Guide to Effective
Privacy Impact Assessments (PIA)

U.S. Department of Commerce

December 2023

Table of Contents

1. Introduction

Section 208(b) of the E-Government Act of 2002 and subsequent guidance[1] from the Office of Management and Budget (OMB) requires all federal agencies to conduct Privacy Impact Assessments (PIA) for any new or substantially changed information technology that creates, collects, stores, maintains, disseminates, discloses, or disposes of personally identifiable information (PII), or any electronic information collection of PII initiated under the Paperwork Reduction Act (PRA).[2]

PIAs ensure that agencies consider the privacy implications of the technologies they intend to use or modify and incorporate appropriate privacy protections when designing, developing, and deploying them. The PIA serves as both an analysis and a formal document detailing the process and outcome of the analysis.[3] PIAs are to be drafted in plain language and must be posted on the agency's website. The publication of PIAs allows the public to understand what agencies are doing with the PII collected and how the PII is protected.

This guide provides a framework for conducting PIAs at the Department of Commerce (Department) and a methodology for assessing how PII is to be managed in electronic information systems. The Department Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) requires that all PIAs at the Department be conducted in accordance with this guidance.

2. PIA Overview

A PIA is an analysis of how information is handled to: i) ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy; ii) determine the risks and effects of creating, collecting, using, processing, storing, maintaining, disseminating, disclosing, and disposing of information in identifiable form[4] in an electronic information system; and iii) examine and evaluate protections and alternate processes for handling information to mitigate potential privacy concerns. A privacy impact assessment is both an analysis and a formal document detailing the process and the outcome of the analysis.[5]

---

[1] OMB Memorandum (M) 03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, issued on September 26, 2003, and OMB Circular A-130, *Managing Information as a Strategic Resource*, issued on July 28, 2016.

[2] Exceptions apply. See Appendix I for a list of exceptions and work with your BCPO to determine if a particular system is exempt from the PIA requirement under the Department policy.

[3] OMB Circular A-130, *Managing Federal Information as a Strategic Resource*, July 28, 2016, Appendix II, section e. "Privacy Impact Assessments."

[4] While Section 208 of the E-Government Act of 2002 refers to "information in identifiable form" when outlining the requirements for conducting a PIA, subsequent implementing guidance from OMB refers to the broader and more widely accepted "PII." At the Department, PIAs are conducted for systems which process both PII and "Business Identifiable Information" (BII).

[5] OMB Circular A-130, Appendix II.

2.1 Purpose and Goals of the PIA

PIAs have three primary goals:

- To identify risks and impacts associated with processing of PII and BII through information technology;
- To evaluate protections provided by the program or system, including controls implemented, design and process decisions made, and other mitigations for identified risks associated with the system; and
- To provide notice to the public about the Department's collection and processing of PII and BII as it relates to specific information technology.

The SAOP/CPO is responsible for reviewing and approving all PIAs in accordance with guidance set forth by OMB. Approved and signed PIAs are a pre-requisite for issuance of a new or renewed Authority-to-Operate (ATO) for information systems at the Department. PIAs are subject to annual review and re-certification by the SAOP. The SAOP/CPO delegates authority to the Bureau Chief Privacy Officers (BCPOs) for the re-certification process (Appendix A: Privacy Bulletin #002, FY 2024) and to conduct Compliance Review Board (CRB) meetings for Low PII Confidentiality Impact Level systems (Appendix B: Privacy Bulletin #003, FY 2024).

2.2 Information Types Necessitating a PIA

At the DOC, PIAs are conducted on information technology that collects and processes both PII and/or Business Identifiable Information (BII).

Personally Identifiable Information (PII) is defined by OMB as "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."[6] Further, OMB has concluded that "the definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual."[7] Examples of PII include:

- Identifying numbers: SSN (including truncated form), driver's license or state identification number, passport number, Alien Registration Number, financial account number, etc.
- General personal data: Name, age, gender, race/ethnicity, citizenship, home address, date of birth, place of birth, education, medical information, religion, military service, etc.
- Work-related data: Occupation, job title, work address, salary, work history, employment performance ratings or other performance information, procurement/contracting records, etc.
- Biometrics: Fingerprints, palm prints, photographs, scars, marks, tattoos, voice recordings, video recordings, hair and eye color, height, weight, DNA sample or profile, dental profile, etc.
- System Administration/Audit Data: User identification, Internet Protocol (IP) address, data/time of access, queries run, etc.

[6] OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016.
[7] OMB M-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010.

Business Identifiable Information (BII) is defined as information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person and privileged or confidential." Commercial or financial information is considered confidential if disclosure is likely to cause substantial harm to the competitive position of the person from whom the information was obtained. Examples of BII include:

- Financial information provided in response to requests for economic census data.
- Business plans and marketing data provided to participate in trade development events.
- Commercial and financial information collected as part of export enforcement actions.
- Proprietary information provided in support of a grant application or related to a federal acquisition action.
- Financial records collected as part of an investigation.

2.3 When to Conduct a PIA

As outlined above, a PIA must be conducted when:

- Developing or procuring any new IT or systems that collect or process[8] PII or BII;
- Initiating, consistent with the PRA, a new electronic collection of information involving the PII of 10 or more persons – excluding agencies, instrumentalities, or employees of the federal government).

Additionally, a PIA must be updated when modifying a system, IT, or an information collection in a way that changes how PII or BII is collected or processed, including changes to business processes, information collection authorities, or other affecting the collection and handling of PII and BII. Finally, a PIA should be updated, or a new PIA conducted where IT, a system, or information collection change creates new privacy risks. Table 1 below outlines common IT or system changes that may create new privacy risks:

TABLE 1

System Change	Description	Example(s)
Conversion	Converting paper-based records to electronic systems.	*See description.*
Anonymous to Non-Anonymous	When functions applied to an existing information collection change anonymous information into directly identifiable PII.	*See description.*
Significant System Management Changes	When new uses of an existing IT system, including application of new technologies, significantly change how PII or BII is managed in the system.	*An agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.*
Significant Merging	When agencies adopt or alter business processes so that government databases holding PII or BII are merged, centralized, matched with	*Databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.*

[8] Process means the creation, collection, storage, maintenance, dissemination, disclosure, or disposal of PII. See also OMB-M-10-23 which requires agencies conduct modified PIAs whenever an agency's use of a third-party website or application (as defined by the memo) "makes PII available to the agency."

System Change	Description	Example(s)
	other databases or otherwise significantly manipulated.	
New Public Access	When user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public.	*See description.*
Commercial Sources	When agencies systematically incorporate into existing information systems databases of PII or BII purchased or obtained from commercial or public sources.[9]	*See description.*
New Interagency Uses	When agencies work together on shared functions involving significant new uses or exchanges of PII or BII, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA.	*The DOC, the lead agency for the Census Decennial, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. The DEPARTMENTwould thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross-agency IT investment.*
Internal Flow or Collection	When alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional PII or BII.	*Agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for PII or BII could warrant examination of privacy issues.*
Alteration of Character of Data	When new PII or BII added to a collection raises the risks to personal privacy.	*The addition of health or financial information.*

2.4 PIA Requirements

In accordance with guidance set forth by OMB, PIAs must analyze and describe, at a minimum,[10] the following facts about information systems, information technology or information collections involving the collection or processing of PII or BII:

- what information is to be collected (e.g., nature and source);
- why the information is being collected (e.g., to determine eligibility);
- intended use of the information (e.g., to verify existing data);
- with whom the information will be shared (e.g., another agency for a specified programmatic purpose);

[9] Note that, per guidance set forth in OMB-M-03-22, merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement.

[10] See also, OMB-10-23, Guidance for Agency Use of Third-Party Websites and Applications, June 25, 2010, which outlines minimum requirements and a modified template for PIAs conducted on third-party applications and social media websites leveraged by Federal agencies to communicate, engage, and interact with the public.

- what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
- how the information will be secured (e.g., administrative and technological controls); and
- whether a system of records, as defined by the Privacy Act of 1974.[11]

2.5 Making PIAs Available to the Public

In accordance with the Section 208 of the E-Government Act of 2002 and OMB guidance, agencies must make PIAs available for public review on their public website. The Department makes PIAs available for review on its website, https://www.commerce.gov/privacy. In addition, members of the public can view the Department's PIA and Privacy Threshold Analysis (PTA) templates, PIA Annual Certification Form, and learn more about how PIAs are conducted at the DOC. Agencies may determine not to make a PIA publicly available when publication would raise security concerns, reveal classified (i.e., national security) information, or reveal sensitive information (e.g., potentially damaging to a national interest, law enforcement effort, or competitive business interest).

3. The Privacy Impact Assessment (PIA) Process

PIAs serve as both an analysis and a formal document detailing the process and outcome of the analysis. Thus, the most effective PIAs are those that are conducted in parallel to the design, development, or acquisition of an information system, technology, or information collection. PIAs present an opportunity for system developers, contracting officials, program managers, and other staff and officials responsible for a system or project to consider privacy implications and compliance obligations early in the project and consider alternative, less privacy-intrusive practices during development, instead of retrospectively, reducing cost and potential deployment delays.

In general, the PIA process[12] is as follows:

1) The System Owner (SO)/Information System Security Officer (ISSO) completes PTA.
2) If the PTA determines a PIA is not required, SO/ISSO sends the PTA to the BCPO (Bureau Chief Privacy Officer) or designee for inclusion into the Assessment and Authorization (A&A) package. Otherwise, if the PTA determines a PIA is required, SO/ISSO completes PIA, PIA Annual Certification Form if the re-certification process is used, or the Controls Assessment Worksheet if a Compliance Review Board (CRB) meeting is needed and submits to BCPO/designee.
3) Once approved by the BCPO/designee, the BCPO/designee submits the PTA, PIA, and certification form or Controls Assessment Worksheet to the SAOP/CPO at CPO@doc.gov for review.
4) The Departmental Privacy Team will confirm if a CRB meeting is required or if the re-certification process can be used.
5) The CRB meeting is held with BCPO, ISSO, SO, Information Technology Security Officer (ITSO), Privacy Act Officer (PAO), and/or Authorizing Official (AO) if required.
6) Once the privacy compliance documentation is reviewed by the Departmental Privacy Team, it is submitted to the SAOP/CPO for review and approval.

[11] The Privacy Act of 1974, As Amended, 5 U.S.C. 552a
[12] Exceptions may apply – all systems and projects are unique.

7) Once approved by the SAOP/CPO, the PTA and PIA are posted on website at www.commerce.gov/privacy and the BCPO/designee will receive the approved PIA.
8) Monitor the system for changes which create new privacy risks and conduct a new PTA, as necessary.
9) Maintain compliance by completing the annual review process for the PIA, as applicable.

