# **Appendix B. PIA Template**

**PRIVACY IMPACT ASSESSMENT**

**PART I.  PIA Contacts and Qualification QUESTIONS**

**A.  Contact Information**

|  |
| --- |
| **System Title**: *Enter the name of the IT system* |
| **Office of Responsibility**: *Enter the service, staff office, or region* |
| **Program Manager Name and Title:** Phone:  E-mail:  Organization Title and Correspondence Code:  *Enter the information for the Program Manager/System Owner of the system* |
| **System or Project Manager/Project PIA Contact Name and Title:**  Phone:  Email:  Organization Title and Correspondence Code:  *Enter the information for the point of contact for the PIA*  *Signature:\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_* |
| **AO Name and Title:** Phone:  Email:  Organization Title and Correspondence Code:  *Enter the information for the Designated Approving Authority for your service, staff office, or region* |

**Note on template formatting:**  Responses to questions should replace the Explanations/Instructions in the space provided in column two.     
  
            
Date PIA completed:   \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Information System Security Officer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**B.  Qualification Questions**

|  |  |
| --- | --- |
| **Question** | **Explanation/Instructions** |
| 1. Does your system collect any information in identifiable form (personal data) on the general public? (YES or NO) If YES, a PIA is required, starting in FY 2004. | *Information in identifiable form (also known as personal data/information) refers to any data collected about an individual that can be used for identification purposes.  It includes information that identifies the individual by name or other unique identifier in conjunction with other data elements such as gender, race, birth date, age, geographic indicator, personal e-mail address, home address, home phone number, health records, Social Security Number (SSN), personal credit card information, and similar personal information. Information permitting the physical or online contacting of a specific individual is considered information in identifiable form.* ***This does not refer to business entities or government agencies, or aggregate data that cannot be traced back to an individual person****.* |
| 2.  Does your system collect any information in identifiable form (personal data/information) on government employees? (YES or NO) If YES, a PIA is required, starting in FY 2005. | *Information in identifiable form refers to any data collected about an employee that can be used for identification purposes. It includes information that identifies the employee by name or other unique identifier in conjunction with other data elements such as gender, race, birth date, age, marital status, home e-mail address, home address, home phone number, health records, SSN, performance appraisals, employment history not related to current job, allegations of misconduct/arrests/ complaints/grievances/performance based actions, payroll deductions, personal credit card information, and similar personal information.* |
| 3.  Has a PIA been done before for the system? (YES or NO) | *If Yes, enter the date of the last PIA.* |

***(Please Note:  If you answered “No” to Question #1 or Question #2, Part II is not required. Part II is for systems that answered “Yes” to either question.* A PIA for an existing system must be completed and reviewed annually. Updates to the PIA are done when there are significant changes to the system or a change in the privacy posture.)**

**PART II.  SYSTEM ASSESSMENT   
  
A.  Data in the System**

|  |  |
| --- | --- |
| **Question** | **Explanation/Instructions** |
| 1. What is the specific purpose of the agency’s use of the information and how does that use fit with the agency’s broader mission? | *Agency should use plain language to disclose the purpose(s) of its use of the information. Agency’s description should provide enough detail to allow the reader to gain full understanding of the purpose(s).* |
| 1.  Describe all information to be included in the system, including personal data. | *a. Briefly describe the purpose of the system and the data that will be in the system, including that of any subsystems.  b. Provide the specific privacy data elements that will be maintained in the system.* |
| 1.a.  What stage of the life cycle is the system currently in? | *Select:  Design/Planning; Development/Implementation; Operation/Maintenance; or Disposal.* |
| 2.a.  What are the sources of the information in the system? | *Describe where the system data originates, whether the privacy information is provided by the user or entered on behalf of the user and by whom, or if it comes programmatically from another system.* |
| 2.b.  What GSA files and databases are used? | *Identify any GSA files and databases that may be used as a source of the information.* |
| 2.c.  What Federal agencies are providing data for use in the system? | *List Federal agencies that are providing the information for use by the system. Specify data provided by each. If none, enter* ***None****.* |
| 2.d.  What State and local agencies are providing data for use in the system? | *List any State and local agencies that are providing data for use in this system. Specify the data provided by each. If none, enter* ***None.*** |
| 2.e.  From what other third party sources will the data be collected? | *List any other sources of data in the system and the data provided. If none, enter* ***None.*** |
| 2.f.  What information will be collected from the individual whose record is in the system? | *List the data that will be collected from the individual.* |
| 3.a.  How will the data collected from sources other than Federal agency records or the individual be verified for accuracy? | *The accuracy of personal information is very important. Indicate the steps that will be taken to ensure that the data is accurate and the integrity of the data remains intact.* |
| 3.b.  How will data be checked for completeness? | *Missing information can be as damaging as incorrect information. Indicate the steps that will be taken to ensure that all of the data is complete.* |
| 3.c.  Is the data current? How do you know? | *Indicate the process that will be used to ensure that the data is relevant and up-to-date.* |
| 4.  Are the data elements described in detail and documented? If yes, what is the name of the document? | *Each of the data elements must be defined and described. Descriptions should include the name, data type, and purpose for collection.* |

