|  |  |
| --- | --- |
|  |  |
| Evaluation of the INSERT SYSTEM/APPLICATION NAME HERE Privacy Impact Assessment Insert PIA Date, PIA Version No. | |
| Reference MITRE ACT Assessment Handbook v1.0  INSERT DATE HERE | |
| Evaluators Name:  Evaluators Email Address:  Evaluators Telephone Number: | |
| **NOTICE**  <Contract notice goes here as needed> | |
|  | |
|  | |
|  | |
|  | |

|  |
| --- |
| Evaluators Instructions  **IMPORTANT:** **This page must be removed prior to either hardcopy or electronic distribution.**  The instructions are intended to provide guidance to the evaluators for consistency when evaluating Privacy Impact Assessment (PIA) for systems.   1. Update all areas highlighted in yellow with the appropriate information. 2. If there are no issues or missing information in the risk assessment related to the PIA table entries then the comments column should have a status of “Met”. 3. If there are issues, missing information or a risk that has not been identified then indicate so in the comments column. 4. General or overall comments and any additional feedback can be added in the Additional Comments section at the end of the document. 5. Identify any grammar or readability issues. 6. Check for misspelled words (run spell-check and visually scan). 7. Confirm time frames that may conflict. 8. If a number of months is specified, confirm that it is in alignment with policies, and standards. 9. For subsystems, state and confirm that the PII collected by the subsystems is covered in separate PIAs. 10. Wording Specifics:     * <Enter sponsor-specific wording specifics here> 11. Sources:     * Identify by name all sources of information collection or retrieval.     * Make sure that URL links that are provided are available and valid. 12. <Add sponsor-specific guidance here> |

# Privacy Impact Assessment Checklist

This Privacy Impact Assessment (PIA) Evaluation Checklist is designed to help assess the completeness of the system’s PIA artifact. <Insert derivation information here as necessary>

## How the Checklist Is Used

1. The PIA is reviewed to verify that each of the requirements noted in the checklist is included in the PIA and analyzed to determine if the information provided adequately addresses the requirement.
2. In the status column, an indication on whether each requirement is:
   * **Met** **-** The requirement has been completely satisfied and no additional information needs to be documented
   * **Partial -** The requirement has been partially satisfied but there is still missing information as explained in the **Comments** column
   * **Not Met -** The requirement has not been satisfied and any additional information noting the reasons are provided in the **Comments** column
   * **N/A -** The requirement is not applicable to the system or application risk assessment that is being evaluated and the reason that it is not applicable is explained in the **Comments** column
3. The comments column contains an explanation if a control is not met, partially met, or not applicable.
4. <Add additional references here>

| **Index** | Privacy Impact Assessment  **Requirement** | **Question Guidance** | **Status: Met, Partial, Not Met or N/A** | Comments |
| --- | --- | --- | --- | --- |
|  | PIA Unique Identifier | Unique Identifier for PIA |  |  |
|  | System Name | Official name for system the PIA is for |  |  |
|  | ~~Identify the Enterprise Performance Lifecycle phase of the system.~~ | ~~The phase of the HHS Enterprise Performance Lifecycle (EPLC) Framework that best matches the phase of the system should be indicated.~~ |  |  |
|  | Is this a FISMA-Reportable system? | This answer should be yes if the System UUID associated with this PIA matches a listing in your OpDiv’s FISMA System Inventory.  This answer should be no if:   * + No System UUID is associated with this PIA; or   + The System UUID does not match a listing in your OpDiv’s FISMA System Inventory. |  |  |
|  | Does the system include a Website or online application available to and for the use of the general public? | If the system includes one or more websites, the response should be yes (unless) <enter edge cases if needed> |  |  |
|  | Identify the operator | Organization that operates the system |  |  |
|  | Point of Contact (POC) | The title, name, organization, e-mail, and phone number of the individual(s) who may be contacted for inquiries about the system should be listed. |  |  |
|  | Is this a new or existing system? | The form should indicate:   * + Existing if the PIA has been signed (i.e., finalized) at least once; or   + New if the PIA has never been signed (i.e., finalized) |  |  |
|  | Does the system have Security Authorization (SA)? | Yes or no response should be indicated. |  |  |
|  | Date of Authorization | If the system requires an SA and does not have one, the date when the system should receive its SA should be provided.  If the system will not require a SA, it should say not applicable. |  |  |
|  | Planned Data of Authorization | If the system requires an SA and does not have one, the date when the system should receive its SA should be provided.  If the system will not require a SA, It should say not applicable. |  |  |
|  | Indicate the following reason(s) for updating this PIA. Choose from the following options. | Explain why the PIA is being updated. This can include:   * The PIA is for a new system * New privacy risks are possible due to an action being taken (e.g., system conversion, new public access, etc.) * Scheduled PIA update |  |  |
|  | Describe in further detail any changes to the system that have occurred since the last PIA. | This section should describe all system changes that have occurred since the PIA was last finalized.  Not applicable if no changes have occurred since the PIA was last finalized. |  |  |