The following sections further detail the steps required for completion and approval of a PIA at the Department.

3.1 Conducting a Privacy Threshold Analysis (PTA)

The first step in the PIA process is conducting a Privacy Threshold Analysis (PTA). A PTA is used to determine if an information system contains PII and/or BII, and whether a PIA is required, a new or modified System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system.[13] A PTA is required for every information system, but not every information system will require completion of a PIA. The current template version (01-2024) of the PTA (Appendix C) must be completed and certified.

3.2 Content of the PTA

Each PTA consists of:

1) A description of the information system and its purpose;
2) A set questions and sub-questions outlining the nature and content of the information system; and
3) A set of signatures indicating review and approval of the:
    a. ISSO or SO
    b. ITSO
    c. PAO
    d. AO
    e. BCPO

Table 2 below outlines the individual sections and questions, and a description of its content.

TABLE 2

Section/Question	Description
Unique Project Identifier	The unique project identifier assigned to the information system or project.
Introduction: Description of the information system and its purpose	a) Whether the information system is a general support system (GSS), a major application, or other type of system as defined in NIST SP 800-37 and OMB Circular A-130. *Identify whether the system is a General Support System (GSS), a Major Application, or some other designation (child system, minor child, third-party service provider, etc.).* b) Where the system is physically located. *Identify the physical location of the servers which house or process the information, and/or the location where physical (hard copies) of information are stored or maintained. Where Cloud Service Providers (CSP) are leveraged, please indicate as appropriate.* *c)* Whether it is a standalone system or interconnects with other systems, including identifying and describing any other systems

[13] NIST Special Publication 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII), April 2010 (available at: http://csrc.nist.gov/publications/nistpubs/800-122/sp800-122.pdf).

Section/Question	Description
	to which it interconnects. *Identify whether the system is standalone or relies on or connects to other systems and include a discussion of: i) what those other systems' names and primary function(s) are; and ii) how and for what purpose the system connects to those other systems. Please note that this question is not intended to address applications which reside on the GSS for which a separate PIA already exists.* d) The purpose of the system. *State the general purposes of the system.* e) The way the system operates to achieve the stated purpose. *Provide a high level, typical "transaction" for the system – focusing on end-user interaction and/or lifecycle of information in the system – from initial collection through use, sharing, and retention or disposal.* f) A general description of the type of information collected, maintained, used, or disseminated by the information system. *Provide an overall description of the type of information collected, maintained, used, or disseminated by the information system.* g) Individuals who have access to information on the system. *Identify the types of users who have access to the information on the system.* *h)* How information in the system is retrieved by the user. *Identify how information is pulled, queried, or otherwise accessed by system users (which may include other systems if an interconnection exists). Where applicable, describe how any automated retrieval works.* *i)* How information is transmitted to and from the system. *Identify methods of intake for the system, including any web or physical forms, oral, mail, or telephone intake of information for the system, whether information is input directly by a user or captured from another system via automated processes. Identify any processes whereby information is transmitted from the system either back to an individual to whom the information pertains via mail, fax, telephone, or via automated processes to another system.* NOTE: If a PIA is required, the responses to: Introduction (a) must be the same in the PIA; Introduction (b) must be the same in the PIA; Introduction (c) must be the same in the PIA; Introduction (e) must be the same in Introduction (d) of the PIA; Introduction (h) must be the same in Introduction (e) of the PIA; and Introduction (i) must be the same in Introduction (f) of the PIA.
1a) What is the status of this information system?	Outlines whether the system is: a) New b) Existing with changes that create new privacy risks and identifies the changes which create new privacy risks[14] (where applicable). c) Existing with changes that do not create new privacy risks and a SAOP approved PIA does not exist. d) Existing with changes that do not create new privacy risks and a SAOP approved PIA exists.

[14] Table 1 of Section 2.3 of this guide.

Section/Question	Description
	NOTE: The response to this question must be the same as Section 1.1 of the PIA, if a PIA is required.
1b) Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?	This IT checklist must be completed for Information Technology (IT) acquisitions within the Department. Completion of this checklist is not required for the acquisition of equipment for specialized Research and Development (R&D) or scientific purposes that are not a National Security System.
2) Is the IT system or its information used to support any activity which may raise privacy concerns?	Identifies whether the system supports activities that raise privacy concerns, as outlined in NIST 800-53, Rev 4, Appendix J. Such activities are those that may not include the collection and use of PII, but still raise privacy concerns – such as audio recordings, video surveillance, building entry readers, and electronic purchase transactions. NOTE: The response to this question must be the same as Section 3.1 of the PIA, if a PIA is required.
3) Does the IT system collect, maintain or disseminate Business Identifiable Information (BII)?	Identifies whether the system processes BII as defined in this guide.
4a) Does the IT system collect, maintain, or disseminate PII?	Identifies whether the system processes PII as defined by OMB and in this guide, and if so; a) to whom the PII pertains (e.g. employees, contractors, or members of the public); b) whether the PII includes SSNs; c) whether PII processed includes information other than system user IDs; and d) whether the PII processed (and the purpose for which it is processed) necessitates a higher PII confidentiality impact level,[15] (e.g. law enforcement, benefits administration, etc.). NOTE: If a PIA is required, the responses to: question 4a must coincide with Sections 2.1 and 5.1 (to whom the PII pertains) of the PIA; 4b must coincide with Section 2.1 (Identifying Numbers) of the PIA; and 4c must coincide with Section 2.1 of the PIA.
4b) Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?	
4c) Does the IT system collect, maintain, or disseminate PII other than user ID?	
4d) Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?	
Certification	Certifies whether the system necessitates a PIA in accordance with answers provided to the questions in the PTA and the guidance set forth in this document. It also documents concurrence of ISSO/SO, ITSO, PAO, AO, and BCPO for the information system. The name, office, phone number, and email address must be completed, along with the signature of the ISSO/SO, ITSO, PAO, AO, and BCPO. All signatures must be received.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a PIA must be completed for the information system. The PTA and the SAOP approved PIA must be a part of the system's Assessment and Authorization (A&A) Package.

3.3 Conducting the PIA

When it has been determined that a PIA is required, the current usable template version 01-2020 (Appendix D) or template version 01-2019 (Appendix E) of the PIA must be completed and fully signed. Remember that PIAs are made publicly available. As such, they should be clear, unambiguous, and understandable to

[15] See NIST 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information.

the general public. The length and breadth of a PIA will vary according to the size and complexity of the information system. In general, please adhere to the following guidelines when drafting responses to the questions posed in the PIA template:

- Use plain language and consider the perspective of a member of the public who is unfamiliar with the information system or technology.
- Spell out each acronym in the first instance it is used 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 public.
- Include the complete name of the reference when first referencing NIST or OMB publications and other documents. The abbreviated format may be used for subsequent references.

3.4 Content of the PIA

Each PIA consists of:

1) A description of the information system and its purpose;
2) A set of questions and sub-questions outlining the nature and content of the system, identified privacy risks and mitigations, and associated compliance; and
3) Certification signatures indicating review and approval of the:
    a. ISSO/SO
    b. ITSO
    c. PAO
    d. AO
    e. BCPO

Table 3 below outlines the individual sections and questions, a description of its content, and guidance on addressing the question.

TABLE 3

Section/Question	Description and Guidance
Unique Project Identifier	The unique project identifier assigned to the information system or project.
Introduction	
(a) Whether it is a general support system, major application, or other type of system.	Identify whether the system is a General Support System (GSS), a Major Application, or some other designation (child system, minor child, third-party service provider, etc.). NOTE: The response must be the same as Introduction (a) of the PTA.
(b) System location	Identify the physical location of the servers which house or process the information, and/or the location where physical (hard copies) of information are stored or maintained. Where Cloud Service Providers (CSP) are leveraged, please indicate as appropriate. NOTE: The response must be the same as Introduction (b) of the PTA.

Section/Question	Description and Guidance
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)	Identify whether the system is standalone or relies on or connects to other systems and include a discussion of i) what those other systems' names and primary function(s) are; and ii) how and for what purpose the system connects to those other systems. Please note that this question is not intended to address applications which reside on the GSS for which a separate PIA already exists. NOTE: The response must be the same as Introduction (c) of the PTA.
(d) The way the system operates to achieve the purpose(s) identified in Section 4	Provide a high level, typical "transaction" for the system – focusing on end-user interaction and/or lifecycle of information in the system – from initial collection through use, sharing, and retention or disposal. NOTE: The response must be the same as Introduction (e) of the PTA.
(e) How information in the system is retrieved by the user	Identify how information is pulled, queried, or otherwise accessed by system users (which may include other systems if an interconnection exists). Where applicable, describe how any automated retrieval works. NOTE: The response must be the same as Introduction (h) of the PTA.
(f) How information is transmitted to and from the system	Identify methods of intake for the system, including any web or physical forms, oral, mail, or telephone intake of information for the system, whether information is input directly by a user or captured from another system via automated processes. Identify any processes whereby information is transmitted from the system either back to an individual to whom the information pertains via mail, fax, telephone, or via automated processes to another system. NOTE: The response must be the same as Introduction (i) of the PTA.
(g) Any information sharing conducted by the system	Discuss any sharing of information by the system, either through manual processes or automated means.
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information	Cite the specific legal authorities which allow for the collection and use of information in the system or operation of the system. Please note that OMB guidance and the Privacy Act of 1974 are not acceptable statutes which authorize the collection or processing of PII. If unsure, the PAO should work with the Bureau Chief Counsel to identify relevant authorities.
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system	Identify the FIPS 199 security categorization assigned to the information system – "High," "Moderate," or "Low."
1. Status of the Information System	
1.1) Indicate whether the information system is a new or existing system.	Identify whether the information system is: a) New b) Existing with changes that create new privacy risks and identifies the changes which create new privacy risks[16] (where applicable). c) Existing with changes that do not create new privacy risks and a SAOP approved PIA does not exist. d) Existing with changes that do not create new privacy risks and a SAOP approved PIA exists. NOTE: The response must be the same as Question 1 of the PTA. Table 1 of this PIA guide provides additional information and examples for each type of change.

[16] Table 1 of Section 2.3 of this guide.

