper/electronic. ___ Paper only.

3. Is there a Certification & Accreditation record within C&A Web?

   _____ Yes. If yes, please indicate the following:

   Confidentiality: ___Low ___Moderate ___High ___Undefined

   Integrity: ___Low ___Moderate ___High ___Undefined

   Availability: ___Low ___Moderate ___High ___Undefined

   _____ No. If no, please identify the FISMA-reportable system, the C&A for which, covers this system.

   _____ Do not know.

   _____ Not applicable - this system is only paper based.

4. Is this a national security system?

   _____ No. _____ Yes. _____ Do not know.

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

5. Does the system collect, maintain, use, or disseminate any information about individuals?

   (When responding to questions in the IPA that include the term "individual," please use the common dictionary definition for that term (i.e., a human being or natural person). While the term "individual" sometimes has a more limited meaning in certain laws and policies, at this early stage of analyzing the information system, OPCL is interested in understanding whether any information concerning a human being or natural person is at issue.)

   _____ No. If no, briefly describe below the information collected, maintained, or disseminated by the system.

   [If you checked no, STOP here after providing the requested description. No further responses are required for sections I and II. Fill out section III below and submit this IPA to DOJ OPCL after obtaining all review signatures on page 1.]

   _____ Yes. If yes, briefly describe below the types of information about individuals in the system, the particular sensitivity of the information, and the reasons why the information is being collected.

   After providing the requested description, proceed to the next question.

6. Please indicate if any of the following characteristics apply to the information in the system about individuals: (Check all that apply.)

   _____ The information directly identifies specific individuals.

   _____ The information is intended to be used, in conjunction with other data elements, to indirectly identify specific individuals.

   _____ The information can be used to distinguish or trace an individual's identity (i.e., it is linked or linkable to specific individuals).

   If you marked any of the above, proceed to the next question.

   _____ None of the above. If none of the above, describe below why the information does not identify specific individuals, or how it is intended to be used, such that it will not indirectly identify specific individuals? **[If you checked this item, STOP here after providing the requested description. No further responses are required for sections I and II. Fill out section III below and submit this IPA to DOJ OPCL after obtaining all review signatures on page 1.]**

[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

7. Does the identifiable information in the system pertain only to government employees, contractors, or consultants?

   _____ No. If no, briefly describe below the types of individuals whose information is being collected, and the general scope of the number of individuals whose information may be collected (e.g., members of the general public, individuals associated with investigations, etc.).

   _____ Yes.

8. Is information about United States citizens or lawfully admitted permanent resident aliens retrieved from the system by a personal identifier?

   _____ No. If no, skip to question I. 11.

   _____ Yes. If yes, first describe below how information is retrieved by a personal identifier (e.g., by name), and then proceed to the next question.

9. Is there an existing Privacy Act system of records notice (SORN) that has been published in the Federal Register to cover this system? (Please consult with your component's SCOP, Privacy Act officer, General Counsel, or OPCL if assistance is needed in responding to this question.)

   _____ No.

   _____ Yes. If yes, provide below the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system.

10. Does the system collect any information directly from United States citizens or lawfully admitted permanent resident aliens who are the subjects of the information?

    _____ No.

    _____ Yes. If yes, are subjects of information from whom the information is directly collected provided a written Privacy Act (e)(3) statement (either on the collection form or via a separate notice)? (An (e)(3) statement indicates: (I) the authority for collection of the information; (ii) whether submission of the information is mandatory or voluntary; (iii) the principal purpose(s) for which the information will be used; (iv) the applicable routine uses; and (v) the effects on the individual, if any, of not providing the information.)

        _____ Yes. If yes, provide links to, or attach copies of, any such forms or notices.
        _____ No.

11. Are Social Security Numbers (SSNs) collected, maintained or disseminated by the system?

_____ No. If no, skip to question I.13.
_____ Yes. If yes, could the program that this system supports operate without SSNs?

_____ Yes.

_____ No. If no, explain why below.

12. Does the system provide any special protection to SSNs (e.g., SSNs are encrypted, only available to certain users, hidden from all users via a look-up table, only in partial form)?

_____ No.

_____ Yes. If yes, describe any special protection provided.

13. Has a security risk assessment been completed for this system?

_____ No.

_____ Yes.

Whether yes or no, briefly describe below any security controls, auditing procedures, and training that have been identified and implemented in order to secure information in the system (e.g., physical and electronic access controls; authentication; encryption; system-specific training for employees).

14. Is the system operated by a contractor?

_____ No.

_____ Yes. If yes, and it is determined that the system is covered by the Privacy Act, then the component must ensure that the contract includes language set forth in the Federal Acquisition Regulation, see 48 C.F.R. 24.104 and 52.224-1 to -2, applying the Privacy Act's provisions to the system.

