Department of the Army
Privacy Impact Assessment (PIA) Guide

OVERVIEW

Pursuant to the E-Government Act of 2002[1], the Department of the Army (DA) must comply with statutory requirements to analyze and ensure personally identifiable information (PII)[2] in electronic form is collected, stored, used, shared, and managed in a manner that protects privacy. The DA fulfills this requirement through the completion of DOD Form 2930, Privacy Impact Assessment (PIA). This document will serve as a guide to assist in the completion of the PIA for the DA.

A PIA is an analysis of whether PII in electronic form is collected, stored, protected, or disseminated in a manner that mitigates potential privacy risk. The purpose of a PIA is to demonstrate that system owners, program managers, and developers have incorporated privacy protections throughout the entire life cycle of a system and or electronic collection.

A PIA must be completed for ALL information systems/electronic collections to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy. In the case where no PII is collected, maintained, used, and/or disseminated, the PIA is still required as well as an ATO and a Certificate of Networthiness, where applicable. The completion of a PIA is a mandatory requirement and requests for waivers will not be granted.[3]

A PIA should be conducted **before**:

- Developing, purchasing, or contracting new information systems or electronic collections;
- Converting paper-based records to electronic records;
- De-anonymizing data resulting in PII; and
- Significantly changing systems or electronic collections[4].

Local Command Privacy Officials and PIA point of contact must submit **all** PIAs electronically via the Privacy Impact Assessment Team Collaboration Hub (PATCH). PATCH is a SharePoint collaboration tool used to manage the submission and approval of PIAs.

Note: Every three (3) years, in conjunction with the recertification and reaccreditation process, PIAs must be reviewed, updated, and resubmitted in PATCH. In addition, if there are significant changes to the system that create new privacy risk, a PIA must be resubmitted.

When required under the Privacy Act of 1974, the information system or electronic collection may require the development of a System of Record Notice (SORN) and other related Federal requirements, such as approval from the Office of Management and Budget (OMB) and the National Archives and Records Administration (NARA).

---

[1] Section 208 of Public Law 107-347.

[2] Personally Identifiable Information (PII) is Information which can be used to distinguish or trace an individual's identity, such as name, Social Security Number, DoD ID, and biometric records, 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, and mother's maiden name.

[3] PIAs submitted in PATCH must be accompanied by a copy of an approved and current ATO. Applications must have a NETCOM Certificate of Networthiness ID Number before submitting the PIA.

[4] See Section 1 item (b) for more details on activities that constitute significant changes.

The DoD PIA policy and guidance is detailed in DoDI 5400.16*, DoD Privacy Impact Assessment (PIA) Guidance*. The Army policy on PIAs is provided in Army Regulation (AR) 25-1, *Army Information Technology*, and AR 25-22, *The Army Privacy Program*.

Questions regarding this guide may be directed to the Army Privacy Office (APO) at usarmy.belvoir.hqda-oaa-ahs.mbx.army-privacy-sorn-ssn-reduction@mail.mil and the Chief Information Officer (CIO) at cio-g6.pia.inbox@mail.mil.

PRIVACY IMPACT ASSESSMENT
DD FORM 2930

1. **DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:**
   Insert the information system/electronic collection name. This name should match or be similar to what is in the Army Portfolio Management Solution (APMS), the DOD IT Portfolio Repository (DITPR), Enterprise Mission Assurance Support Service (eMass), or Army Information Technology Repository (AITR).

   Example: Civilian Human Resources Regional Reports System **not** CHRRR 2017. Spell out all acronyms.

2. **DOD COMPONENT NAME:**
   Insert the name of the Component responsible for the maintenance and operation of the information system/electronic collection.

3. **PIA APPROVAL DATE:**
   This is the date the PIA is approved by the Army CIO Reviewing Official – not the date the PIA was drafted or submitted. CIO will complete this section once the document receives final approval.

