



PRIVACY IMPACT ASSESSMENT (PIA)

**DoD Information System/Electronic Collection Name:
IT System Name and Acronym as it appears in the DITPR**

**DoD Component Name:
Please spell out all acronyms**

SECTION 1: IS A PIA REQUIRED?

- a. **Will this Department of Defense (DoD) information system or electronic collection of information (referred to as “electronic collection” for the purpose of this form) collect, maintain, use, and/or disseminate personally identifiable information (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).**

Note: Family members, dependants, and those who have not reported for duty as civilian employees or military personnel are considered members of the general public.

- (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 DoD IT Portfolio Repository (DITPR) as “Federal employees.”

b. If “No,” ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

Note: The Army System that updates DITPR is the Army Portfolio Management Solution (APMS).

Examples of acceptable DITPR entries if “No” is checked:

“A PIA is not required because this DoD information system or electronic collection does not 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.”

“A PIA is not required because this DoD information system or electronic collection is a National Security System.” See NIST Special Publication 800-59 for definition.

For those cases where a PIA is not required, proceed to Section 4, obtain the Program Manager (PM), component/local Information Assurance Manager/Official (IAM/IAO), and component/local Privacy Official signatures and forward the PIA to DA CIO/G-6 PIA Team via email to CIO_G6PIA@conus.army.mil.

c. If “Yes,” then a PIA is required. Proceed to Section 2.

Section 208 of the E-Government Act of 2002 requires all federal government agencies to conduct PIAs for all new or substantially changed systems that collects, maintains, or disseminates personally identifiable information.

Note: If the PII collected is strictly internal government operations related (i.e., Recall Roster, Internal Phone Roster, etc.. Must relate to a system or repository in addition the proponent does not update DITPR. DITPR will be updated with the monthly APMS push.

SECTION 2: PIA SUMMARY INFORMATION

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

- New DoD Information System New Electronic Collection
- Existing DoD Information System Existing Electronic Collection
- Significantly Modified DoD Information System

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- Yes, DITPR Enter DITPR System Identification Number

Note: Enter the DITPR ID Number, along with the ATTIRS ID Number in APMS

If the system is not registered in the DITPR, check "No". However, if there is a AITR (AITR Number can be found in APMS under the "Required Data" Form on Tab1 (Army Requirements) General Information Section), number (usually for applications) those could be listed here with an explanation of why the system isn't registered in DITPR.

- Yes, SIPRNET Enter SIPRNET Identification Number
- No

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- Yes Enter UPI

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

Note: A table of UPIs for the Presidential Budget is posted on the US Army CIO website <http://www.army.mil/ciog6/privacy.html>. To find the UPI for a particular IT System, search for the Acronym or system title. If not found then the system does not have a UPI number select NO."

Enter the UPI in the above text field in the following format:

- No

d. Does the DoD information system or electronic collection have a Privacy Act System of Records Notice (SORN)?

A Privacy Act SORN is 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 identifier.

Yes Enter Privacy Act SORN Identifier

Enter the SORN number only in the above text box. If there is a question regarding the existence of a SORN or if a SORN needs to be created or updated, contact your Privacy Official with any questions regarding SORN issues.

DoD Component-assigned designator, not the Federal Register number. Consult the Component Privacy Office for additional information or access DoD Privacy Act SORNs at: <http://www.defenselink.mil/privacy/notices/>

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

No

e. Does this DoD information system or electronic collection have an OMB Control Number?
Contact the Component Information Management Control Officer or DoD Clearance Officer for this information. This number indicates OMB approval to collect data from 10 or more members of the public in a 12-month period regardless of form or format.

Note: "The OMB Control Number table can be found on the US Army CIO web site (<http://www.army.mil/ciog6/privacy.html>). Search for the system title, if not found then the system does not have an OMB Control Number select NO.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order (E.O.) of the President, or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) Cite the authority for this DoD information system or electronic collection to collect, use, maintain and/or disseminate PII. Can be found under the "Authority for Maintenance of the System" on the SORN, this information can be copied and paste onto document.

(a) Whenever possible, cite the specific provision of the statute and/or E.O. that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/or E.O. does not exist, determine if an indirect statutory authority can be cited. An indirect authority may be cited if the authority requires the operation or administration of a program, the execution of which will require the collection and maintenance of a system of records, ((b) is valid only if no SORN exists).