**B.  Access to the Data**

|  |  |
| --- | --- |
| **Question** | **Explanation/Instructions** |
| 1. a. Who will have access to the data in the system? | *Provide a list of users or groups of users of the entire system (i.e. government agencies, public access, etc.) and a separate list of people who will have access to privacy data.* |
| 1.b.  Is any of the data subject to exclusion from disclosure under the Freedom of Information Act (FOIA)? If yes, explain the policy and rationale supporting this decision. | *If so, reference the specific exemption under the FOIA (5 U.S.C. Section (b)(1) through (9)), to support your rationale.    Dept. of Justice guidance on exemptions:*  [*http://www.usdoj.gov/oip/foi-act.htm*](http://www.usdoj.gov/oip/foi-act.htm) *FOIA text:*  [*http://www.usdoj.gov/oip/foia\_updates/Vol\_XVII\_4/page2.htm*](http://www.usdoj.gov/oip/foia_updates/Vol_XVII_4/page2.htm)*,* |
| 2.  How is access to the data by a user determined? Are criteria, procedures, controls, and responsibilities regarding access documented? | *List any policies or procedures used to implement access to the system and privacy data. If there are supporting documents such technical and operational manuals or a system security plan, list them here.* |
| 3.  Will users have access to all data in the system or will the users’ access be restricted? Explain. | *Specify to what degree users can access their own privacy data after it has been entered. If there are any restrictions on access to this data, identify the restrictions.* |
| 4.  What controls are in place to prevent the misuse (e.g. browsing) of data by those having access? | *Reference technical, managerial, administrative, and operational controls in place supporting management of the data.* |
| 5.a.  Do other systems share data or have access to data in this system? If yes, explain. | *List any systems that will either send or receive data in this system. Explain the purpose of the connection and the methods used to ensure integrity and security of the data being exchanged.* |
| 5.b.  Who will be responsible for protecting the privacy rights of the clients and employees affected by the interface? | *List the title and office of the person(s) responsible to ensure that the privacy data is being handled properly. This typically should be the System Manager.* |
| 6.a.  Will other agencies share data or have access to data in this system (International, Federal, State, Local, Other)? | *List any entities that may access the data in this system and specify which data. If there are none, enter* ***None****.* |
| 6.b.  How will the data be used by the agency? | *Describe in detail how each piece of data will be used, including programmatic functions, indexing, aggregation, reporting, etc.* |
| 6.c.  Who is responsible for assuring proper use of the data? | *This should typically be the same person(s) listed for question 5.b.* |
| 6.d.  How will the system ensure that agencies only get the information to which they are entitled? | *List the controls and security mechanisms in place to ensure that exchange of data is appropriate.* |
| 7.  What is the life expectancy of the data? | *Indicate whether the data will be collected and used for a one-time process or whether the data will be maintained in a database. Indicate how long the one-time process typically takes or how long data will be maintained. If shared with other systems, provide indication on life expectancy from those systems as well. Use GSA Handbook CIO P 1820.1, GSA Records Maintenance and Disposition System, as a guide for determining the disposition requirements.* |
| 8.  How will the data be disposed of when it is no longer needed? | *Provide explanation of data disposal process. Indicate methods for disposing of data from operational databases as well as for archiving systems.* |

