

**PRIVACY IMPACT ASSESSMENT (PIA) For the**

|  |
| --- |
| Agency Name: |
| Agency System Name: |

**SECTION 1: IS A PIA REQUIRED?**

**a. Will this \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_( Abbreviation ) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).**

1. Yes, from members of the general public.
2. Yes, from Federal personnel\* and/or Federal contractors.
3. Yes, from both members of the general public and Federal personnel and/or Federal contractors.
4. No

\* "Federal personnel" are referred to in the IT Portfolio Repository (DITPR) as "Federal employees."

1. **If "No," ensure that the status is annotated for the reason(s) why a PIA is not required. Also, ensure that the reason(s) are recorded in appropriate documentation.**

**If "Yes ," then a PIA is required. Proceed to Section 2.**

**SECTION 2: PIA SUMMARY INFORMATION**

1. **Why is this PIA being created or updated? Choose one:**

**New Information System New**  **Electronic Collection**

**Existing Information System Existing**  **Electronic Collection**

**Significantly Modified Information System**

1. **Does this information system or electronic collection require a Privacy Act System Statements?**

A Privacy Act statements are required if the information system or electronic collection contains information about U.S. citizens or lawful permanent U.S. residents that is retrieved by name or other unique identifiers. If the collective of information in part or in whole can be used to specifically identify and or locate a person, it is considered PII and requires a Privacy Impact Assessment.

**Yes**  **No**

1. **Summary of the information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.**
2. Describe the purpose of this information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.
3. Briefly describe the privacy risks associated with the PII collected and how these risks are

addressed to safeguard privacy.

1. **With whom will the PII be shared through data exchange, both within your Component and outside your Component (e.g., other Components, State or Federal Agencies)?**  Indicate all that apply.

**Within the Component.**

Specify:

**State and Local Agencies.**

Specify:

**Yes** **Contractor** Enter name and describe the language in the contract that safeguards PII.

Specify:

**Yes** **Other** e.g., commercial providers, colleges

Specify:

**Yes** **Other Components.**

**Other Federal Agencies.**

Specify:

1. **Do individuals have the opportunity to object to the collection of their PII?**

**Yes**   **No**

1. If "Yes," describe method by which individuals can object to the collection of PII.

Specify:

1. If "No," state the reason why individuals cannot object.

Specify:

1. **Do individuals have the opportunity to consent to the specific uses of their PII?**

**Yes**   **No**

* 1. If "Yes," describe the method by which individuals can give or withhold their consent.

Specify:

* 1. If "No," state the reason why individuals cannot give or withhold their consent.

Specify:

1. **What information is provided to an individual when asked to provide PII data?** Indicate all that apply.

Privacy Act Statement  Privacy Advisory

None  Other

Describe Each Applicable Format:

**NOTE:**

**Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.**

**A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.**

# SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

1. **For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.**
   1. **What PII will be collected?** Indicate all individual PII or PII groupings that apply below.

|  |  |  |
| --- | --- | --- |
| Name | Other Names Used | Spouse Information |
| Home Address | Date of Birth | Parent Information |
| Mailing Address | Birth Place | Child Information |
| Telephone # | Driver’s License Number | Medical Information |
| Cell Phone # | Other ID Numbers | Military Records |
| Emergency Number | E-mail Address | Tax Records |
| Emergency Contact | Security Clearance | Medical Records |
| SSN | Legal Status | Bank records |
| Truncated SSN | Gender | Eligibility Records |
| Mother’s Maiden Name | Race | Disability Information |
| Marital Status | Religious Preference | Other Information |
| Ethnicity | Education Information |  |
| Citizenship Status | Biometrics |  |
| Financial Information | Employment Information |  |
| Law Enforcement Information |  |  |

Describe Other or Considerations to be noted.

* 1. **What is the source for the PII collected (e.g., individual, existing information systems, other Federal information systems or databases, commercial systems)?**

|  |  |  |
| --- | --- | --- |
| Paper | Web | Face to Face |
| Fax | Email | Telephone |
| System to System | KIOSK | Other |
|  |  | Describe Other or Considerations to be noted. |

* 1. **Why are you collecting the PII selected ?**

|  |  |  |
| --- | --- | --- |
| Verification | Authentication | Identification |
| Data matching | Service Provision | Other |

Describe Other or Considerations to be noted.

* 1. **What is the intended use of the PII collected (e.g., mission-related use, administrative use)?**

1. **Does this information system or electronic collection create or derive new PII about individuals through data aggregation?** (See Appendix for data aggregation definition.)