Section/Question	Description and Guidance
2. Information in the System	
2.1) Indicate what PII/BII is collected, maintained, or disseminated.	Identify all PII/BII types using the checkboxes provided. Where a certain PII or BII type processed by the system is not presented, indicate using the "other" box for each sub-category. The sub-categories are: Identifying Numbers; General Personal Data; Work-Related Data; Distinguishing Features/Biometrics; System Administration/Audit Data; and Other Information.
2.2) Indicate sources of the PII/BII in the system.	Identify from whom the PII/BII is collected and the method of collection. Please note, for systems with a web-collection or similar input, select "online." Additionally, note that the question is seeking who or what entity is providing the information, not the association of the individual to whom the information pertains to an entity. For example, an information system that receives a monthly upload from another Federal agency system which contains PII about that agency's employees would have the box for "Other Federal Agencies" checked, whereas a system that received that same monthly update by asking employees to enter their own information in the information system through a web form would have "Online" selected under "Directly from Individual about Whom the Information Pertains."
2.3) Describe how the accuracy of information in the system is ensured.	Discuss how PII/BII will be collected (directly from individuals or from a third-party); by what mechanism (paper form, web or electronic form, telephonically, etc.); what opportunities exist for individuals to amend or correct information in the system; whether information is verified and if so by what means (manual checks, automated checks or other technical means, etc.); what level of data quality is necessary; and what processes will exist to ensure data quality.
2.4) Is the information covered by the Paperwork Reduction Act?	Identify any information in the system which is covered by the Paperwork Reduction Act (PRA) and, where applicable, provide the OMB control number and the agency number associated with the collection of that information.
2.5) Indicate the technologies used that contain PII/BII in ways that have not been previously deployed.	Identify any technologies which use or contain PII/BII which have not been previously deployed relative to the system (rather than the organization or Federal government at large), or, if not applicable, select "There are not any technologies used that contain PII/BII in ways that have not been previously deployed."
3. System Supported Activities	
3.1) Indicate IT system supported activities which raise privacy risks/concerns.	Identifies whether the system supports activities that raise privacy concerns, as outlined in NIST 800-53, Rev 4, Appendix J. Such activities are those that may not include the collection and use of PII, but still raise privacy concerns – such as audio recordings, video surveillance, building entry readers, and electronic purchase transactions. NOTE: The response must be the same as Question 2 of the PTA.
4. Purpose of the System	
4.1) Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated.	Identify the primary and any secondary purposes PII/BII in the system will be used for. Please note common, routine uses, such as disclosure to law enforcement or similar related to a breach of the system do not need to be selected, unless the activities are unique to the system.
5. Use of the Information	
5.1) In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained,	For each purpose identified in Section 4.1 of the PIA, describe how the PII/BII that is identified in Section 2.1 of the PIA will be used and identify the population to whom the information pertains – generally (e.g. The Department employees and contractors, Federal employees and contractors, members of the public, foreign nationals, visitors, etc.). Example: *Visitors to the HCHB provide their name, a driver's license, and the name of their point of contact when scheduling a visit to the HCHB. This information is*

Section/Question	Description and Guidance
or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).	*used by the HCHB physical security team to ensure physical security of the HCHB and Department employees. The name and driver's license information are used to establish identity of the visitor and the name of the point of contact is used to identify a Department employee responsible for the visitor and validate the visitor's stated purpose of visit.*
5.2) Describe any potential threats to privacy as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)	Identify potential threats to privacy posed by the use of information in the system and controls implemented, design or business process decisions made, or other actions taken to mitigate the risk. Please note **ALL** systems which process PII/BII implicate some element of risk, such as insider threat. PIAs should document that risk and the actions taken to reduce or eliminate the risk. Do not answer this section with not-applicable or "no risk." Consider the following Fair Information Practice Principles (FIPPs) when thinking about privacy risks associated with data usage: Risks related to Purpose Specification: Specifically articulate the authority that permits collection and use of PII and specify this authority and use at the time of collection. Limit subsequent uses of the data to the original purpose for which it was collected or other purposes compatible with the original collection purpose. Risks related to Use Limitation: PII should not be disclosed, made available, or otherwise used for purposes other than those specified except (a) with the consent of the individual or (b) by the authority of law. Risks related to Collection Limitation/Data Minimization: PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose. Risks Related to Data Quality and Integrity: PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up-to-date. Risks related to Data Security: Agencies should institute reasonable security safeguards to protect PII against loss, unauthorized access, destruction, misuse, modification, or disclosure. Risks related to Accountability and Auditing: Agency personnel and contractors are accountable for complying with measures implementing the FIPPs, for providing training to all employees and contractors who use PII, and for auditing the actual use and storage of PII.
6. Information Sharing and Access	
6.1) Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared.	Identify entities which the system may share information with, or which information from the system may be shared with, as well as the mechanism(s) by which information will be shared. Remember to include other systems which the system may connect to for the purpose of sharing information. Ensure the answer aligns with statements made about interconnections in the System Description (c) and information sharing conducted by the system in the System Description (g) of the PIA. Case-by-Case: Manual processes to include physical, oral, email, etc. to include small numbers of records or individual data. Bulk Transfer: Automated or semi-automated processes, or those which involve connections between two (2) systems or large transfers of data between the system and recipient(s). Direct Access: System credentials or access granted, or data made available through open, or public means.

Section/Question	Description and Guidance
	If PII/BII will not be shared, indicate by checking the "PII/BII will not be shared" box. Please note that the intent of this question is not to cover routine, common uses, such as sharing as a result of a breach or incident involving the system, etc.
6.2) Does the Department bureau/operating unit (BOU) place a limitation on re-dissemination of PII/BII shared with external agencies/entities?	Describe any limitations that may be placed on external agencies to further share the information provided by the Department bureau/operating unit. In some cases, the external agency may have a duty to share the information.
6.3) Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.	Indicate whether the system connects with or receives information from other IT systems, both internal and external to the Department. Provide the name of the technology or system and the purpose for the interconnections. Describe the technical controls in place to prevent PII/BII leakage. Ensure the answer aligns with statements made about interconnections in the System Description (c) of the PIA.
6.4) Identify the class of users who will have access to the IT system and the PII/BII.	Identify all types of individuals who will have access to the system or information maintained by the system – i.e. have an account, or general, open access in the case of a publicly available, open system.
7. Notice and Consent	
7.1) Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system.	Identify the mechanisms by which notice is provided to individuals whose PII/BII is collected or processed. Where applicable, indicate if a Privacy Act System of Records Notice (SORN) for the system has been published in the Federal Register and whether a Privacy Act (§ e(3)) Statement is provided at the point of collection from the individual to whom the information pertains. If so, cite the location where the Privacy Act Statement can be viewed. In cases where no Privacy Act Statement is necessary or available, provide the location where a Privacy Policy can be viewed. Indicate and describe any additional or other notice provided or made available to individuals regarding collection and use of their information. If no notice is provided or if notice is not provided directly to individuals to whom the information pertains, explain why.
7.2) Indicate whether and how individuals have an opportunity to decline to provide PII/BII.	Indicate whether individuals may decline to provide PII/BII and describe how they may do so, including how notice of this ability is provided and the consequences of not providing PII or BII.
7.3) Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.	Indicate whether individuals may consent to uses of PII/BII and describe how they may do so, including how notice of this ability is provided and any consequences associated with not consenting to particular uses of PII/BII.
7.4) Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.	Indicate whether individuals may request or receive access to, amend, or correct information about them in the system. Identify the process for individuals to make such corrections or requests for corrections and how notice of this process is made available to individuals. In cases where the system is a Privacy Act System of

Section/Question	Description and Guidance
	Records, cite the applicable Privacy Act/FOIA regulations and procedures for accessing records.
8. Administrative and Technological Controls	
8.1) Indicate the administrative and technological controls for the system.	Check all applicable controls for the system. Remember to include an explanation if access to the PII/BII is being monitored, tracked, or recorded, if applicable, and provide the date of the most recent Assessment and Authorization if an existing information system. If needed, work with the Contracting Officer's Representative or Contracting Officer in reference to requirements in contracts.
8.2 – Provide a general description of the technologies used to protect PII/BII on the IT system.	To the greatest extent possible, outline the technologies and technical controls in place to protect PII/BII on the system. To reduce risk to the security posture of the system, do not identify specific appliances, software, etc. Provide the encryption standard for PII/BII at rest and in transit (where applicable). Refer to NIST SP 800-122 controls for protecting the confidentiality of PII for applicable controls. NOTE: The BCPO is responsible for reviewing the system's security assessments and determining if there are risks found.
9. Privacy Act	
9.1) Is the PII/BII searchable by a personal identifier (e.g., name or SSN?	Indicate whether the PII/BII is searchable by a personal identifier, which may be an individual's name or some identifying number, symbol, or other identifying particular assigned to an individual.
9.2) Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a.	Indicate whether the system, as used, constitutes a "System of Records" as defined in the Privacy Act of 1974, as amended. Generally, this is triggered by the retrieval of records by a personal identifier, such as a name or other identifying number or symbol. Where a System of Records is implicated, identify whether a System of Records Notice (SORN) exists to cover the system and provide a reference to the SORN (name, number and hyperlink). If not, indicate that the system does not constitute a System of Records OR a System of Records Notice is currently in development/has been submitted.
10. Retention of Information	
10.1) Indicate whether these records are covered by an approved records control schedule and monitored for compliance.	All Federal records must be scheduled for retention and disposal in accordance with the Federal Records Act. Indicate whether records in the system are covered by an existing approved records control schedule and provide the name and number of the applicable schedule. If an approved records control schedule does not exist, indicate the status of a proposed schedule for the records. Indicate whether the system monitors for compliance with the schedule. If compliance is not monitored, explain why not.
10.2) Indicate the disposal method of the PII/BII.	Identify the mechanism or method by which PII/BII in the system is disposed of or destroyed in accordance with the applicable records schedule and in accordance with the Department policy.
11. NIST Special Publication (SP) 800-122 PII Confidentiality Impact Level	
11.1) Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed.	Identify the confidentiality impact level (Low, Moderate, or High) of PII in the system in accordance with guidance set forth in NIST SP 800-122. It is important to remember that the PII Confidentiality Impact Level is **not the same** as the Federal Information Processing Standards (FIPS) 199 security impact category for the system. When evaluating and assigning a level, only consider the impact on individuals and the organization caused by a loss of confidentiality of PII/BII in the system.
11.2) Indicate which factors were used to determine the above PII confidentiality impact level.	Identify the factors used to determine the impact from a loss of confidentiality, integrity, or availability of PII taken into account: Identifiability; Quantity of PII; Data Field Sensitivity; Context of Use; Obligation to Protect Confidentiality; and Access to and Location of PII.
12. Analysis	

