

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



**Initial Privacy Assessment (IPA)
Instructions & Template
(Revised July 2023)**

What is an Initial Privacy Assessment? An Initial Privacy Assessment (IPA) is the first step in a process to identify potential privacy issues and mitigate privacy risks. The IPA asks basic questions to help Components assess whether additional privacy protections may be needed in designing or implementing a project¹, and whether compliance work may be needed, for example, whether a Privacy Act System of Records Notice (SORN) or an E-Government Act Privacy Impact Assessment (PIA) is required, and/or whether an information collection triggers Paperwork Reduction Act requirements. Before completing an IPA, the Component’s Senior Component Official for Privacy (SCOP) or designee should discuss the project and whether an IPA needs to be drafted with the Component’s assigned OPCL attorney-advisor.

When should an IPA be completed? An IPA should be completed as early as possible during the design and development of, or any significant modification to, a project in which the Department may, create, collect, use, process, store, maintain, disseminate, disclose, or dispose of personally identifiable information (PII). If the project will involve procuring technology, the IPA should be completed as requirements are being developed for the procurement to ensure that privacy requirements are identified in the solicitation and the costs of implementing privacy requirements are reflected in the contract offers. An IPA must be completed when (1) required by DOJ policy or procedures;² or (2) otherwise directed by the CPCLO, OPCL, or your Component’s SCOP.

Who should prepare the IPA? The IPA should be prepared by the SCOP, together with, as appropriate, the Component’s Office of General Counsel, information systems managers, IT security staff, and the program-specific office responsible for the system. A full list of Component SCOPs can be found on the DOJ intranet at: <https://dojnet.doj.gov/privacy/scop.php>.

Send the IPA to: privacy.compliance@usdoj.gov, with a copy to the Component’s assigned attorney-advisor. (For classified IPAs, please call 202-514-0208 to coordinate.)

¹ The term “project” is used to scope the activities (e.g., creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, or disposing of information) covered by an IPA. A project is intended to be technology-neutral, and may include an information system, a digital service, an information technology, a combination thereof, or some other activity that may create potential privacy issues or privacy risks that would benefit from an IPA. The scope of a project covered by an IPA is discretionary, but components should work with their SCOP and OPCL attorney advisor to ensure that the scope of the IPA meets the compliance and risk management needs of the component. Depending on the information practices, components may find it beneficial to split projects into distinct sets, completing multiple IPAs.

² See e.g., *DOJ Security and Privacy Assessment and Authorization Handbook*, version 9 (requiring an IPA for an information system seeking an “Authorization to Operate,” and that creates, collects, uses, processes, stores, maintains, disseminates, discloses, and/or disposes of personally identifiable information); DOJ Instruction 0300.02.01, *Social Media Account Management and Approval* (Feb. 2018) (requiring an IPA prior to creating an approved DOJ social media account).



[INSERT CLASSIFICATION/CONTROL MARKINGS, IF APPROPRIATE]

Department of Justice
Initial Privacy Assessment (IPA)

DOJ/OPCL (Rev. 07/2023)

NAME OF PROJECT:
COMPONENT:
DATE SUBMITTED TO OPCL:

COMPONENT PRIVACY POINT OF CONTACT (POC) Name: Title: Office: Phone: Bldg./Room Number: Email:	INFORMATION SYSTEM SECURITY OFFICER (applicable if different from POC) Name: Title: Office: Phone: Bldg./Room Number: Email:
PROJECT MANAGER/OWNER Name: Title: Office: Phone: Bldg./Room Number: Email:	SENIOR COMPONENT OFFICIAL FOR PRIVACY (if applicable, or if different from POC) Name: Title: Office: Phone: Bldg./Room Number: Email:

IPA REVIEW SIGNATURES	
PROJECT MANAGER/OWNER Signature and date:  <hr/> (If signed by Project 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 and date:  <hr/> (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.compliance@usdoj.gov. (For classified IPAs, please call 202-514-0208 to coordinate delivery.)

Note: Submission of this IPA is only part of DOJ's privacy compliance processes. The IPA process is not complete until a) the Component completes the IPA; b) OPCL has reviewed it as to the necessity for any further privacy work (such as expanded responses, enhanced security controls, or others); and c) OPCL has completed its Final Determination.

Upon completion, the Component shall upload the completed IPA, including the Final Determination indicating OPCL's review and approval, into the Joint Cybersecurity Assessment and Management System (JCAM) tool if necessary.