|  | Describe the purpose of the system. | This response should describe:   * + What functions are supported by the system; and   + What the system does for each of those functions   This response should be:   * + Thorough enough that a reader with no prior knowledge of the system or what it supports will be able to understand the rest of the PIA; and   + Simple enough that a reader with limited technical knowledge will be able to understand the explanation.   Example:  “Google Maps (Maps) is a desktop and mobile web mapping service. It offers satellite imagery, street maps, 360 panoramic view of streets, real-time traffic conditions, and route planning for traveling by foot, car, bicycle, or public transportation.”  **Consideration:**  If there are any ‘Shared Services’ provide their main function and the PIA that covers these Shared Services. |  |  |
|  | Describe the type of information the system will collect, maintain (store), or share. (Subsequent questions will identify if this information is PII and ask about the specific data elements.) | List and/or describe all the types of information that are collected into and/or maintained in the system regardless of:   * + Whether that information is PII;   + How long that information is stored.   **Make sure to discuss information collected from system users in order to control system access. Unless users enter a system through separate access control software, systems that require a login usually collect usernames, passwords, and/or e-mails.** |  |  |
|  | Provide an overview of the system and describe the information it will collect, maintain (store), or share, either permanently or temporarily. | Describe why each type of information listed in <question number> is collected into and/or maintained in the system or shared with another system. This description should:   * + Consider all information regardless of whether it is PII; and   + Specify what information is collected about each category of individual.   Example:  “We use the information we collect for web mapping services in order to provide, maintain and improve Maps. The information is used to provide real time directions, traffic conditions, and route planning.  **We use the information we collect from system users in order to provide customizable services and provide account support**.” |  |  |
|  | Does the system collect, maintain, use, or share PII? | * The response should be yes if the system collects and/or maintains any PII for any length of time.   + This includes any type of PII regardless of sensitivity.   + This includes any system which:     - Acts as a conduit for PII (even if it is not maintained in the system). * Collects and/or maintains PII for a short-term purpose then discards it. * Personally Identifiable Information (PII): Defined in OMB M-07-16 Footnote 1 as information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother’s maiden name, etc. Other examples may include:   + Work information, including work e-mails and work phone numbers   + Job titles since many people have a title that is unique to them   + Home phone numbers and addresses, even if they are publicly available   + Family relationships * E-mails provided when registering for a system |  |  |
|  | Indicate the type of PII that the system will collect or maintain. | Each element of PII collected into and/or maintained in the system should be:   * + Identified from the list of commonly included PII; or   + Briefly described in the text boxes.   This includes every element of PII regardless of:   * + Type   + Sensitivity   + Whether it is from employees or the public   If any types of PII discussed in the rest of the PIA should also be selected and/or described in this answer. |  |  |
|  | Indicate the categories of individuals about whom PII is collected, maintained, or shared. | In the text box, whose PII is collected, maintained, or shared via the system should be Indicate, or described. |  |  |
|  | For what primary purpose is the PII used? | This should have a response since a system should not collect and/or maintain PII for any length of time unless it is needed for at least one primary use. However, not applicable is an appropriate response for <question number> if there is no secondary use.  Example: “The PII collected is used to create user accounts, which provide a customizable application and a means of contacting users regarding account maintenance or issues.” |  |  |
|  | Describe the secondary uses for which the PII will be used (e.g. testing, training or research) | Not applicable is an appropriate response for Q19 if there is no secondary use.  Example: “The PII collected is used to create user accounts, which provide a customizable application and a means of contacting users regarding account maintenance or issues.” |  |  |
|  | Identify legal authorities governing information use and disclosure specific to the system and program. | The following authorities require that you complete a SORN or other documentation in order to use or disclose PII. Apart from rare exceptions, these authorities do not provide authority for a system to use or disclose PII and therefore should not be included in this response:   * + The Privacy Act of 1974   + The Freedom of Information Act   + The Federal Information Security Management Act   + The E-Government Act of 2002   + OMB Memorandum M-03-22   + The Health Information Portability and Accountability Act (HIPAA)   + The HIPAA Privacy and/or Security Rules located at 45 CFR Parts 160, 162, and 164   If no other authorities are known, you may cite to [5 USC 301, Departmental regulations](http://www.gpo.gov/fdsys/pkg/USCODE-2011-title5/html/USCODE-2011-title5-partI-chap3-sec301.htm) (user credentials) |  |  |
|  | Describe the function of sensitive PII (SPII). | If the SPII is collected into and/or maintained in the system for any length of time, this space should describe:   * + All the ways that SPII is used in the system   + When, where, and why that SPII is disclosed and/or shared   + Why the system uses the SPII instead of another identifier   + If the SPII is not collected into and/or maintained in the system, the response should be not applicable   Note: For this use case, SPII is any PII that, if lost, compromised, or unnecessarily disclosed, would cause the individual substantial harm, embarrassment, inconvenience, or unfairness. Examples include:   * Social Security Number * Biometric information * Certain pieces information in conjunction with the individual’s identity * Contextually sensitive information |  |  |