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

Pursuant to the E-Government Act of 2002, Federal agencies are required to make PIAs available to the public via a public-facing website. Therefore, the contents in the PIA should be clear, unambiguous, and understandable to the public. Only Section 1 of this form will be available to the public. Do **not** include information that would raise security concerns, or reveal classified or sensitive information.

a) The PII is:

Whom is the PII in the information system/electronic collection about?

- *From members of the general public*
  - Members of the general public include (but are not limited to):
    - Individuals, partnerships, associations, and corporations,
    - State, Tribal, or Local governments,
    - Foreign Nationals,
    - Retired Federal employees, veterans, and reservists, and
    - Family members and dependents of service members or Federal employees.
- *From both members of the general public and Federal employees and/or Federal contractors*
  - See directly above and directly below for group descriptions.

- *From Federal employee and/or Federal contractors*
    - Federal employees are members of an internal population, but a full and complete PIA is still required. Federal employees include Officers and employees of the Government of the United States, members of the uniformed services (including member of the Reserve Components), and individuals entitled to receive immediate or deferred retirement benefits[5].
    - Federal contractors are individuals who enter into a contract with the United States or any department or agency thereof for the rendition of personal services; or furnishing any material, supplies, or equipment; or selling any land or buildings; and if the payment for the performance of the contract or payment for the material, supplies, equipment, land, or building is to be made in whole or in part from funds appropriated by the Congress[6].
- *Not Collected*
    - Do not select this option if PII is stored, maintained, used, or disseminated by the information system/electronic collection. Only select this option if there is no PII in the entire lifecycle of the information system/electronic collection.
    - If PII is not collected, stored, maintained, used or disseminated, complete Sections 1, 3 and 4.

b) The PII is in:

This question will help individuals understand where the PII is being collected, maintained, used, or disseminated.

- *New DoD Information Systems*
    - An *Information System* is a set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information – including Automated Information Systems (AIS) applications, enclaves, outsourced information technology (IT) based processes and platform IT interconnections.
    - Select this option if the system is new to the Army network.
- *Existing DoD Information Systems*
    - See definition of *Information System* directly above. Select this option if the Army system has an Authorization to Operate (ATO), but was not assessed with a PIA during the ATO process[7] or if the PIA has expired.

[5] 5 U.S. Code § 552a(a)(13).
[6] 11 CFR 100.10.
[7] DODI 5400.16, DoD Privacy Impact Assessment (PIA) Guidance.

- *Significantly Modified DoD Information Systems*
  - Per the E-Government Act of 2002 and DoDI 5400.16, significant modifications includes:

Significant Management Changes	Example: Employing new relational database technologies or web-based processing to access multiple data stores.
Significant Merging	Example: Merging and aggregation of multiple databases into one central repository.
New Public Access	Example: Enabling user-authenticating technology, such as passwords to an information systems accessed by members of the public.
Commercial Sources	Example: Adding PII obtained from commercial or public sources *into* an existing IT systems or databases.
New Interagency Uses	Example: Working with other non-DoD Federal agencies on shared functions involving exchanges of PII, such as cross cutting E-government initiatives.
Alteration in Character of Data	Example: Adding a new data element not previously collected, such as health or financial information.

- *New Electronic Collection*
  - **Any** new collection of information enabled by IT. Select this option if this specific data collection (the type and manner) did not exist before. For example, if the data was collected electronically before, but in a different electronic format, platform, website, etc..
- *Existing Electronic Collection*
  - An electronic collection of information currently in use, but not previously assessed through a PIA or if the PIA has expired.

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

Describe the purpose of the information system or electronic collection in a way that a nontechnical individual could understand. The description should be a minimum of four sentences and should: (1) Describe the system's purpose; (2) Walkthrough a primary transaction performed on or by the system; and (3) Include a general overview of the modules, subsystems, and their functions.

d) Why is the PII collected and/or what is the intended use of the PII?