(c) DoD Components can use their general statutory grants of authority (“internal housekeeping”) as the primary authority. The requirement, directive or instruction implementing the statute within the DoD Component should be identified, ((c) is valid only if no SORN exists).

Be sure to insert all Authority for Maintenance of the System found in the SORN that applies

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

Describe purpose - State why this system contains an individual’s PII and how it is used and protected. Write a brief detailed statement that a layman can understand.

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

Describe privacy risk - Describe (not list) the risks and safeguards.
Section 3d addresses physical, technical and administrative controls.

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

Within the DoD Component.

Specify (agencies, not systems)

Other DoD Components.

Specify (agencies, not systems)

Other Federal Agencies.

Specify (agencies, not systems)

State and Local Agencies.

Specify (agencies, not systems)

Contractor (enter name and describe the language in the contract that safeguards PII.)

Specify

Other (e.g., commercial providers, colleges).

Specify

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

Yes

No

(1) If "Yes," describe the method by which individuals can object to the collection of PII. **Include consequences, if any, if an individual objects.**

(2) If "No," state the reason why individuals cannot object.

j. 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. **Include consequences, if any, if an individual withholds their consent.**

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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

Privacy Act Statement

Privacy Advisory

Other

None

Describe each applicable format.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. (Component for Army refers to DA CIO/G-6.) Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

Only PIAs that pertain to the Public are posted on the CIO G6 web site (<http://www.army.mil/ciog6/privacy.html>).

A Component can 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

a. 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.

<input type="checkbox"/> Name	<input type="checkbox"/> Other Names Used	<input type="checkbox"/> Social Security Number (SSN)
<input type="checkbox"/> Truncated SSN	<input type="checkbox"/> Driver's License	<input type="checkbox"/> Other ID Number
<input type="checkbox"/> Citizenship	<input type="checkbox"/> Legal Status	<input type="checkbox"/> Gender
<input type="checkbox"/> Race/Ethnicity	<input type="checkbox"/> Birth Date	<input type="checkbox"/> Place of Birth
<input type="checkbox"/> Personal Cell Telephone Number	<input type="checkbox"/> Home Telephone Number	<input type="checkbox"/> Personal Email Address
<input type="checkbox"/> Mailing/Home Address	<input type="checkbox"/> Religious Preference	<input type="checkbox"/> Security Clearance
<input type="checkbox"/> Mother's Maiden Name	<input type="checkbox"/> Mother's Middle Name	<input type="checkbox"/> Spouse Information
<input type="checkbox"/> Marital Status	<input type="checkbox"/> Biometrics	<input type="checkbox"/> Child Information
<input type="checkbox"/> Financial Information	<input type="checkbox"/> Medical Information	<input type="checkbox"/> Disability Information
<input type="checkbox"/> Law Enforcement Information	<input type="checkbox"/> Employment Information	<input type="checkbox"/> Military Records
<input type="checkbox"/> Emergency Contact	<input type="checkbox"/> Education Information	<input type="checkbox"/> Other

If "Other," specify or explain any PII grouping selected. (i.e., passport information, NSPS data, etc.)

(2) **What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)? Where does the information come from. If information is obtained from system then state the system not the agencies.**

Describe.

(3) **How will the information be collected? Indicate all that apply. If you check "Other", describe in the text box provided.**

- Paper Format
- Telephone Interview
- Email
- Information Sharing from System to System
- Face-to-Face Contact
- Fax
- Web Site

Other (Describe)

(4) Why are you collecting the PII selected (e.g., verification, identification, authentication, data matching)?

Elaborate on why the collection of PII is necessary.

Describe

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

Elaborate on the intended use of the PII.

Describe

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

If there is a question as to whether a system derives new PII about an individual through data aggregation, please contact the CIO/G-6 PIA Team via email at CIO_G6PIA@conus.army.mil. (See Appendix)

Yes

No

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

c. Who has or will have access to PII in the DoD information system or electronic collection? Indicate all that apply.

(Question: Does the developer use real data for testing? If so then select Developers.) If you check "Other", describe in the text box provided.

Users Developers System Administrators Contractors

Other (Describe)

d. How will the PII be secured?

(1) Physical Controls.