|  | Cite the legal authority to use the SPII (if needed). | If SPII is collected into and/or maintained in the system, as stated in <question number> and <question number> and requires legal authorization to do so, this response should:   * + Cite the legal authorities which permit or require the use of the SPII   + Explain how those authorities permit the use of the SPII if not evident from the cited authorities   If SPII is not collected into and/or maintained in the system, the response should be not applicable. |  |  |
|  | Are records in the system retrieved by one or more PII data elements (if applicable)? | The goal of this question is to ask whether the Privacy Act applies. The Privacy Act does not include the term PII; it instead asks whether retrieval occurs by a name of an individual or some identifying number, symbol, or other identifying particular assigned to an individual. This is only applicable to government systems. |  |  |
|  | Identify the number and title of the Privacy Act System of Records Notice (SORN) that is being used to cover the system or identify if a SORN is being developed (if applicable). | Records stored in different systems may be subject to different SORNs. Be sure to only list the SORNs that apply to information maintained in the system being evaluated as part of the PIA. Avoid citing SORNs that only apply to information:   * + Before it is transferred into the system * After it has been disclosed from the system |  |  |
|  | Identify the sources of PII in the system. | These sources include:   * + Directly from Individual About Whom the Information Pertains   + Government Sources   + Non-Government Sources   A direct collection may result in the need to select one or more methods and one or more sources. |  |  |
|  | Identify the OMB information collection approval number and expiration date (if applicable). | OMB collection approval number required when you are collecting PII directly from the individual for whom it pertains. |  |  |
|  | Identify with whom the PII is shared or disclosed and for what purpose. | Identify all entities and organizations the PII is shared with, internal and external to the owning organization. Explain the reasons for this sharing. |  |  |
|  | Identify applicable authorizations for external sharing of information. | For all external organizations that the PII is shared with, provide the justifications and statutory authorizations for the sharing. |  |  |
|  | Describe any agreements in place that authorizes the information sharing or disclosure (e.g., Computer Matching Agreement, Memorandum of Understanding (MOU), or Information Sharing Agreement (ISA)). | If PII in the system is shared or disclosed subject to one or more agreements, a description of the sharing and disclosures that are permitted under each agreement should be provided.    If sharing or disclosure of PII in the system is not subject to an agreement, the author should have provided:   * + What sharing or disclosures are occurring without an agreement   + Why no agreement is required or in place |  |  |
|  | Describe the procedures for accounting for disclosures. | Every time the organization discloses a record externally for a reason other than the Freedom of Information Act (FOIA), document the following:   * + - The date, nature, and purpose of each disclosure     - The name and address of the recipient   If no records in the system are subject to the Privacy Act, this answer can be not applicable. |  |  |
|  | Describe the process in place to notify individuals that their personal information will be collected. If no prior notice is given, explain the reason. | If the system collects information directly from an individual, the collection is governed by the Privacy Act, and the individual will receive a Privacy Act Statement (PAS) (written, verbal, or otherwise) before or when their records are collected into the system:   * + This section should describe how and when the PAS is provided   + Provide the text of the PAS (or a link to the PAS if will not fit in the textbox provided)   If the system collects information directly from an individual, the collection is governed by the Privacy Act, and the individual will not receive a PAS (written, verbal, or otherwise) before or when their records are collected into the system, describe why the PAS will not be provided.  If the system collects information directly from an individual, the collection is not governed by the Privacy Act, and the individual will still receive some type of notice (written, verbal, or otherwise) this section should also:   * + State how and when the notice is provided   + Provide the text of that notice or summarize what it includes   If the system collects information directly from an individual, the collection is not governed by the Privacy Act, and the individual will not receive notice (written, verbal, or otherwise) before/when/after his/her PII is collected into the system, describe why the notice will not be provided.  Only consider whether an individual’s PII will be collected from the individual directly into the system. If the system only collects PII from another system, the first system should provide the notice so not applicable is an appropriate answer. |  |  |
|  | Is the submission of PII by individuals voluntary or mandatory? | Select mandatory if one’s refusal to provide at least some of the PII maintained in the system may lead to a civil or criminal penalty.  Select voluntary in all other situations regardless of the repercussions that may result from one’s refusal to provide the requested PII. |  |  |