Section/Question	Description and Guidance
12.1) Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy.	Identify potential threats to privacy that exist in light of the information collected or the sources or from whom/where the information in the system is obtained/collected. Identify any controls implemented, design or business process decisions made, or other actions taken to mitigate the risk. For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why. Please note **ALL** systems which process PII/BII implicate some element of risk. PIAs should document that risk and the actions taken to reduce or eliminate the risk. Do not answer this section with not-applicable or "no risk." Consider the following Fair Information Practice Principles (FIPPs) when thinking about privacy risks associated with data usage: Risks related to Openness/Transparency: To the extent feasible, agencies should be open about developments, practices, and policies with respect to the collection, use, dissemination, and maintenance of PII. Agencies should publish information about policies in this area, including the privacy policy, and contact information for data corrections and complaints, as well as System of Records Notices, PIAs, and other similar notice documentation. Individual Participation: To the extent practicable, involve the individual in the process of using PII and seek individual consent for the collection, use, dissemination, and maintenance of PII. Agencies should also provide mechanisms for appropriate access, correction, and redress regarding the agency's use of PII. Risks related to Collection Limitation/Data Minimization: PII should be collected only if the data is directly relevant and necessary to accomplish the specified purpose. PII should be obtained by lawful and fair means and retained only as long as is necessary to fulfill the specified purpose. Risks Related to Data Quality and Integrity: PII collected should be relevant to the purposes identified for its use and should be accurate, complete, and up-to-date.
12.2) Indicate whether the conduct of this PIA results in any required business process changes.	Indicate whether the conduct of the PIA resulted in any business process changes related to system use or business process around information collection, use, disposal, or disclosure as it relates to the system. Discuss any business process changes. Example: *As a result of conducting the PIA, Customer Service Representatives will now verify contact information with subject individuals telephonically prior to updating a record.*
12.3) Indicate whether the conduct of this PIA results in any required technology changes.	Indicate whether the conduct of the PIA resulted system or technology changes that altered how information is collected, used, disclosed, maintained, or otherwise processed by the system. Discuss any technology changes. Example: *After conducting the PIA, new User Role types were defined and created to ensure a separation of duties and ensure need to know amongst Customer Service Representatives, Call Center Contact Representatives, and System Administrators.*
Points of Contact and Signatures	Identifies the points of contact for the information system and documents concurrence of each contact (SO/ISSO, ITSO, PAO, AO, and BCPO). The name, office, phone number, and email address must be completed, along with the signature of the ISSO/SO, ITSO, PAO, AO, and BCPO. All signatures must be received.

3.5 Conducting the Controls Assessment

For a new system processing PII/BII, an existing system with changes that create new privacy risks, and an existing PII processing system without a current SAOP approved PIA, a Controls Assessment Worksheet (Appendix F) must be completed and approved by the bureau's Chief Information Officer. The Controls Assessment identifies the status of the security and privacy controls applicable to the PII Confidentiality Impact Level.

3.6 Content of the Controls Assessment

The steps for completion of the Controls Assessment Worksheet are:

1. Identify the name of PII/BII processing system in row 1.
2. In CELL D2, select the applicable NIST SP 800-122 PII Confidentiality Impact Level for the system from the drop-down menu. The applicable NIST SP 800-122 PII Confidentiality Impact Level can be found in Section 11.1 of the PIA.
3. Using the Filter functions for the "Low," "Moderate," and "High" columns, filter for "X" for the applicable PII Confidentiality Impact Level. (For "High" PII Confidentiality Impact Level systems, also include * and -- for additional relevant controls).
4. After filtering, assess each control and document the current implementation status by selecting from the drop-down menu under COLUMN H, System Implementation.
5. For any controls other than "Implemented," include a brief explanation in the "Notes and Findings" (COLUMN I).

3.7 Conducting the PIA Compliance Review Board (CRB) Meeting

The BCPO must submit the privacy compliance documentation (PTA, PIA, and Controls Assessment Worksheet) to the SAOP/CPO at CPO@doc.gov at least 60 days in advance of the ATO (new PII/BII processing system) or ATO expiration date (existing PII/BII processing system without a current SAOP approved PIA or existing PII/BII processing system and there are changes which create new privacy risks in which a CRB meeting is required). The SAOP conducts the PIA CRB meeting with the BCPO, ISSO, SO, ITSO, PAO, and/or AO to discuss system/data characterization, information sharing practices, website/mobile application processes, privacy controls, and risk assessments. The PIA CRB Risk Analysis Guide (Appendix G) outlines the critical areas discussed during a CRB meeting. A CRB meeting must be conducted at least once every three (3) years.

The SAOP/CPO has delegated authority to the BCPOs to conduct CRB meetings for Low PII Confidentiality Impact Level systems (Appendix B: Privacy Bulletin #003, FY 2020).

3.8 Conducting the Annual Review and Certification Process

For existing systems in which there is a current SAOP approved PIA (good for one year only), an annual review must be conducted. The current template version (01-2020) of the PTA (Appendix C) must be completed and certified. If it is determined that there are changes which create new privacy risks, then a CRB meeting must be conducted. If it is determined that there are not any changes which create new privacy risks, the PIA annual certification process can be used, unless it has been more than three (3) years since the last CRB meeting was conducted.

If the PIA annual certification process is used, then the following privacy compliance documentation must be submitted by the SAOP at CPO@doc.gov at least 60 days in advance of the SAOP approved PIA expiration date (if before ATO expiration date or if after ATO expiration date and the certification process will be used):

- PTA – Template version number 01-2020 (Appendix C);
- PIA – Template version number 01-2020 (Appendix D) or template version number 01-2019 (Appendix E) with updates **only** to Section 1.1 (Status of the Information System), Section 6.2 (Limitation on re-dissemination of PII/BII if using template version number 01-2020), Section 8.1 (Administrative and Technological Controls – date of most recent Assessment & Authorization only), and if needed, Sections 12.2 and/or 12.3 (Analysis); and
- PIA Annual Review Certification Form (Appendix H).

The SAOP/CPO has delegated authority to the BCPOs for the re-certification process (Appendix A: Privacy Bulletin #002, FY 2020).

3.9 SAOP Approval of the PIA

During the CRB meeting, SAOP verbal concurrence may be granted if it is determined that there are not any additional privacy risks. If SAOP verbal concurrence is granted, it is contingent upon receipt of the revised privacy compliance documents requested during the CRB meeting. Once the revised documentation is received, it is reviewed by the Deputy Director for Departmental Privacy Operations who will recommend SAOP written approval or return the documentation to the BCPO with comments. Once the approval recommendation is received, the SAOP provides written approval of the PIA. The SAOP approved PIA is sent to the BCPO and posted on the Department's privacy website at www.commerce.gov/privacy within three (3) business days.

When the PIA annual certification process is used, the Departmental Privacy Operations Team reviews the privacy compliance documentation to confirm that there are no changes which create new privacy risks. If there are not any changes which create new privacy risks, the Deputy Director for Departmental Privacy Operations will recommend SAOP written approval. Once the approval recommendation is received, the SAOP provides written approval of the PIA. The SAOP approved PIA is sent to the BCPO and posted on the Department's privacy website at www.commerce.gov/privacy within three (3) business days.

4. Departmental Privacy Contacts

U.S. Department of Commerce
1401 Constitution Avenue, N.W.
Washington, DC 20230

Email: CPO@doc.gov
Telephone: (202) 482-1190
Website Link: www.commerce.gov/privacy

Charles Cutshall
Senior Agency Official for Privacy/Chief Privacy Officer

Tahira Murphy
Deputy Director for Departmental Privacy Operations
Deputy Director for Departmental Privacy Act Operations

Appendix A: Privacy Bulletin #002, FY 2024

_____ 12/23/2024

Approved for Release
Charles Cutshall
Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)

Date

DEPARTMENT OF COMMERCE
OFFICE OF PRIVACY AND OPEN GOVERNMENT

PRIVACY BULLETIN #002, FY 2024

SUBJECT: Delegation of SAOP Concurrence for the Re-issuance of an Authorization to Operate (ATO) for Personally Identifiable Information (PII)/Business Identifiable Information (BII) Processing Systems Eligible for the Re-certification Process

EFFECTIVE DATE: Upon release of this Privacy Bulletin

EXPIRATION DATE: Effective until superseded or revoked

SUPERSEDES: Privacy Bulletin #002, FY 2020

BACKGROUND: Office of Management and Budget (OMB) Memorandum 14-04 and Commerce policy require Senior Agency Official for Privacy (SAOP) approval as a pre-condition for the issuance/re-issuance of an Authorization to Operate (ATO).

PURPOSE: This Bulletin provides the criteria, as well as instruction to the Bureau Chief Privacy Officers (BPCOs) on reviewing and approving Privacy Impact Assessments (PIAs) for PII processing systems which are eligible for the re-certification process.

COVERAGE: This bulletin applies to Bureau Chief Privacy Officers (BCPOs).

PROCEDURE: The responsibilities for key stakeholders are as follows:

1. Bureau Chief Privacy Officers (BCPOs):
   a. Review the bureau/operating unit's PII/BII Processing System Inventory to confirm that the last Compliance Review Board (CRB) meeting was held within three (3) years. If it has been less than three (3) years, continue to follow the instruction below. If it has been more than three (3) years and the PII Confidentiality Impact Level is Moderate or High, submit the privacy compliance documentation to the SAOP at CPO@doc.gov in order for a CRB meeting to be scheduled to be held with the SAOP. Otherwise, if the PII Confidentiality Impact Level is Low, follow the guidance and instruction of Privacy Bulletin #003, FY 2024.

b. Review the Privacy Impact Assessments (PIAs) posted on the the Department Privacy Program web page at www.commerce.gov/privacy to confirm that there is a current SAOP approved PIA (good for one (1) year only) for the information system.
c. Review the Privacy Threshold Analysis (PTA) and updated PIA to confirm that there are not any changes which create new privacy risks and there are not any new collections of PII/BII.
d. Review the PIA Annual Review Certification Form to ensure the appropriate reviews have been conducted by the reviewer, Privacy Act Officer, and BCPO.
e. Complete the BCPO Concurrence of PIA Memorandum (Appendix) and submit it, as well as the PTA, PIA, and PIA Annual Review Certification Form to the SAOP at CPO@doc.gov within three (3) work days of BCPO concurrence of the PIA on behalf of the SAOP.

2. Senior Agency Official for Privacy (SAOP) and Deputy Director for Departmental Privacy Operations:
   a. Review the privacy compliance documentation received.
   b. Ensure posting of the BCPO approved PIA, in addition to the corresponding PTA on the Department's privacy web page at www.commerce.gov/privacy within three (3) business days.
   c. Update the Departmental PII/BII Processing System Inventory.

ACCOUNTABILITY:

- OMB Circular A-130 requires Federal agencies to:
  - Ensure compliance with all applicable statutory, regulatory, and policy requirements and use PIAs and other tools to manage privacy risks;
  - Conduct PIAs in accordance with the E-Government Act and make the PIAs available to the public in accordance with OMB policy;
  - Review authorization packages for information systems that involve PII; and
  - Establish and maintain a privacy continuous monitoring program.
- The PTA and PIA will be published on the Department's privacy web page.