I. DESCRIPTION OF THE INFORMATION SYSTEM, INFORMATION TECHNOLOGY, DIGITAL SERVICE, OR OTHER PROJECT

1. Provide an overview of the project, explaining the information lifecycle, as the Department creates, collects, uses, processes, stores, maintains, disseminates, discloses, and/or disposes of information in accordance with applicable requirements. If this IPA addresses a significant change to an existing project, please describe the types of changes being implemented and the purpose for those changes. If you select multiple categories below, be sure to provide an overview that addresses any distinctions. Please discuss each of the following:
 - a. Federal law and Federal Government policy create distinct obligations depending on how the Department creates, collects, uses, processes, stores, maintains, disseminates, discloses, and disposes of information. Please select the category (or categories) that best describes your project:
 - (i) Procuring, implementing, developing, or modifying an existing, “information system,”³ as defined in 44 U.S.C. § 3502;⁴
 - (ii) This information system is classified as a “national security system,” as defined at 40 U.S.C. § 11103(a);⁵
 - (iii) Procuring, implementing, developing, or modifying an existing, “information technology,”⁶ as defined in 40 U.S.C. § 11101;⁷
 - (iv) Procuring, implementing, developing, or modifying an existing, or utilizing a third-party “digital service,” as defined by Office of Management and Budget (OMB) Memorandum M-17-06;⁸
 - (v) Procuring, implementing, developing, or modifying an existing, “collection of information,” as defined in 44 U.S.C. § 3502;⁹ or
 - (vi) Other or unknown (please describe in Question I.1.e)

³ While similar, “information system” and “information technology” are separately defined under federal law and may trigger separate privacy risks and compliance obligations. Generally speaking, an “information system” describes a discrete set of information resources organized for the collection, maintenance, use, and dissemination of information.

⁴ <https://www.gpo.gov/fdsys/granule/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapI-sec3502>.

⁵ <https://www.gpo.gov/fdsys/granule/USCODE-2011-title40/USCODE-2011-title40-subtitleIII-chap111-sec11103>.

⁶ One such information resource that makes up an information system is an “information technology,” for example, a computer responsible for the automatic processing of the information within the information system.

⁷ <https://www.gpo.gov/fdsys/granule/USCODE-2011-title40/USCODE-2011-title40-subtitleIII-chap111-sec11101>.

⁸ See OMB Memorandum 17-06, 3, available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-06.pdf (“digital services are defined . . . as online information resources or services” that “provide government information or services to the public or a specific user group across a variety of delivery platforms and devices and support the proper performance of an agency function.”); see also *id.* at 3, n. 4 (“Digital services include the delivery of digital information (i.e., data or content) and transactional services (e.g., online forms, benefits applications) across a variety of platforms, devices, and delivery mechanisms (e.g., websites, mobile applications, and social media)”).

⁹ <https://www.gpo.gov/fdsys/granule/USCODE-2011-title44/USCODE-2011-title44-chap35-subchapI-sec3502>.

- b. the legal authority, or authorities, that authorizes the project:
 - c. the overall purpose that the information and/or project are designed to serve and a high-level explanation of how the project achieves that purpose:
 - d. whether the information is electronic, in hard copy, or both:
 - e. at a high-level, the general types of information collected, maintained, used, or disseminated as part of the project (specific details will be requested below):
 - f. the types of users with access to information, e.g., internal DOJ, other Federal Government users, State or local government users, foreign authorities, or members of the public:
 - g. if this is a significant change to an existing project, describe the types of changes being implemented and their purpose:
 - h. whether, and to what extent, DOJ contractors will be creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information:
2. Does the project create, collect, use, process, store, maintain, disseminate, disclose, or dispose of any “information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other information that is linked or linkable to a specific individual,” i.e., personally identifiable information (PII)?¹⁰

¹⁰ For purposes of this IPA, please use this definition, which is the definition of PII set forth in OMB Circular A-130. See Circular A-130, at ¶ 57, page 33. OPCL views this definition as essentially the same, in practice, as the definition in the E-Government Act of information in “identifiable form”: any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. See Section 208(d) of the E-Government Act of 2002. Also, please use the common dictionary definition of “individual,” i.e., natural person. However, please answer these questions as to small businesses -- those with 5 or fewer individuals involved -- as the information could be personally identifiable in context, e.g., a sole proprietorship or small partnership. Please also consider whether the information of users or administrators may be implicated in this project.

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. Submit this IPA to DOJ OPCL after obtaining all review signatures on page 1.]

Yes. If yes, please identify whether this system will collect, handle, disseminate, store and/or access any of the information in Column (1). If yes, please check all that apply in Column (2) and indicate in Columns (3)(a)-(d) to whom the information relates.