|  | Describe the method for individuals to opt-out of the collection or use of their PII. If there is no option to object to the information collection, provide a reason. | If there are situations in which the system requests PII from individuals and those individuals have the choice to opt-out of the use or collection of their PII, this section should describe:   * + The opt-out processes   + When those processes may be used   If there are situations in which the system requests PII from individuals and those individuals do not have the choice to opt-out of the use or collection of their PII, this section should describe:   * + When individuals cannot opt-out   + The reason why individuals cannot opt-out   In some situations, the answer may be that the individual was given the opportunity to opt-in to the collection hence no need to provide an opt-out. |  |  |
|  | Describe the process to notify and obtain consent from the individuals whose PII is in the system when major changes occur to the system (e.g., disclosure and/or data uses have changed since the notice at the time of original collection).  Alternatively, describe why they cannot be notified or have their consent obtained. | Before an individual’s PII will be used for a purpose materially different from that given at the time of collection, this section should explain:   * + When and how notice will occur or why that will not occur   + When and how individuals will have an opportunity to consent to the materially different purpose or why that will not occur   If PII maintained in a system is subject to the Privacy Act, a SORN should describe some of the ways those records will be used within the agency and some of the reasons why the records may be disclosed to parties outside the agency. If a system will change in a way that will conflict with the SORN, a new or revised SORN may need to be published in the Federal Register. A 30-day public notice and comment period should elapse before the agency implements the changes reflected in the new SORN. |  |  |
|  | Describe the process in place to resolve an individual's concerns when they believe their PII has been inappropriately obtained, used, or disclosed, or that the PII is inaccurate. If no process exists, explain why not. | If records in a system are subject to the Privacy Act, individuals will generally have the right to:   * + Find out if the system contains records about themselves   + Request access to their records * Request that their records be amended or corrected if they contain PII which is inaccurate, irrelevant, untimely, or incomplete   If a defined redress process gives individuals an opportunity to raise concerns that their PII in the system has been inappropriately obtained, used, or disclosed, the response to this question should include:   * + The name of the office that would handle those concerns   + A description of how an individual may raise questions or concerns   + A description of how the concerns will be considered, investigated, and resolved   If a defined process gives individuals an opportunity to raise concerns that their PII in the system is inaccurate, the response to this question should:   * + State the name of the office that would handle those concerns   + A description of how an individual may raise questions or concerns   + A description how the concerns will be considered, investigated, and resolved   If there is not a defined process in place to address any of the situations, explain why such a process does not exist. |  |  |
|  | Describe the process in place for periodic reviews of PII contained in the system to ensure the data's integrity, availability, accuracy and relevancy. If no processes are in place, explain why not. | Describe any system processes which are designed to ensure that:   * + PII is not improperly or inadvertently modified or destroyed   + Individuals who provide or modify PII cannot repudiate that action   + PII is available when needed   + PII is sufficiently accurate for the purposes needed   + Outdated, unnecessary, irrelevant, incoherent, and inaccurate PII is removed from the system |  |  |
|  | Identify who will have access to the PII in the system and the reason why they require access. | The types of individuals who should have access to the PII maintained in the system must be identified. A description of the following is needed:   * + The PII that specific type of individual may access   + The reason for granting that type of individual such access   All relevant roles should be selected, even if an individual fills multiple roles. For example, some systems allow contractors to access PII in their role as developers. |  |  |
|  | Describe the procedures in place to determine which system users (administrators, developers, contractors, etc.) may access PII | Explain the administrative procedures used to determine why the categories of individuals described in <question number> should have access to PII maintained in the system. |  |  |
|  | Describe the methods in place to allow those with access to PII to only access the minimum amount of information necessary to perform their job. | Explain what system controls limit a user’s access to the type, amount, or categories of PII necessary to perform their job functions as determined in <question number>, or why those system controls do not exist. |  |  |
|  | Identify training and awareness provided to personnel (system owners, managers, operators, contractors and/or program managers) using the system to make them aware of their responsibilities for protecting the information being collected and maintained. | <question number> asks what general privacy and security trainings are provided to system users while <question number> asks what training is provided to a type of system user because of their access to certain system information. If training seems to fit within both <question number> and <question number>, you may select whether to discuss that training in either answer.  State if system users receive any general privacy and security training before and/or while they have access to the system, this section should describe:   * + The type, frequency, and topics of the trainings   + The categories of users who receive each type of training |  |  |