Indicate all that apply not only to compound or building access but also to the room that the system resides in. If the system resides in a government facility then minimum controls are Security Guards and Identification Badges. If you check "Other", describe in the text box provided.

- | | | |
|--|---|--|
| <input type="checkbox"/> Security Guards | <input type="checkbox"/> Cipher Locks | <input type="checkbox"/> Identification Badges |
| <input type="checkbox"/> Combination Locks | <input type="checkbox"/> Key Cards | <input type="checkbox"/> Closed Circuit Television |
| <input type="checkbox"/> Safes | <input type="checkbox"/> Other (Describe) | |

(2) Technical Controls. Indicate all that apply. **If you check "Other", describe in the text box provided.**

- | | |
|--|---|
| <input type="checkbox"/> User Identification | <input type="checkbox"/> Biometrics |
| <input type="checkbox"/> Password | <input type="checkbox"/> Firewall |
| <input type="checkbox"/> Intrusion Detection System (IDS) | <input type="checkbox"/> Virtual Private Network (VPN) |
| <input type="checkbox"/> Encryption | <input type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input type="checkbox"/> External Certificate Authority (CA) Certificate | |
| <input type="checkbox"/> Common Access Card (CAC) | |
| <input type="checkbox"/> Other (Describe) | |

(3) Administrative Controls. Indicate all that apply. **If you check "Other", describe in the text box provided.**

- Periodic Security Audits
- Regular Monitoring of Users' Security Practices
- Methods to Ensure Only Authorized Personnel Access to PII
- Encryption of Backups Containing Sensitive Data

Backups Secured Off-site

Other (Describe)

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)? Check the appropriate box and enter the date. Ensure this information and APMS are the same. The area in APMS is APMS under the "Required Data" Form on "Tab4 (DITPR Compliance Tab1)" FISMA Section."

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 (DATO) Date Granted:

Interim Authorization to Test (IATT) Date Granted:

No, this DoD Information system does not require certification and accreditation.

f. 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.

The following is an example response:

Use: This statement has nothing to do with the question. Replace with "Controls are in place and effective in mitigating all risks to an acceptable level for protecting systems and data up to and including 'For Official Use Only' Privacy Act data.

g. For existing DoD information systems or electronic collections, what measures have been put in place to address identified privacy risks? The following suggested wording may be tailored as appropriate to the system in question.

Describe:

Due to the level of safeguarding addressed in Section 3d, we believe the risk to individuals' privacy to be minimal. There are no identifiable privacy risks at this time.

h. For new DoD information systems or electronic collections, what measures are planned for implementation to address identified privacy risks? Same as question g.

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 or Designee (i.e., at system local level - system owner/POC)

Signature: _____

Name: _____

Title: _____

Organization: _____

Work Telephone Number: _____

DSN: _____

Email Address: _____

Date of Review: _____

Other Official (Usually the Command IAM/IAO - at system local level)

Signature: _____

Name: _____

Title: _____

Organization: _____

Work Telephone Number: _____

DSN: _____

Email Address: _____

Date of Review: _____

Other Official (Usually the Command Privacy Officer- at system local level)

Signature: _____
Name: _____
Title: _____
Organization: _____
Work Telephone Number: _____
DSN: _____
Email Address: _____
Date of Review: _____

At this point in the process, forward the signed PIA to the CIO/G-6 PIA Team (CIO_G6PIA@conus.army.mil).

Army Senior Information Assurance Officer or Designee (NETCOM)

Signature: _____
Name: _____
Title: _____
Organization: _____
Work Telephone Number: _____
DSN: _____
Email Address: _____
Date of Review: _____

Army Privacy Officer (PO)

Signature: _____

Name:

Title:

Organization:

Work Telephone Number:

DSN: _____

Email Address:

Date of Review: _____

Army CIO/G-6 (Reviewing Official):

Signature: _____

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review: _____

Once the Army CIO/G-6 has approved and signed the PIA, the CIO/G-6 PIA Team will forward a copy of the PIA to OSD. OSD will forward to OMB, as required.

The CIO/G-6 PIA Team will update DITPR, forward a copy of the approved PIA to the submitting command and post the PIA summary on the CIO/G-6 web site.

Publishing:

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

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD 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.

DoD 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 of Information. 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, DoD dependents are considered members of the general public.

Personally Identifiable Information. 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, 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 DoD 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 an 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.