General Categories of Information that May be Personally Identifiable

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public – U.S. Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
<i>Example: Personal contact information, e.g., email address, phone number, home address</i>	X	C & D	<i>Email addresses of members of the public (U.S. or non-USPERs).</i>
Name:			
Business contact information, e.g., email address, phone number, address of a business:			
Personal contact information, e.g., email address, phone number, home address:			
Other personal information, e.g., date of birth or age, place of birth, gender, race, religion, education or employment information, military service information:			
Social Security number (full or truncated):			
Government assigned identifiers, e.g., tax identification number, driver’s license, alien registration number, passport number:			
Vehicle identifiers, e.g., VIN, license plate number:			
Health information or records, e.g., medical notes, disability, accommodations:			
Financial information, e.g., financial accounts, credit card information, income, debts, taxpayer information:			

(1) General Categories of Information that May Be Personally Identifiable	(2) Information is collected, processed, disseminated, stored and/or accessed by this information technology (please check each applicable row)	(3) The information relates to: A. DOJ/Component Employees, Contractors, and Detailees; B. Other Federal Government Personnel; C. Members of the Public – U.S. Citizens or Lawful Permanent Residents (USPERs); D. Members of the Public - Non-USPERs	(4) Comments
Employment performance or disciplinary information, e.g., performance improvement plan, warnings, or reprimands:			
Electronic device identifiers, e.g., mobile devices:			
Criminal records information or civil law enforcement information, e.g., criminal history, arrests, allegations of violation of civil laws such as tax evasion or fraud:			
Information related to or compiled for grand jury, criminal prosecution or civil litigation or administrative proceedings:			
Photos, videos, voice recording, or biometrics, e.g., fingerprints, palm prints, facial recognition:			
System admin/audit data, e.g., user ID, passwords, IP address, date/time of access:			
Other categories of PII:			

II. INFORMATION SYSTEM ASSESSMENT

Complete this section only if your project will implement/develop, or modify an existing, “information system,” as selected in Question I.1.a., above. You may need to consult with the Information System Security Officer or Program Manager/Owner.

- Has any system that is part of the project completed a Certification and Accreditation (C&A) or received an Authorization to Operate (ATO)?

No. If no, please indicate reason; if ATO is pending, please provide anticipated completion date:

Yes. If yes, please provide the name of the IT system under which the certified/re-certified ATO was granted and the date of the ATO expiration:

2. What is, or are the anticipated Federal Information Processing Standards (FIPS) security categorization(s), as defined in FIPS Publication 199, Standards for Security Categorization of Federal Information and Information Systems, for the highest sensitivity information contained on this system?¹¹

Low.¹²

Moderate.¹³

High.¹⁴

a. Will the anticipated FIPS security categorization of the system match the security categorization of the most sensitive information in the system, per the “high water mark” standard?¹⁵

Yes.

No. If no, explain below and state the anticipated categorization of the system:

III. SOCIAL SECURITY NUMBER ASSESSMENT

Complete this section only if your project will collect Social Security numbers (SSNs), full or truncated, as indicated in the chart in Question I.2 above.

1. For what purpose(s) will you be collecting and using Social Security Numbers (SSNs)?

2. Could the project operate without collecting or using SSNs?

Yes.

No. If no, explain why below:

¹¹ See <https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf>.

¹² A low system is defined in FIPS 199 as one from which the unauthorized disclosure of information could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.

¹³ A moderate system is defined in FIPS 199 as one from which the unauthorized disclosure of information could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.

¹⁴ A high system is defined in FIPS 199 as one from which the unauthorized disclosure of information could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

¹⁵ As articulated in FIPS 199: “Determining the security category of an information system requires slightly more analysis and must consider the security categories of all information types on the information system. For an information system, the potential impact values assigned to the respective security objectives (confidentiality, integrity, availability) shall be the highest values (i.e., high water mark) from among those security categories that have been determined for each type of information resident on the information system.”

3. Does the project 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. If no, please explain why special protections are not being implemented:

Yes. If yes, describe any special protection provided:

IV. PRIVACY IMPACT ASSESSMENTS

Complete this section only if your project will develop or maintain an information technology, as selected in Question I.1.a., above:

1. Was the information technology developed prior to April 17, 2003?

Yes.

No.

Comments:

2. Does a privacy impact assessment (PIA) for this information technology already exist?

No. If no, please explain why a PIA has not been created (e.g., an omission, or the system was developed prior to April 17, 2003, and no significant changes have occurred since that time that would have triggered a PIA):

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? 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 information technology.

- A change from information in a format that is anonymous or non-identifiable to a format that is identifiable to particular individuals.
- A new use of an information technology, including application of a new technology that changes how PII is managed. (For example, a change that would create a more open environment and/or avenue for exposure of information that previously did not exist.)
- A change that results in PII being merged, centralized, or matched with other databases.
- A new method of authenticating the use of and access to PII by members of the public.
- A systematic incorporation of databases of PII purchased or obtained from commercial or public sources.
- A new interagency use or shared agency function that results in new uses or exchanges of PII.
- A change that results in a new use or disclosure of PII.
- A change that results in new items of PII being added into the information technology.
- Other changes that may raise significant privacy concerns (**please describe**):

- No, the information technology has not undergone any significant changes since the PIA was last published.