Describe how and why the information system or electronic collection collects, uses, maintains, and/or disseminates PII in electronic form. Include the entire lifecycle of the PII (e.g., **collection, retention, processing** - how it will be used to complete a task or assignment (e.g., use to verify eligibility, to identify an individual, authenticate, etc.,) **disclosure**, and **destruction**/disposal). For example, if the PII will be used in or by a system to verify eligible individuals for a benefit, and the results will be presented in a report, be sure to include if and why the report will be stored and how it will be used.

e) Do individuals have the opportunity to object to the specific uses of their PII?

This question is directed at the Fair Information Practice Principle (FIPPS)[8] of *Transparency* to determine if the Army is transparent and provides notice to the individual about the use and dissemination of their PII.

Indicate whether the individual has an opportunity to decline or opt-out of some or all uses of their PII that is collected, maintained, used, or disseminated by the information systems. Provide additional details based on the selected response. For example, explain if the individual does not have the opportunity to object because the information in the system is retrieved from another information system and not the individual.

f) Do individuals have the opportunity to consent to the specific uses of their PII?

This question is directed at the FIPPS principle of *Transparency* to determine if the Army is transparent and provides notice to the individual regarding the use of their PII.

Indicate whether the individual has the opportunity to consent to specifics uses (or if the consent is given to cover all uses (current or potential)) of their information. Provide additional details based on the selected response. For example, explain if the individual does not have the opportunity to object because the information in the system is retrieved from another information system and not the individual.

[8] In 1972, the Advisory Committee on Automated Personal Data Systems explored the impact of computerized record-keeping on individuals and proposed a Code of Fair Information Practice Principles (FIPPs). FIPPs has evolved into eight (8) generally accepted principles that formed the basis for all subsequent codes and laws related to information collection, especially the Privacy Act of 1974.

g) When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or Privacy Advisory must be provided.

This statement refers to whether the individual is aware that their PII is going to be collected, maintained, used, and/or disseminated before the collection occurs**.**

Pursuant to the Privacy Act of 1974[9], as amended, notice – also known as a PAS, is required when information collected will be maintained in a Privacy Act System of Records (SOR)[10], regardless of the medium used to collect the information (i.e., forms, personal interviews, telephonic interviews, and other methods). Also, provide a PAS and or Privacy Advisory/Notice when individuals are asked to confirm that their data previously collected is still current and correct. Individuals do not have to sign the PAS or the Privacy Notice.

The PAS should be in the following format complete with headings: **Authority**, **Principle Purpose**, **Routine Uses**, and **Disclosure**. If the PAS does not clearly identify those four (4) sections, the PIA will be rejected. The contents from each section of the PAS should be similar and align to the System of Records Notice (SORN) that covers the information system or electronic collection.

Authority: The legal authority for collecting the information – Federal statute, executive order (EO), regulation.

Principle Purpose: The purpose(s) for collecting the information and how DA will use it.

Routine Uses: To whom DA may disclose the information to outside of the Department and for what purposes.

Disclosure: Mandatory or Voluntary: Indicate whether providing the information is mandatory or voluntary. Collections can only be mandatory when a Federal statute, EO, regulation, or other lawful order specifically imposes a duty on the person to provide the information; and the person is subject to a specific penalty for failing to provide the requested information.

Include the number and citation of the SORN applicable to the information system or electronic collection.

PAS Example:

PRIVACY ACT STATEMENT

AUTHORITY: 10 U.S.C.; Public Law 104-134 (April 26, 1996)

PRINCIPAL PURPOSE(s): To solicit and collect information from Army Competitive Category Colonels and General Officers for the purpose of career management and professional development.

ROUTINE USE: The information gathered will be used for assignment, career management, and professional development purposes. Individual officers will have the ability to submit assignment preferences, as well as personal data relating to their careers. Human resource managers will use this information in the slating and development processes. Management reports will be used to review progress and slates at a macro level. All users' personally-identifiable information and actions while interacting with the information system will be collected and retained for information assurance purposes.