REFERENCES:

- OMB Circular A-130, *Managing Information as a Strategic Resource*
- OMB Memorandum 14-01, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*

PROGRAM CONTACT INFORMATION:

Office of Privacy and Open Government
(202) 482-1190
PrivacyAct@doc.gov

APPENDIX:

MEMORANDUM FOR: Charles Cutshall
Senior Agency Official for Privacy (SAOP) and Chief Privacy Officer (CPO)

FROM: _____
Bureau Chief Privacy Officer (BCPO)

SUBJECT: BCPO Concurrence of Privacy Impact Assessment (PIA) for the Re-certification Process

I certify that the following criteria has been met for _____:
(Name of PII processing system)

- ☐ The PII confidentiality impact level is: ☐ Low ☐ Moderate ☐ High
- ☐ The last Compliance Review Board (CRB) meeting was held on _____.
- ☐ The current SAOP approved PIA expires on _____.
- ☐ There are not any changes which create new privacy risks.
- ☐ There are not any new collections of PII/BII.
- ☐ The following sections of the PIA have been updated accordingly (*check all that apply*):
  - ☐ Section 1.1 (Status of the Information System)
  - ☐ Section 8.1 (Administrative and Technological Controls – most recent Assessment and Authorization date)
  - ☐ Section 12.2 (Analysis - Required Business Process Changes)
  - ☐ Section 12.3 (Analysis – Required Technology Changes)
  - ☐ Current certification signatures on the PTA and PIA.

The following documents are attached (check all that apply):

- ☐ PTA
- ☐ PIA
- ☐ PIA Annual Review Certification Form

Appendix B: Privacy Bulletin #003, FY 2024

_____ 09/28/2020

Approved for Release Date
Charles Cutshall
Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO)

DEPARTMENT OF COMMERCE
OFFICE OF PRIVACY AND OPEN GOVERNMENT

PRIVACY BULLETIN #003, FY2024

SUBJECT: Delegation of SAOP Concurrence for the Re-issuance of an Authorization to Operate (ATO) for Low Personally Identifiable Information (PII) Confidentiality Impact Level Processing Systems

EFFECTIVE DATE: Upon release of this Privacy Bulletin

EXPIRATION DATE: Effective until superseded or revoked

SUPERSEDES: Privacy Bulletin #00, FY2020

BACKGROUND: Office of Management and Budget (OMB) Memorandum 14-04 and Commerce policy require Senior Agency Official for Privacy (SAOP) approval as a pre-condition for the issuance/re-issuance of an Authorization to Operate (ATO).

PURPOSE: This Bulletin provides the criteria, as well as instruction to the Bureau Chief Privacy Officers (BPCOs) on reviewing and approving Privacy Impact Assessments (PIAs) for Low PII Confidentiality Impact Level processing systems that require a Compliance Review Board (CRB) meeting.

COVERAGE: This bulletin applies to Bureau Chief Privacy Officers (BCPOs).

PROCEDURE: The responsibilities for key stakeholders are as follows:

1. Bureau Chief Privacy Officers (BCPOs):
   a. Review the last SAOP approved PIA to confirm that the PII Confidentiality Impact Level was deemed Low.
   b. Review the PTA and PIA to confirm that there are not any new collections of PII/BII which would increase the PII confidentiality impact level to Moderate or High.
   c. If the PII Confidentiality Impact Level is Moderate or High, submit the privacy compliance documentation to the SAOP at CPO@doc.gov in order for a CRB meeting to be scheduled to be held with the SAOP.
   d. Review the bureau/operating unit's PII/BII Processing System Inventory to confirm that the last CRB meeting was held more than three (3) years ago.
   e. Review the Controls Assessment Worksheet to confirm that the appropriate security and privacy controls are in place.

f. Review the Cyber Security Assessment Management (CSAM) tool to confirm that any applicable Plans of Action and Milestones (POA&Ms) are in place.
g. Conduct the CRB meeting with the Information System Security Officer (ISSO), System Owner (SO), Information Technology Security Officer (ITSO), and Privacy Act Officer, in addition to the Approving Official (AO) if needed.
h. Approve the PIA with signature if it has been determined that there are not any additional privacy risks.
i. Complete the BCPO Concurrence of PIA Memorandum (Appendix) and submit it, as well as the PTA, PIA, and Controls Assessment Worksheet to the SAOP at CPO@doc.gov within three (3) work days of BCPO concurrence of the PIA on behalf of the SAOP.

2. Senior Agency Official for Privacy (SAOP) and Deputy Director for Departmental Privacy Operations:
   a. Review the privacy compliance documentation received.
   b. Ensure posting of the BCPO approved PIA, in addition to the corresponding PTA on the Department's privacy web page at www.commerce.gov/privacy within three (3) business days.
   c. Update the Departmental PII/BII Processing System Inventory.

ACCOUNTABILITY:

- OMB Circular A-130 requires Federal agencies to:
  - Ensure compliance with all applicable statutory, regulatory, and policy requirements and use PIAs and other tools to manage privacy risks;
  - Conduct PIAs in accordance with the E-Government Act and make the PIAs available to the public in accordance with OMB policy;
  - Ensure that the design of information collections is consistent with the intended use of the information, and the need for new information is balanced against any privacy risks;
  - Identify privacy control assessment methodologies and metrics;
  - Review authorization packages for information systems that involve PII; and
  - Establish and maintain a privacy continuous monitoring program.
- The PTA and PIA will be published on the Department's privacy web page.

REFERENCES:

- OMB Circular A-130, *Managing Information as a Strategic Resource*
- OMB Memorandum 14-01, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*

PROGRAM CONTACT INFORMATION:

Office of Privacy and Open Government
(202) 482-1190
PrivacyAct@doc.gov

APPENDIX:

MEMORANDUM FOR: Charles Cutshall
Senior Agency Official for Privacy (SAOP) and
Chief Privacy Officer (CPO)

FROM: _____
Bureau Chief Privacy Officer (BCPO)

SUBJECT: BCPO Concurrence of Privacy Impact Assessment (PIA) for Low PII Confidentiality Impact Level PII/BII Processing System

I certify that the following criteria has been met for _____:
(Name of PII processing system)

- ☐ The CRB meeting was held on _____.
- ☐ Date of SAOP concurrence of LOW PII confidentiality impact level: _____.
- ☐ Basis for BCPO exercise of SAOP CRB delegated authority.
  Check one of the following:
  - ☐ There are not any new collections of PII/BII.
  - ☐ There are new collections of PII/BII that do not change the PII confidentiality impact level.
- ☐ The appropriate security and privacy controls are in place and/or there is an approved Plan of Action and Milestones. The date of the annual review was conducted on _____.

The following documents are attached (check all that apply):

- ☐ PTA
- ☐ PIA
- ☐ Controls Assessment Worksheet

Appendix C: Department of Commerce Privacy Threshold Analysis (Template Version Number: 01-2024)

U.S. Department of Commerce
[Bureau Name]

Privacy Threshold Analysis
for the
[IT System Name]

U.S. Department of Commerce Privacy Threshold Analysis

[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: This Privacy Threshold Analysis (PTA) is a questionnaire to assist with determining if a Privacy Impact Assessment (PIA) is necessary for this IT system. This PTA is primarily based from the Office of Management and Budget (OMB) privacy guidance and the Department of Commerce (DOC) IT security/privacy policy. If questions arise or further guidance is needed in order to complete this PTA, please contact your Bureau Chief Privacy Officer (BCPO).

Description of the information system and its purpose: *Provide a general description (in a way that a non-technical person can understand) of the information system that addresses the following elements:*

The E-Government Act of 2002 defines "information system" by reference to the definition section of Title 44 of the United States Code. The following is a summary of the definition: "Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information. See: 44. U.S.C. § 3502(8).

a) Whether it is a general support system, major application, or other type of system
b) System location
c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
d) The purpose that the system is designed to serve
e) The way the system operates to achieve the purpose
f) A general description of the type of information collected, maintained, used, or disseminated by the system
g) Identify individuals who have access to information on the system
h) How information in the system is retrieved by the user
i) How information is transmitted to and from the system

Questionnaire:

1. Status of the Information System

1a. What is the status of this information system?

____ This is a new information system. *Continue to answer questions and complete certification.*

____ This is an existing information system with changes that create new privacy risks. *Complete chart below, continue to answer questions, and complete certification.*

Changes That Create New Privacy Risks (CTCNPR)					
a. Conversions		d. Significant Merging		g. New Interagency Uses	
b. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
c. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment. *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2015 or 01-2017). *Continue to answer questions and complete certification.*

____ This is an existing information system in which changes do not create new privacy risks, and there is a SAOP approved Privacy Impact Assessment (version 01-2019 or later). *Skip questions and complete certification.*

1b. Has an IT Compliance in Acquisitions Checklist been completed with the appropriate signatures?

____ Yes. This is a new information system.

____ Yes. This is an existing information system for which an amended contract is needed.

____ No. The IT Compliance in Acquisitions Checklist is not required for the acquisition of equipment for specialized Research and Development or scientific purposes that are not a National Security System.

____ No. This is not a new information system.

2. Is the IT system or its information used to support any activity which may raise privacy concerns?

NIST Special Publication 800-53 Revision 4, Appendix J, states "Organizations may also engage in activities that do not involve the collection and use of PII but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary." Examples include, but are not limited to, audio recordings, video surveillance, building entry readers, and electronic purchase transactions.

____ Yes. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

____ No.

3. Does the IT system collect, maintain, or disseminate business identifiable information (BII)?

As per DOC Privacy Policy: "For the purpose of this policy, business identifiable information consists of (a) information that is defined in the Freedom of Information Act (FOIA) as "trade secrets and commercial or financial information obtained from a person [that is] privileged or confidential." (5 U.S.C.552(b)(4)). This information is exempt from automatic release under the (b)(4) FOIA exemption. "Commercial" is not confined to records that reveal basic commercial operations" but includes any records [or information] in which the submitter has a commercial interest" and can include information submitted by a nonprofit entity, or (b) commercial or other information that, although it may not be exempt from release under FOIA, is exempt from disclosure by law (e.g., 13 U.S.C.)."

____ Yes, the IT system collects, maintains, or disseminates BII.

____ No, this IT system does not collect any BII.

4. Personally Identifiable Information (PII)

4a. Does the IT system collect, maintain, or disseminate PII?

As per OMB 17-12: "The term PII refers to 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."

____ Yes, the IT system collects, maintains, or disseminates PII about: *(Check all that apply.)*

____ DOC employees
____ Contractors working on behalf of DOC
____ Other Federal Government personnel
____ Members of the public

____ No, this IT system does not collect any PII.

If the answer is "yes" to question 4a, please respond to the following questions.