V. PRIVACY ACT ASSESSMENTS

1. Please indicate if the information identified in the chart in Question I.2, above, meets the following criteria to be classified as a “records” under the Privacy Act:
 - Maintained by the Department;
 - Maintained as an item, collection, or grouping of information about a United States citizens or lawfully admitted permanent resident aliens about whom the record pertains; and
 - Contains the United States citizen’s or lawfully admitted permanent resident alien’s name, or the identifying number, symbol, or other identifying particular assigned to the individual (e.g., a finger or voice print or a photograph).

Comments:

[If you did not check all of the boxes, STOP here. No further responses are required for section V. Move on to Section VI below.]

2. Are these records maintained in a “system of records” (e.g., are the records about United States citizens or lawfully admitted permanent resident aliens retrieved, in practice, by a personal identifier)?

No.

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

3. Is there an existing Privacy Act System of Records Notice (SORN) that has been published in the *Federal Register* to cover this system of records?

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 **(please describe)**.

VI. INFORMATION COLLECTION REQUIREMENTS

1. Will information be collected through or on any type of form or series of questions, either electronically (e.g., web form or questionnaire, or mobile application) or in hard copy?

No.

Yes. If yes, please explain:

- a) If yes, does the form have, or do you expect the form to need, an OMB control number pursuant to the Paperwork Reduction Act (PRA)?

No.

Yes. If yes, please identify the OMB control number and its date of expiration:

VII. DIGITAL SERVICES ASSESSMENT

Complete this section only if your project will implement/develop, modify an existing, or utilize a third-party, “digital service,” as selected in Question I.1.a., above,¹⁶ and if this service will be used to implement the principles of the *Open Government Directive* or engage with the public.¹⁷

1. Have you published a privacy policy for each digital service?

Yes.

No.

2. Has the provider of the digital service provided a privacy policy?¹⁸

No.

Yes.

a) If yes, please attach or provide a link to the most recent¹⁹ provider’s privacy policy:

b) If yes, do you have a Privacy Notice²⁰ on each third-party website or application?

¹⁶ See OMB Memorandum 17-06, 3, available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2017/m-17-06.pdf (“digital services are defined . . . as online information resources or services” that “provide government information or services to the public or a specific user group across a variety of delivery platforms and devices and support the proper performance of an agency function.”); see also *id.* at 3, n. 4 (“Digital services include the delivery of digital information (i.e., data or content) and transactional services (e.g., online forms, benefits applications) across a variety of platforms, devices, and delivery mechanisms (e.g., websites, mobile applications, and social media”); OMB Memorandum 10-23, 8, available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2010/m10-23.pdf (“The term ‘third-party websites or applications’ refers to web-based technologies that are not exclusively operated or controlled by a government entity, or web-based technologies that involve significant participation of a nongovernment entity. Often these technologies are located on a ‘.com’ website or other location that is not part of an official government domain. However, third-party applications can also be embedded or incorporated on an agency’s official website.”)

¹⁷ This section does not need to be completed if this service is used for only internal agency activities, or to activities that are part of authorized law enforcement, national security, or intelligence activities.

¹⁸ See OMB Memorandum 10-23, 8, available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2010/m10-23.pdf (“Before an agency uses any third-party website or application to engage with the public, the agency should examine the third party’s privacy policy to evaluate the risks and determine whether the website or application is appropriate for the agency’s use.”).

¹⁹ See OMB Memorandum 10-23, 8, available at https://www.whitehouse.gov/wp-content/uploads/legacy_drupal_files/omb/memoranda/2010/m10-23.pdf (“[T]he agency should monitor any changes to the third party’s privacy policy and periodically reassess the risks.”).

²⁰ See OMB Memorandum 10-23, 6, available at https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf (“To the extent feasible, an agency should post a Privacy Notice, described [in more detail in OMB Memorandum 10-23], on the third-party website or application itself.”).

No. If not, explain why it is not feasible to do so:

Yes. If so, please attach or paste that Privacy Notice here (**please add notice**):

3. Does this project involve a third-party website or online service directed to individuals under the age of thirteen, or involve an operator that has actual knowledge that it is collecting personal information from an individual under the age of thirteen?²¹

No.

Yes.

a. If yes, does the operator provide notice on its website of what information is collected from children by the operator, how the operator uses such information, and the operator's disclosure practices for such information?²²

b. If yes, does the operator obtain verifiable parental consent for the collection, use, or disclosure of personal information from children?²³

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

²¹ If personally identifiable information of children (persons under the age of thirteen) is collected, the Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6501-6505 (COPPA) may apply, and further analysis of certain privacy policies and statements is required.

²² See 15 U.S.C. § 6502(b)(1)(A).

²³ See *id.*