15. Status of system:

_____ This is a new system in development. **[If you checked this block, STOP here. No further responses are required for this section and section II. Fill out section III and submit this IPA to DOJ OPCL after obtaining all review signatures on page 1.]**

_____ This is an existing system. Please continue with section II.

II. EXISTING SYSTEMS

1. What this system developed prior to April 17, 2003?

   ____ No. If no, indicate the approximate date the system was first developed, and proceed to question II.3.

   ____ Yes. If yes, proceed to question II.2

2. Has the system undergone any significant changes since April 17, 2003?

   _____ No. If no, skip to question II.5.

   _____ Yes. If yes, explain the nature of those changes. After providing the requested explanation, proceed to the next question.

3. Do the changes to the system involve a change in the type of records maintained, the individuals on whom records are maintained, or the use or dissemination of information from the system?

   _____ No. _____ Yes.

4. Please indicate if any of the following changes to the system have occurred:
   (Check all that apply.)

   _____ A conversion from paper-based records to an electronic system.

   _____ A change from information in a format that is anonymous or nonidentifiable to a format that is identifiable to particular individuals.

   _____ A new use of an IT system, including application of a new technology, that changes how information in identifiable form is managed. (For example, a change that would create a more open environment and/or avenue for exposure of data that previously did not exist.)

   _____ A change that results in information in identifiable form being merged, centralized, or matched with other databases.

   _____ A new method of authenticating the use of and access to information in identifiable form by members of the public.

   _____ A systematic incorporation of databases of information in identifiable form purchased or obtained from commercial or public sources.

   _____ A new interagency use or shared agency function that results in new uses or exchanges of information in identifiable form.

   _____ A change that results in a new use or disclosure of information in identifiable form.

_____ A change that results in new items of information in identifiable form being added into the system.

5. Does a PIA for this system already exist?

_____ No.

_____ Yes. If yes:

a. Provide the date and title of the PIA and whether the PIA is posted on the web (and if so, include the link):
b. Has the system undergone any significant changes since the PIA was last published?
____ No.
____ Yes. If yes, please describe here.

III. COMPONENT RECOMMENDATION

A. Privacy Impact Assessment (PIA) Analysis:

___ No PIA required:

___ No "information in identifiable form" (IIF)[2] is collected, maintained, or disseminated by the system.
___ Internal government operations.
___ Legacy system with no changes creating new privacy risks.
___ Other – see other section 208 exceptions to conducting a PIA[3]. (*Please describe here what exception applies to this system).*

___ PIA required: System collects, maintains, or disseminates IIF using IT and no section 208 exceptions apply. [Note: indicate whether it is national security system, excepted by E-Govt. Act, but which requires a PIA per DOJ policy]

Provide description of IIF in system.

___ Adapted PIA required: The component's use of a social media web service/application triggers the adapted PIA requirement in OMB Memorandum M-10-23 because it '*make[s] PII available*'[4] to the component.

___ The Department-wide PIA for Third-Party Social Web Services covers this use of the social web service and no new PIA is required.

---

[2] Refer to DOJ PIA Guidance for definitions of IIF.
[3] Refer to OMB Memorandum M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002", Attachment A.II, for a description of section 208 exceptions for conducting a PIA.
[4] Refer to OMB Memorandum M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications", and DOJ PIA Guidance, for a definition of "make[s] PII available".

___ The Department-wide PIA for Third-Party Social Web Services does not cover this use of the social web service and a new PIA is required.[5]

B. Privacy Act Analysis:

___ System of Records Notice is required:

___ SORN exists (*If yes, provide here the system name and number, as well as the Federal Register citation(s) for the most recent complete notice and any subsequent notices reflecting amendment to the system*):

___ SORN covers this system and no modification is required

___ SORN covers this system but modifications are required (*state here reason why modifications would be required*)

___ SORN does not exist and needs to be drafted.

___ No System of Records Notice is required (*state here reason why no SORN is required*).

C. Other Privacy and Civil Liberties Issues to Consider (e.g., 552a(e)(3) notice requirement; third-party website privacy notice – see section 4(c) of OMB M-10-23)

Description of issue and recommended actions to be taken.

D. Component Summary Recommendation:

1. PIA required: [Yes/No]

Provide any reasons for recommendation.

2. SORN required: [Yes/No]
   a. If yes, a current SORN covers the use of this system? [Yes/No].
   b. If yes, current SORN modifications are required [Yes/No].
   c. If yes, a new SORN is required? [Yes/No].

Provide any reasons for recommendation.

[After obtaining all review signatures on page 1, the IPA template should be submitted to DOJ OPCL.]

[5] See DOJ PIA Guidance for completing an adapted PIA.

IV. OPCL FINAL DETERMINATION (*TO BE COMPLETED BY OPCL ATTORNEY*)

___ OPCL concurs with the component's recommendation. See above.
___ OPCL modifies the component's recommendation. See below.

A. PIA required: [Yes/No]

OPCL determination.

B. SORN required: [Yes/No]

OPCL determination.

____ Other privacy and civil liberties issues to be addressed (e.g., 552a(e)(3) notice required).

Description of issue and recommended actions to be taken.

OPCL reviewer/attorney: _____

Date signed: _____