4b. Does the IT system collect, maintain, or disseminate Social Security numbers (SSNs), including truncated form?

____ Yes, the IT system collects, maintains, or disseminates SSNs, including truncated form.

Provide an explanation for the business need requiring the collection of SSNs, including truncated form.
Provide the legal authority which permits the collection of SSNs, including truncated form.

____ No, the IT system does not collect, maintain, or disseminate SSNs, including truncated form.

4c. Does the IT system collect, maintain, or disseminate PII other than user ID?

____ Yes, the IT system collects, maintains, or disseminates PII other than user ID.

____ No, the user ID is the only PII collected, maintained, or disseminated by the IT system.

4d. Will the purpose for which the PII is collected, stored, used, processed, disclosed, or disseminated (context of use) cause the assignment of a higher PII confidentiality impact level?

Examples of context of use include, but are not limited to, law enforcement investigations, administration of benefits, contagious disease treatments, etc.

____ Yes, the context of use will cause the assignment of a higher PII confidentiality impact level.

____ No, the context of use will not cause the assignment of a higher PII confidentiality impact level.

If any of the answers to questions 2, 3, 4b, 4c, and/or 4d are "Yes," a Privacy Impact Assessment (PIA) must be completed for the IT system. This PTA and the SAOP approved PIA must be a part of the IT system's Assessment and Authorization Package.

CERTIFICATION

_____ I certify the criteria implied by one or more of the questions above **apply** to the [IT SYSTEM NAME] and as a consequence of this applicability, I will perform and document a PIA for this IT system.

_____ I certify the criteria implied by the questions above **do not apply** to the [IT SYSTEM NAME] and as a consequence of this non-applicability, a PIA for this IT system is not necessary.

Information System Security Officer or System Owner Name: Office: Phone: Email: Signature: _____ Date signed: _____	**Information Technology Security Officer** Name: Office: Phone: Email: Signature: _____ Date signed: _____
Privacy Act Officer Name: Office: Phone: Email: Signature: _____ Date signed: _____	**Authorizing Official** Name: Office: Phone: Email: Signature: _____ Date signed: _____
Bureau Chief Privacy Officer Name: Office: Phone: Email: Signature: _____ Date signed: _____	

Appendix D: Department of Commerce Privacy Impact Assessment (Template Version Number: 01-2024)

U.S. Department of Commerce
[Bureau Name]

Privacy Impact Assessment
for the
[IT System Name]

Reviewed by: _____, Bureau Chief Privacy Officer

☐ Concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Non-concurrence of Senior Agency Official for Privacy/DOC Chief Privacy Officer
☐ Concurrence of the BCPO (This is an existing information system that is eligible for an annual certification)

_____

Signature of Senior Agency Official for Privacy/DOC Chief Privacy Officer Date

U.S. Department of Commerce Privacy Impact Assessment
[Name of Bureau/Name of IT System]

Unique Project Identifier: [Number]

Introduction: System Description

Provide a description of the system that addresses the following elements:
The response must be written in plain language and be as comprehensive as necessary to describe the system.

(a) Whether it is a general support system, major application, or other type of system
(b) System location
(c) Whether it is a standalone system or interconnects with other systems (identifying and describing any other systems to which it interconnects)
(d) The way the system operates to achieve the purpose(s) identified in Section 4
(e) How information in the system is retrieved by the user
(f) How information is transmitted to and from the system
(g) Any information sharing conducted by the system
(h) The specific programmatic authorities (statutes or Executive Orders) for collecting, maintaining, using, and disseminating the information
(i) The Federal Information Processing Standards (FIPS) 199 security impact category for the system

Section 1: Status of the Information System

1.1 Indicate whether the information system is a new or existing system.

_____ This is a new information system.
_____ This is an existing information system with changes that create new privacy risks. *(Check all that apply.)*

Changes That Create New Privacy Risks (CTCNPR)					
d. Conversions		d. Significant Merging		h. New Interagency Uses	
e. Anonymous to Non-Anonymous		e. New Public Access		h. Internal Flow or Collection	
f. Significant System Management Changes		f. Commercial Sources		i. Alteration in Character of Data	
j. Other changes that create new privacy risks (specify):					

____ This is an existing information system in which changes do not create new privacy risks, and there is not a SAOP approved Privacy Impact Assessment.

____ This is an existing information system in which changes do not create new privacy

risks, and there is a SAOP approved Privacy Impact Assessment.

____ This is an existing information system that is eligible for an annual certification, in which security and privacy controls are properly implemented, changes do not create new privacy risks and there is a SAOP approved Privacy Impact Assessment.

Section 2: Information in the System

2.1 Indicate what personally identifiable information (PII)/business identifiable information (BII) is collected, maintained, or disseminated. *(Check all that apply.)*

Identifying Numbers (IN)					
a. Social Security*		f. Driver's License		j. Financial Account	
b. Taxpayer ID		g. Passport		k. Financial Transaction	
c. Employer ID		h. Alien Registration		l. Vehicle Identifier	
d. Employee ID		i. Credit Card		m. Medical Record	
e. File/Case ID					
n. Other identifying numbers (specify):					
*Explanation for the business need to collect, maintain, or disseminate the Social Security number, including truncated form:					

General Personal Data (GPD)					
a. Name		h. Date of Birth		o. Financial Information	
b. Maiden Name		i. Place of Birth		p. Medical Information	
c. Alias		j. Home Address		q. Military Service	
d. Gender		k. Telephone Number		r. Criminal Record	
e. Age		l. Email Address		s. Marital Status	
f. Race/Ethnicity		m. Education		t. Mother's Maiden Name	
g. Citizenship		n. Religion			
u. Other general personal data (specify):					

Work-Related Data (WRD)					
a. Occupation		e. Work Email Address		i. Business Associates	
b. Job Title		f. Salary		j. Proprietary or Business Information	
c. Work Address		g. Work History		k. Procurement/contracting records	
d. Work Telephone Number		h. Employment Performance Ratings or other Performance Information			
l. Other work-related data (specify):					

Distinguishing Features/Biometrics (DFB)					
a. Fingerprints		f. Scars, Marks, Tattoos		k. Signatures	

Distinguishing Features/Biometrics (DFB)					
b. Palm Prints		g. Hair Color		l. Vascular Scans	
c. Voice/Audio Recording		h. Eye Color		m. DNA Sample or Profile	
d. Video Recording		i. Height		n. Retina/Iris Scans	
e. Photographs		j. Weight		o. Dental Profile	
p. Other distinguishing features/biometrics (specify):					

System Administration/Audit Data (SAAD)					
a. User ID		c. Date/Time of Access		e. ID Files Accessed	
b. IP Address		f. Queries Run		f. Contents of Files	
g. Other system administration/audit data (specify):					

Other Information (specify)

2.2 Indicate sources of the PII/BII in the system. *(Check all that apply.)*

Directly from Individual about Whom the Information Pertains					
In Person		Hard Copy: Mail/Fax		Online	
Telephone		Email			
Other (specify):					

Government Sources					
Within the Bureau		Other DOC Bureaus		Other Federal Agencies	
State, Local, Tribal		Foreign			
Other (specify):					

Non-government Sources					
Public Organizations		Private Sector		Commercial Data Brokers	
Third Party Website or Application					
Other (specify):					

2.3 Describe how the accuracy of the information in the system is ensured.

2.4 Is the information covered by the Paperwork Reduction Act?

	Yes, the information is covered by the Paperwork Reduction Act. Provide the OMB control number and the agency number for the collection.
	No, the information is not covered by the Paperwork Reduction Act.

2.5 Indicate the technologies used that contain PII/BII in ways that have not been previously deployed. *(Check all that apply.)*

Technologies Used Containing PII/BII Not Previously Deployed (TUCPBNPD)			
Smart Cards		Biometrics	
Caller-ID		Personal Identity Verification (PIV) Cards	
Other (specify):			

	There are not any technologies used that contain PII/BII in ways that have not been previously deployed.

Section 3: System Supported Activities

3.1 Indicate IT system supported activities which raise privacy risks/concerns. *(Check all that apply.)*

Activities			
Audio recordings		Building entry readers	
Video surveillance		Electronic purchase transactions	
Other (specify):			

	There are not any IT system supported activities which raise privacy risks/concerns.

Section 4: Purpose of the System

4.1 Indicate why the PII/BII in the IT system is being collected, maintained, or disseminated. *(Check all that apply.)*

Purpose			
For a Computer Matching Program		For administering human resources programs	
For administrative matters		To promote information sharing initiatives	
For litigation		For criminal law enforcement activities	
For civil enforcement activities		For intelligence activities	
To improve Federal services online		For employee or customer satisfaction	

Purpose			
For web measurement and customization technologies (single-session)		For web measurement and customization technologies (multi-session)	
Other (specify):			

Section 5: Use of the Information

5.1 In the context of functional areas (business processes, missions, operations, etc.) supported by the IT system, describe how the PII/BII that is collected, maintained, or disseminated will be used. Indicate if the PII/BII identified in Section 2.1 of this document is in reference to a federal employee/contractor, member of the public, foreign national, visitor or other (specify).

5.2 Describe any potential threats to privacy, such as insider threat, as a result of the bureau's/operating unit's use of the information, and controls that the bureau/operating unit has put into place to ensure that the information is handled, retained, and disposed appropriately. (For example: mandatory training for system users regarding appropriate handling of information, automatic purging of information in accordance with the retention schedule, etc.)

Section 6: Information Sharing and Access

6.1 Indicate with whom the bureau intends to share the PII/BII in the IT system and how the PII/BII will be shared. *(Check all that apply.)*

Recipient	How Information will be Shared		
	Case-by-Case	Bulk Transfer	Direct Access
Within the bureau			
DOC bureaus			
Federal agencies			
State, local, tribal gov't agencies			
Public			
Private sector			
Foreign governments			
Foreign entities			
Other (specify):			

	The PII/BII in the system will not be shared.

6.2 Does the DOC bureau/operating unit place a limitation on re-dissemination of PII/BII shared with external agencies/entities?

	Yes, the external agency/entity is required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the external agency/entity is not required to verify with the DOC bureau/operating unit before re-dissemination of PII/BII.
	No, the bureau/operating unit does not share PII/BII with external agencies/entities.

6.3 Indicate whether the IT system connects with or receives information from any other IT systems authorized to process PII and/or BII.

	Yes, this IT system connects with or receives information from another IT system(s) authorized to process PII and/or BII. Provide the name of the IT system and describe the technical controls which prevent PII/BII leakage:
	No, this IT system does not connect with or receive information from another IT system(s) authorized to process PII and/or BII.