**Yes**   **No**

**If "Yes," explain what risks are introduced by this data aggregation and how this risk is mitigated.**

Describe:

**Who has or will have access to PII in this information system or electronic collection**? Indicate all that apply.

|  |  |  |
| --- | --- | --- |
| Users | Developers | Application Admins |
| System Administrators | Management | Other |

Describe:

**How will PII be secured?** Indicate all that apply.

|  |  |  |
| --- | --- | --- |
| Security Guards | Key Cards | Combination Locks |
| Identification Badges | Cipher Locks | Closed Circuit TV (CCTV) |
| Locked File Cabinets | Safes | Other |

Describe Others:

**Technical Controls?** Indicate all that apply.

|  |  |  |
| --- | --- | --- |
| User Names | Firewall | Encryption |
| Password | Intrusion Protection System | Public Key Distribution |
| Authentication | Intrusion Detection System | Digital Certificates |
| Multi Factor Authentication | VPN | BioMetrics |
| Other Means | Other Security Appliance | Common Access Card |

Describe Others:

**Administrative Controls?** Indicate all that apply.

|  |  |  |
| --- | --- | --- |
| Self Assessments | Offsite Backups | Monitoring |
| Risk Assessments | Offline Updates | Control Testing |
| Security Assessments | Encrypted Backups | Incident Testing |
| Third Party Audits | Restricted Access PII | DR Testing |
| Other Means |  |  |

Describe Others:

1. **Does this information system process or require audits under with the PCI Payment Card Industry, IRS, Social Security Administration, National Database of New Hires, or Criminal Justice System?**

**Yes. Indicate the certification and accreditation status:**

**Authorization to Operate (ATO) Date Granted:**

**Interim Authorization to Operate (IATO) Date Granted:**

**Denial of Authorization to Operate Date:**

**Interim Authorization to Test Date Granted:**

**No, this information system does not require certification and accreditation.**

1. **How do information handling practices at each stage of the "information life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individuals' privacy?**

Describe:

1. **For existing information systems or electronic collections, what measures have been put in place to address identified privacy risks?**

Describe:

1. **For new information systems or electronic collections, what measures are planned for implementation to address identified privacy risks?**

Describe:

**SECTION 4: REVIEW AND APPROVAL SIGNATURES**

**Prior to the submission of the PIA for review and approval, the PIA must be coordinated by the Program Manager or designee through the Information Assurance Manager and Privacy Representative at the local level.**

|  |  |
| --- | --- |
| **Program Manager** |  |
| Name |  |
| Title |  |
| Organization |  |
| Work Number |  |
| E-mail Address |  |
| Date of Review |  |
| Date of Approval |  |

|  |  |
| --- | --- |
| **Business Owner (Data Custodian)** |  |
| Name |  |
| Title |  |
| Organization |  |
| Work Number |  |
| E-mail Address |  |
| Date of Review |  |
| Date of Approval |  |

|  |  |
| --- | --- |
| **Privacy Officer** |  |
| Name |  |
| Title |  |
| Organization |  |
| Work Number |  |
| E-mail Address |  |
| Date of Review |  |
| Date of Approval |  |

|  |  |
| --- | --- |
| **Information Security Officer** |  |
| Name |  |
| Title |  |
| Organization |  |
| Work Number |  |
| E-mail Address |  |
| Date of Review |  |
| Date of Approval |  |

|  |  |
| --- | --- |
| **Information Technology** |  |
| Name |  |
| Title |  |
| Organization |  |
| Work Number |  |
| E-mail Address |  |
| Date of Review |  |
| Date of Approval |  |

|  |  |
| --- | --- |
| **Agency Signature Authority (Data Owner)** |  |
| Name |  |
| Title |  |
| Organization |  |
| Work Number |  |
| E-mail Address |  |
| Date of Review |  |
| Date of Approval |  |

**Publishing:**

Only Sections 1 and 2 of this PIA will be published. Each Component will maintain a central repository of PIAs on the Component's public Web site. Components will submit an electronic copy of each approved PIA to the CIO at: Name Here@Ks.gov

If the PIA document contains information that would reveal sensitive information or raise security concerns the Component may restrict the publication of the assessment to include Sections 1 and 2.

**APPENDIX**

Data Aggregation. Any process in which information is gathered and expressed in a summary form for purposes such as statistical analysis. A common aggregation purpose is to compile information about particular groups based on specific variables such as age, profession, or income.

Information System. A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes automated information system (AIS) applications, enclaves, outsourced information technology (IT)-based processes and platform IT interconnections.

Electronic Collection. Any collection of information enabled by IT.

Federal Personnel. Officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the United States (including survivor benefits). For the purposes of PIAs, dependents are considered members of the general public.

Personally Identifiable Information (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also,

*America's Job Link Alliance-Technical Support Privacy Impact Assessment*

information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

Privacy Act Statements. When an individual is requested to furnish personal information about himself or herself for inclusion in a system of records, providing a Privacy Act statement is required to enable the individual to make an informed decision whether to provide the information requested.

Privacy Advisory. A notification informing an individual as to why information is being solicited and how such information will be used. If PII is solicited by a Web site (e.g., collected as part of an email feedback/ comments feature on a Web site) and the information is not maintained in a Privacy Act system of records, the solicitation of such information triggers the requirement for a privacy advisory (PA).

System of Records Notice (SORN). Public notice of the existence and character of a group of 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. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.