**C.  Attributes of the Data**

|  |  |
| --- | --- |
| **Question** | **Explanation/Instructions** |
| 1.  Is the use of the data both relevant and necessary to the purpose for which the system is being designed? | *List each data element and the relevance to the system.* |
| 2.a.  Will the system derive new data or create previously unavailable data about an individual through aggregation from the information collected? | *Yes or No. If yes, provide details on the derivation of the data. An example would be to create a credit risk rating based on credit history.* |
| 2.b.  Will the new data be placed in the individual's record (client or employee)? | *Yes or No.* |
| 2.c.  Can the system make determinations about individuals that would not be possible without the new data? | *Yes or No. Explain why or why not.* |
| 2.d.  How will the new data be verified for relevance and accuracy? | *Since this is privacy data about an individual that was not provided by the individual, the relevance and accuracy are very important. Provide details on processes used to verify this information.* |
| 3.a.  If the data is being consolidated, what controls are in place to protect the data and prevent unauthorized access? Explain. | *Enter* ***N/A*** *if the data is not being consolidated. Otherwise, describe the controls used to ensure that aggregated or consolidated privacy data remains protected.* |
| 3.b.  If processes are being consolidated, are the proper controls remaining in place to protect the data and prevent unauthorized access? Explain. | *Enter* ***N/A*** *if the processes are not being consolidated. Otherwise, describe the controls used to ensure that aggregated or consolidated privacy data remains protected.* |
| 4.  How will the data be retrieved? Can it be retrieved by personal identifier? If yes, explain. | *Explain all processes for retrieving the data. If personal identifiers (i.e. name, SSN, employee number, etc.) are used, list the identifiers.* |
| 5.  What are the potential effects on the privacy rights of individuals of:   a.  Consolidation and linkage of files and systems;  b.  Derivation of data;   c.  Accelerated information processing and decisionmaking; and  d.  Use of new technologies. How are the effects to be mitigated? | *Explain how the privacy rights of the individual may be protected or jeopardized based on a, b, c, and d. List all mitigation strategies used to ensure that the rights of the individuals are not compromised.* |

**D.  Maintenance of Administrative Controls**

|  |  |
| --- | --- |
| **Question** | **Explanation/Instructions** |
| 1.a.  Explain how the system and its use will ensure equitable treatment of individuals. | *Describe the processes in place to ensure fair and equitable treatment of individuals and their privacy data. If judgments are to be made based on the privacy data, indicate the rationale to be used to make the judgments and how the judgments will be kept fair and equitable.* |
| 1.b.  If the system is operated in more than one site, how will consistent use of the system be maintained at all sites? | *Describe technical, managerial, and operational controls in place to ensure that data integrity and protection is maintained across sites. Also, describe how data will be kept current and consistent between locations.* |
| 1.c.  Explain any possibility of disparate treatment of individuals or groups. | *Describe any potential situation where data could be evaluated differently. List the data elements that may impact disparate treatment (i.e. race, gender, etc.).* |
| 2.a.  What are the retention periods of data in this system? | *How long will data be kept (years, months, day, hours)? Use GSA records disposition schedules to determine requirements.* |
| 2.b.  What are the procedures for eliminating the data at the end of the retention period? Where are the procedures documented? | *Provide detailed explanation of the data disposal process. Indicate methods for disposing of data from operational databases as well as archiving procedures. List documents supporting these procedures and the locations of these documents.* |
| 2.c.  While the data is retained in the system, what are the requirements for determining if the data is still sufficiently accurate, relevant, timely, and complete to ensure fairness in making determinations? | *Describe data management procedures and updating requirement.* |
| 3.a.  Is the system using technologies in ways that Federal agencies have not previously employed (e.g. Caller-ID)? | *Yes or No. If yes, describe any technologies that may be used to collect or display privacy data.* |
| 3.b.  How does the use of this technology affect individuals’ privacy? | *Is the data more vulnerable to inadvertent or unintentional display? Does it improve the protection of the privacy data?* |
| 4.a.  Will this system provide the capability to identify, locate, and monitor individuals? If yes, explain. | *Describe the rationale and processes for identifying, locating, and monitoring individuals. This can include street address, e-mail, cell phone, as well as GPS data.* |
| 4.b.  Will this system provide the capability to identify, locate, and monitor groups of people? If yes, explain. | *Describe the rationale and processes for identifying, locating, and monitoring groups of individuals. This can include street address, email, cell phone, as well as GPS data.* |
| 4.c.  What controls will be used to prevent unauthorized monitoring? | *Describe managerial, technical, and operational controls used to manage monitoring activities.* |
| 5.a.  Under which Privacy Act System of Records notice (SOR) does the system operate? Provide number and name. | *List the Privacy Act Systems of Records Notice name and number here. Contact the* GSA Privacy Act Officer for *guidance.* |
| 5.b.  If the system is being modified, will the SOR require amendment or revision? Explain. | *If any of the information in the SOR is altered, such as acquisition of new privacy information, new implementations, etc., explain how or why the SOR should be amended. Coordinate preparation of a revised SOR with the GSA Privacy Act Officer.* |