6.4 Identify the class of users who will have access to the IT system and the PII/BII. *(Check all that apply.)*

Class of Users			
General Public		Government Employees	
Contractors			
Other (specify):			

Section 7: Notice and Consent

7.1 Indicate whether individuals will be notified if their PII/BII is collected, maintained, or disseminated by the system. *(Check all that apply.)*

	Yes, notice is provided pursuant to a system of records notice published in the Federal Register and discussed in Section 9.	
	Yes, notice is provided by a Privacy Act statement and/or privacy policy. The Privacy Act statement and/or privacy policy can be found at: _____.	
	Yes, notice is provided by other means.	Specify how:
	No, notice is not provided.	Specify why not:

7.2 Indicate whether and how individuals have an opportunity to decline to provide PII/BII.

	Yes, individuals have an opportunity to decline to provide PII/BII.	Specify how:
	No, individuals do not have an opportunity to decline to provide PII/BII.	Specify why not:

7.3 Indicate whether and how individuals have an opportunity to consent to particular uses of their PII/BII.

	Yes, individuals have an opportunity to consent to particular uses of their PII/BII.	Specify how:
	No, individuals do not have an opportunity to consent to particular uses of their PII/BII.	Specify why not:

7.4 Indicate whether and how individuals have an opportunity to review/update PII/BII pertaining to them.

	Yes, individuals have an opportunity to	Specify how:

	review/update PII/BII pertaining to them.	
	No, individuals do not have an opportunity to review/update PII/BII pertaining to them.	Specify why not:

Section 8: Administrative and Technological Controls

8.1 Indicate the administrative and technological controls for the system. *(Check all that apply.)*

	All users signed a confidentiality agreement or non-disclosure agreement.
	All users are subject to a Code of Conduct that includes the requirement for confidentiality.
	Staff (employees and contractors) received training on privacy and confidentiality policies and practices.
	Access to the PII/BII is restricted to authorized personnel only.
	Access to the PII/BII is being monitored, tracked, or recorded. Explanation:
	The information is secured in accordance with the Federal Information Security Modernization Act (FISMA) requirements. Provide date of most recent Assessment and Authorization (A&A): _____ ☐ This is a new system. The A&A date will be provided when the A&A package is approved.
	The Federal Information Processing Standard (FIPS) 199 security impact category for this system is a moderate or higher.
	NIST Special Publication (SP) 800-122 and NIST SP 800-53 Revision 4 Appendix J recommended security controls for protecting PII/BII are in place and functioning as intended; or have an approved Plan of Action and Milestones (POA&M).
	A security assessment report has been reviewed for the information system and it has been determined that there are no additional privacy risks.
	Contractors that have access to the system are subject to information security provisions in their contracts required by DOC policy.
	Contracts with customers establish DOC ownership rights over data including PII/BII.
	Acceptance of liability for exposure of PII/BII is clearly defined in agreements with customers.
	Other (specify):

8.2 Provide a general description of the technologies used to protect PII/BII on the IT system. *(Include data encryption in transit and/or at rest, if applicable).*

Section 9: Privacy Act

9.1 Is the PII/BII searchable by a personal identifier (e.g, name or Social Security number)?

____ Yes, the PII/BII is searchable by a personal identifier.

____ No, the PII/BII is not searchable by a personal identifier.

9.2 Indicate whether a system of records is being created under the Privacy Act, 5 U.S.C. § 552a. *(A new system of records notice (SORN) is required if the system is not covered by an existing SORN).*

As per the Privacy Act of 1974, "the term 'system of records' means a group of any records under the control of any 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."

	Yes, this system is covered by an existing system of records notice (SORN). Provide the SORN name, number, and link. *(list all that apply)*:
	Yes, a SORN has been submitted to the Department for approval on (date).
	No, this system is not a system of records and a SORN is not applicable.

Section 10: Retention of Information

10.1 Indicate whether these records are covered by an approved records control schedule and monitored for compliance. *(Check all that apply.)*

	There is an approved record control schedule. Provide the name of the record control schedule:
	No, there is not an approved record control schedule. Provide the stage in which the project is in developing and submitting a records control schedule:
	Yes, retention is monitored for compliance to the schedule.
	No, retention is not monitored for compliance to the schedule. Provide explanation:

10.2 Indicate the disposal method of the PII/BII. *(Check all that apply.)*

Disposal			
Shredding		Overwriting	
Degaussing		Deleting	
Other (specify):			

Section 11: NIST Special Publication 800-122 PII Confidentiality Impact Level

11.1 Indicate the potential impact that could result to the subject individuals and/or the organization if PII were inappropriately accessed, used, or disclosed. *(The PII Confidentiality Impact Level is not the same, and does not have to be the same, as the Federal Information Processing Standards (FIPS) 199 security impact category.)*

	Low – the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
	Moderate – the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
	High – the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.

11.2 Indicate which factors were used to determine the above PII confidentiality impact level. *(Check all that apply.)*

	Identifiability	Provide explanation:
	Quantity of PII	Provide explanation:
	Data Field Sensitivity	Provide explanation:
	Context of Use	Provide explanation:
	Obligation to Protect Confidentiality	Provide explanation:
	Access to and Location of PII	Provide explanation:
	Other:	Provide explanation:

Section 12: Analysis

12.1 Identify and evaluate any potential threats to privacy that exist in light of the information collected or the sources from which the information is collected. Also, describe the choices that the bureau/operating unit made with regard to the type or quantity of information collected and the sources providing the information in order to prevent or mitigate threats to privacy. (For example: If a decision was made to collect less data, include a discussion of this decision; if it is necessary to obtain information from sources other than the individual, explain why.)

12.2 Indicate whether the conduct of this PIA results in any required business process changes.

	Yes, the conduct of this PIA results in required business process changes. Explanation:
	No, the conduct of this PIA does not result in any required business process changes.

12.3 Indicate whether the conduct of this PIA results in any required technology changes.

	Yes, the conduct of this PIA results in required technology changes. Explanation:
	No, the conduct of this PIA does not result in any required technology changes.

Points of Contact and Signatures

Information System Security Officer or System Owner Name: Office: Phone: Email: I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: _____ Date signed: _____	**Information Technology Security Officer** Name: Office: Phone: Email: I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: _____ Date signed: _____
Privacy Act Officer Name: Office: Phone: Email: I certify that the appropriate authorities and SORNs (if applicable) are cited in this PIA. Signature: _____ Date signed: _____	**Authorizing Official** Name: Office: Phone: Email: I certify that this PIA is an accurate representation of the security controls in place to protect PII/BII processed on this IT system. Signature: _____ Date signed: _____
Bureau Chief Privacy Officer Name: Office: Phone: Email: I certify that the PII/BII processed in this IT system is necessary and this PIA ensures compliance with DOC policy to protect privacy. Signature: _____ Date signed: _____	

Appendix E: Controls Assessment Worksheet

Name of PII-Processing System:

800-122 PII Confidentiality Impact Rating:

Control	800-122 Control	800-53 J Control	Low	Moderate	High	Mod to High Jump	System Implementation	Notes and Findings
AC-1			X	X	X			
AC-2			X	X	X			
AC-2(8)				--	--			
AC-2(9)				*	*			
AC-2(13)			X	X	X			
AC-3	X		X	X	X			
AC-3(9)	*			X	X			
AC-3(10)	*			*	*			
AC-4	*			X	X			
AC-4(8)					X	*		
AC-4(12)								
AC-4(15)				X	X			
AC-4(17)				X	X			
AC-4(18)				X	X			
AC-5	X			X	X			
AC-6	X			X	X			
AC-6(1)	*				X	*		
AC-6(2)	*			X	X			
AC-6(3)	*				*			
AC-6(5)	*				X			
AC-6(7)	*		X	X	X			
AC-6(9)	*			X	X			
AC-6(10)	*			X	X			
AC-8				*	*			
AC-11			X	X	X			
AC-12								
AC-14				*	*			
AC-16			X	X	X			
AC-16(3)			X	X	X			
AC-17	X		X	X	X			
AC-17(1)	*		X	X	X			
AC-17(2)	*		X	X	X			

Name of PII-Processing System:

800-122 PII Confidentiality Impact Rating:

Control	800-122 Control	800-53 J Control	Low	Moderate	High	Mod to High Jump	System Implementation	Notes and Findings
AC-18(1)			X	X	X			
AC-19	X		X	X	X			
AC-19(5)	*		X	X	X			
AC-20			X	X	X			
AC-20(1)			X	X	X			
AC-20(3)			X	X	X			
AC-21	X		X	X	X			
AC-22			X	X	X			
AC-23				*	*			
AT-1			X	X	X			
AT-2			X	X	X			
AT-3			X	X	X			
AT-4			X	X	X			
AU-1			X	X	X			
AU-2	X		X	X	X			
AU-3			X	X	X			
AU-4				X	X			
AU-4(1)				*	*			
AU-6	X			X	X			
AU-6(3)	*			X	X			
AU-6(10)	*			X	X			
AU-7			X	X	X			
AU-7(1)				X	X			
AU-7(2)				X	X			
AU-9			X	X	X			
AU-9(3)				X	X			
AU-9(4)				*	*			
AU-10				X	X			
AU-10(1)				X	X			
AU-11(1)				*	*			
AU-12				X	X			
AU-12(3)				X	X			
AU-14				*	*			
AU-14(2)				*	*			
AU-14(3)				*	*			
AU-16(2)								

Name of PII-Processing System:

800-122 PII Confidentiality Impact Rating:

Control	800-122 Control	800-53 J Control	Low	Moderate	High	Mod to High Jump	System Implementation	Notes and Findings
CA-1			X	X	X			
CA-2				X	X			
CA-3				X	X			
CA-3(3)			X	X	X			
CA-3(5)			X	X	X			
CA-6			X	X	X			
CA-7				X	X			
CA-8					X	*		
CA-9				X	X			
CA-9(1)				X	X			
CM-3(6)			X	X	X			
CM-4			X	X	X			
CM-4(1)				X	X			
CM-4(2)				X	X			
CM-8(1)								
CP-1			X	X	X			
CP-2			X	X	X			
CP-2(5)								
CP-2(8)								
CP-4								
CP-7				*	*			
CP-9				X	X			
CP-10				X	X			
IA-2	X		X	X	X			
IA-2(6)	*			X	X			
IA-2(7)	*			X	X			
IA-2(11)	*			X	X			
IA-3								
IA-4			X	X	X			
IA-4(3)				X	X			
IA-5				X	X			
IA-6								
IA-7			X	X	X			
IA-8				X	X			
IR-1			X	X	X			
IR-2			X	X	X			

Name of PII-Processing System:

800-122 PII Confidentiality Impact Rating:

Control	800-122 Control	800-53 J Control	Low	Moderate	High	Mod to High Jump	System Implementation	Notes and Findings
IR-4			X	X	X			
IR-4(3)								
IR-5			X	X	X			
IR-6			X	X	X			
IR-7			X	X	X			
IR-8			X	X	X			
IR-10			X	X	X			
MA-1				X	X			
MA-2								
MA-4(6)			X	X	X			
MA-5			X	X	X			
MP-1			X	X	X			
MP-2	X		X	X	X			
MP-3	X		X	X	X			
MP-4	X		X	X	X			
MP-5	X		X	X	X			
MP-5(4)	*		X	X	X			
MP-6	X			X	X			
MP-6(1)	*		X	X	X			
MP-6(8)	*			X	X			
MP-7				X	X			
MP-7(1)				X	X			
MP-8(3)				X	X			
PE-1								
PE-2			X	X	X			
PE-2(1)								
PE-3			X	X	X			
PE-4								
PE-5			X	X	X			
PE-6								
PE-8								
PE-17			X	X	X			
PE-18					X	*		
PL-1								
PL-2			X	X	X			
PL-4			X	X	X			

Name of PII-Processing System:

800-122 PII Confidentiality Impact Rating:

Control	800-122 Control	800-53 J Control	Low	Moderate	High	Mod to High Jump	System Implementation	Notes and Findings
PL-8			X	X	X			
PS-1			X	X	X			
PS-2			X	X	X			
PS-3			X	X	X			
PS-3(3)			X	X	X			
PS-4			X	X	X			
PS-5			X	X	X			
PS-6			X	X	X			
PS-7			X	X	X			
PS-8			X	X	X			
RA-1			X	X	X			
RA-2			X	X	X			
RA-3			X	X	X			
SA-2			X	X	X			
SA-3			X	X	X			
SA-4			X	X	X			
SA-8			X	X	X			
SA-9								
SA-9(5)			X	X	X			
SA-11				X	X			
SA-11(5)					X	*		
SA-15(9)				X	X			
SA-17			X	X	X			
SA-21			X	X	X			
SC-2				X	X			
SC-4			X	X	X			
SC-7(14)								
SC-8	X		X	X	X			
SC-8(1)	*		X	X	X			
SC-8(2)	*			X	X			
SC-12			X	X	X			
SC-13			X	X	X			
SC-28	X		X	X	X			
SC-28(1)	*		X	X	X			
SI-1			X	X	X			
SI-3								

Name of PII-Processing System:

800-122 PII Confidentiality Impact Rating:

Control	800-122 Control	800-53 J Control	Low	Moderate	High	Mod to High Jump	System Implementation	Notes and Findings
SI-4	X		X	X	X			
SI-5								
SI-7			X	X	X			
SI-7(6)			X	X	X			
SI-8								
SI-10				X	X			
SI-11								
SI-12			X	X	X			
PM-1			X	X	X			
PM-2				*	*			
PM-3			X	X	X			
PM-5			X	X	X			
PM-7			X	X	X			
PM-9			X	X	X			
PM-10			X	X	X			
PM-11			X	X	X			
PM-12			X	X	X			
PM-13				*	*			
PM-14			X	X	X			
PM-15			X	X	X			
AP-1		X	X	X	X			
AP-2		X	X	X	X			
AR-1		X	X	X	X			
AR-2		X	X	X	X			
AR-3		X	X	X	X			
AR-4		X	X	X	X			
AR-5		X	X	X	X			
AR-6		X	X	X	X			
AR-7		X	X	X	X			
AR-8		X	X	X	X			
DI-1		X	X	X	X			
DI-1(1)		*		X	X			
DI-1(2)		*		X	X			
DI-2		X		*	*			
DI-2(1)		*		*	*			
DM-1		X	X	X	X			

Name of PII-Processing System:

800-122 PII Confidentiality Impact Rating:

Control	800-122 Control	800-53 J Control	Low	Moderate	High	Mod to High Jump	System Implementation	Notes and Findings
DM-2		X	X	X	X			
DM-2(1)		*						
DM-3		X	X	X	X			
DM-3(1)		*		*	*			
IP-1		X	X	X	X			
IP-1(1)		*						
IP-2		X	X	X	X			
IP-3		X	X	X	X			
IP-4		X	X	X	X			
IP-4(1)		*		*	*			
SE-1		X	X	X	X			
SE-2		X	X	X	X			
TR-1		X	X	X	X			
TR-1(1)		*		*	*			
TR-2		X	X	X	X			
TR-2(1)		*	X	X	X			
TR-3		X	X	X	X			
UL-1		X	X	X	X			
UL-2		X	X	X	X			

References:

Implemented
Partially Implemented
Planned
Alternative Implementation
Not Applicable
Not Selected
Not Implemented - Risk Accepted

Appendix F: PIA CRB Risk Analysis Guide

Privacy Impact Assessment Compliance Review Board
Risk Analysis Guide
(Date of Meeting)

Name of IT System:
Authorization to Operate (ATO) date:
ATO expiration date:

A Privacy Threshold Analysis (PTA) must be completed for a system processing PII/BII in order to determine if a Privacy Impact Assessment (PIA) is required. The purposes of a PIA are to ensure effective compliance with the Privacy Act for notice and disclosure and to confirm appropriate privacy protections are in place. The following critical areas will be discussed during this meeting:

- System/Data characterization
  - System location/Status
  - Type/Sources of information
  - Purpose/Use of information
  - Retention of information
  - Legal authority
  - FIPS 199 security impact category
  - Notice and consent
  - Records retrieval
  - System of records notice(s)
  - NIST SP 800-122 PII confidentiality impact level
- Information Sharing Practices
  - Access
  - Computer Matching Program
  - Connection with other IT systems
- Website/Mobile application processes
  - Website(s)
  - Website privacy policy/Privacy Act statement
  - Mobile application(s)
  - Tracking technologies
- Status of privacy controls
  - Plan of Action and Milestones
  - IT Security controls
- Risk Assessment Review
  - Threats and vulnerabilities
  - Summary risk

Appendix G: PIA Annual Review Certification Form

PRIVACY IMPACT ASSESSMENT (PIA)

ANNUAL REVIEW CERTIFICATION FORM

(Last SAOP approved PIA with updated signatures must accompany this form)

Name of PIA:_____

FISMA Name/ID (if different):

_____

Name of IT System/ Program Owner:

_____

Name of Information System Security Officer:_____

Name of Authorizing Official(s):_____

Date of Last PIA Compliance Review Board (CRB): _____

(This date must be within three (3) years.)

Date of PIA Review:_____

Name of Reviewer:_____

REVIEWER CERTIFICATION - I certify that on the PIA Review date identified above, I have reviewed the IT system/program and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of Reviewer: _____

Date of Privacy Act Review: _____

Name of the Reviewing Privacy Act Officer (PAO): _____

PAO CERTIFICATION - I certify that on the Privacy Act Review date identified above, I have reviewed all Privacy Act related issues cited in this PIA, such as, the legal authorities, SORNs, privacy act statements, etc. and have confirmed that there have been no changes to the system/program which require revising the last SAOP approved version of the PIA which is currently posted on the Commerce website at commerce.doc.gov/privacy.

Signature of the PAO: _____

Date of Bureau Chief Privacy Officer (BCPO) Review: _____

Name of the Reviewing BCPO:_____

BCPO CERTIFICATION - I certify that on the BCPO Review date identified above, I have reviewed the security and privacy risks presented by the collection, processing, storage, maintenance, and/or dissemination of business or personally identifiable information (B/PII) on this system/ program in the context of the current threat environment, along with any open Plans of Action and Milestones (POA&Ms) and have confirmed that there has been no increase in privacy risks since the date that the PIA was last approved by the DOC SAOP.

Signature of the BCPO: _____

Appendix H: Privacy Impact Assessment Exemptions

In accordance with guidance outlined in OMB-M-03-22, certain types of IT systems may be exempt from the PIA requirement. These include any system "where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged, as in the following circumstances:"

- for government-run websites, IT systems or collections of information to the extent that they do not collect or maintain PII about members of the general public (this includes government personnel and government contractors and consultants);

- for government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or obtaining additional information;

- for national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act);

- when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act (see 5 U.S.C. §§ 552a(8-10), (e)(12), (o), (p), (q), (r), (u)), which specifically provide privacy protection for matched information;

- when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the E-Government Act of 2002;

- if agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generates information in identifiable form; or

- for minor changes to a system or collection that do not create new privacy risks.

Consult your BCPO to determine if a system is exempt from the PIA requirement under DOC policy.

Appendix I: References and Recommended Reading

Department of Commerce Privacy Program Plan, December 2024.

Department Memorandum: Commerce Policy Regarding 1) Implementing National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 Revision 4, Appendix J Privacy Controls, and 2) Senior Agency Official for Privacy (SAOP) Approval as a Precondition for the Issuance of an Authorization to Operate (ATO), November 18, 2014.

National Institute of Standards and Technology (NIST) Internal Report (IR) 8062, *An Introduction to Privacy Engineering and Risk Management in Federal Systems*, January 2017.

NIST Special Publication (SP) 800-122, *Guide to Protecting the Confidentiality of PII*, April 2010.

NIST SP 800-53, Rev 4, *Security and Privacy Controls for Federal Information Systems*, April 2013.

NIST SP 800-37, Rev 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy,* December 2018.

Federal Information Processing Standards Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, February 2004.

OMB-M-03-22, *Guidance for Implementing the Privacy Provisions of the E–Government Act of 2002*, September 26, 2003.

OMB-M-10-23, *Guidance for Agency Use of Third-Party Websites and Applications*, June 25, 2010.

OMB-M-14-04, *Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management*, November 18, 2013.

OMB-M-16-24, *Role and Designation of Senior Agency Officials for Privacy*, September 15, 2016.

OMB-M-17-06, *Policies for Federal Agency Public Websites and Digital Services*, November 8, 2016.

Model Privacy Impact Assessment for Agency Use of Third-Party Websites and Applications, December 29, 2011.

OMB Circular A-130 (Appendix II), *Managing Information as a Strategic Resource*, July 28, 2016.

E-Government Act of 2002 (Public Law 107–347, 116 Stat. 2899, 44 U.S.C. § 101, H.R. 2458/S. 803)

Federal Information Security Modernization Act of 2014 (FISMA Reform) (Pub.L. 113-283)

Privacy Act of 1974 (Public Law 93–579, 88 Stat. 1896, enacted December 31, 1974, 5 U.S.C. § 552a), As Amended

Paperwork Reduction Act of 1980 (PRA) (Public Law No. 96-511, 94 Stat. 2812, codified at 44 U.S.C. §§ 3501–3521, As Amended