|  | Describe training system users receive (above and beyond general security and privacy awareness training). | If system users receive any privacy and/or security awareness training because they have access to this particular system, the following should be documented:   * + The type, frequency, and content of those trainings   + Which users receive which trainings   If system users do not receive any privacy and security trainings specifically because they have access to this particular system, write not applicable. |  |  |
|  | Do contracts include Federal Acquisition Regulation (FAR) and other appropriate clauses ensuring adherence to privacy provisions and practices? | This answer should be yes if specific regulations are included that require adherence to privacy provisions and practices.  This answer should be no if:   * + No FAR clauses are needed   + FAR clauses are needed but not yet included |  |  |
|  | Describe the process and guidelines in place with regard to the retention and destruction of PII. | For government systems: state the NARA approved records retention citation number.  If there is no NARA number, describe the proposed timeline for records retention and destruction or explain why it is not needed  For non-government systems: describe the records retention and destruction process if available. |  |  |
|  | Describe, briefly but with specificity, how the PII will be secured in the system using administrative, technical, and physical controls. | This response should provide a high-level overview of the system’s administrative, technical, and physical security controls, a few examples of each control may be appropriate (use of passwords, a clearance is required).   * Administrative controls: Administrative actions, policies, and procedures designed to manage (1) the selection, development, implementation, and maintenance of the security measures designed to protect the PII and (2) the conduct of those with access to the PII.   + Includes: Training requirements, sanction policy, risk analysis, and log-in monitoring. * Technical controls: The technology, policies, and procedures used to protect the PII and control access to the PII.   + Includes: Encryption, automatic logoff, and 2-factor authorization. * Physical controls: The physical measures, policies, and procedures designed to protect electronic information systems, buildings, and equipment from unauthorized intrusions, environmental hazards, and natural hazards.   + Includes: Facility access controls and disposal controls. |  |  |
|  | Identify the publicly-available URL: | A link should be listed to the main page of any website which is:   * + Available to and for the use of the general public   + Part of the system being reviewed by this PIA.   If a URL is unavailable because a website is not yet available to the general public, state that the website is currently in the development stage, but do not provide the URL of the development website. |  |  |
|  | Does the website have a posted privacy notice (if applicable)? | For the purposes of this question, website refers to a system’s website available to and for the use of the general public.  Yes indicates if a privacy notice that complies with all E-Government Act and OMB Memoranda is posted on:   * + All known major entry points (regardless of whether PII is collected)   + All pages that collect substantial personal information from the public |  |  |
|  | Is the privacy policy available in a machine-readable format? | Yes indicates if all the system’s websites that are available to and for the use of the general public include a machine-readable privacy policy. |  |  |
|  | Does the Website use web measurement and customization technology? | Response indicates whether any of the system’s websites, which are available to and for the use of the general public, use any web measurement and customization technologies.   * Web measurement and customization technology includes:   + Temporary and permanent cookies   + Web bugs/beacons   Any other technology used to remember a user’s online interactions with a website in order to conduct measurement and analysis of usage or to customize the user’s experience. |  |  |
|  | Select the type of website measurement and customization technologies is in use and if it is used to collect PII. (Select all that apply) | The types of web measurement and customization technologies used by the system’s websites that are available to and for the use of the general public should be documented.  For each type of technology selected, select whether it collects PII. |  |  |
|  | Does the website have any information or pages directed at children under the age of thirteen? | Should be indicated whether the system’s website, available to and for the use of the general public, contains any information or pages directed at children under the age of thirteen, such that it would be subject to the Children’s Online Privacy Protection Act of 1998 (COPPA). |  |  |
|  | Is there a unique privacy policy for the website and does the unique privacy policy address the process for obtaining parental consent if any information is collected? | Whether the websites, referenced in <question number>, include a privacy policy that satisfies all COPAA requirement should be indicated here. |  |  |
|  | Does the website contain links to websites external to the organization? | If the system includes website links to external websites outside of the evaluated organization’s purview, document the links and the organizations they belong to. |  |  |
|  | Is a disclaimer notice provided to users that follow external links to websites not owned or operated by the organization? | This response indicates whether or not an individual will see an alert which says they are moving from a website which is controlled by the evaluated organization to a website not controlled by the evaluated organization. If no alert is given, explain why. |  |  |

## Additional Comments