DISCLOSURE: Voluntary. Public Law 104-134 (April 26, 1996) requires that any person doing business with the Federal Government furnish a social security number. This is an amendment to title 31, Section 7701. Furnishing the social security number, as well as other data, is voluntary, but failure to do so may delay or prevent action.

[9] 5 U.S.C. § 552a.

[10] A SOR is a group of records (i.e., a collection or grouping of information about an individual that is maintained by an agency) about an individual that is retrieved by their name or other unique identifier. See item (k) of this Section for more details.

For additional guidance on drafting a PAS, please refer to OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act* or contact your local Command Privacy Official.

Privacy Advisory. A Privacy Advisory is used when an individual is asked to provide personal information about themselves that will not be stored in a Privacy Act SOR. The Advisory should inform the individual as to why the information is being solicited and how the information will be used. It should include a brief description of the Army's practices with respect to the PII, if applicable, that the Army is collecting, maintaining, using, or disseminating information. All solicitation methods in any format, including but not limited to, forms, paper, website, web portal, e-mail, should include a Privacy Advisory.

A Privacy Advisory should be placed or provided near or before the collection of information. For example, on a website near the data fields collecting data or if face-to-face, provided verbally or printed/posted before information is solicited from the individual. Also, use a Privacy Advisory when asking individuals to confirm that their data is current and correct.

h) With whom will the PII be shared through data exchange, both within your DOD Component and outside your Component?

Sharing PII can create and/or increase privacy risk. Indicate with whom the PII collected will be shared.

Sharing PII outside the Army must be for a purpose compatible with the purpose for which the PII was collected. If this information system is a Privacy Act SOR (*see* details and definition in item (k) of this section below), disclosures outside DoD must include those published in the SORN under the section "Routine Uses". In addition, a Memorandum of Understanding (MOU), Data Sharing Agreements, etc., may be required. Consult with your local Command Office of the Judge Advocate General (OTJAG) and the APO.

i) Source of the PII collected is:

Indicate where or from whom the PII in the information system or electronic collection will be obtained. Indicate if the PII will be collected from another system or an individual. If PII is collected from information systems, including databases or commercial systems, list the name of each system and/or database in the text box provided.

Tip: The listed source of the PII should be included in item (d) of this section of the PIA – which describes the lifecycle of the PII.

j) How will the information be collected:

Indicate how the information will be collected. Select **all** that apply. If information is being collected face-to-face or via a telephone interview, the DA is still required to inform the individual why their information is being collected and how it will be used. For information collected via Official Form(s), provide the Form Number in the text box provided.

Tip: The method of collection should be described in item (d) of this section of the PIA –which describes the lifecycle of the PII.

k) Does this DoD Information system or electronic require a Privacy Act System of Records Notice (SORN)?

Pursuant to the Privacy Act of 1974, agencies are required to publish a SORN in the Federal Register (FR) for newly created and revised SORs. A System of Records (SOR) is a group of records[11] about an individual in which the records about that individual **is** actually retrieved by the individuals name or other unique identifier (e.g., symbol, social security number, DoD ID Number, etc.). **The information must actually be retrieved by a personal identifier** to trigger the SORN requirement of the Privacy Act.

Provide the SORN System Identifier and if a SORN has not published, enter the date the draft SORN was sent to APO. **An example of a SORN Identifier is A0100-1-123 ABC.** The FR citation is not the SORN Identifier. Note: If an exemption is claimed for the system, the DoD Privacy Office requires The Army General Counsel to review and approve the exemption.

DA SORNs are available at https://www.rmda.army.mil/privacy/sorns/. For more information, see OMB Circular A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act*, AR 25-22, The Privacy Program, or consult with the APO at usarmy.belvoir.hqqa-oaa-ahs.mbx.army-privacy-sorn-ssn-reduction@mail.mil.

l) What is the National Archives and Records Administration (NARA) approved, pending, or general record scheduled (GRS) disposition authority for the system or for the records maintained in the system?

NARA is the oversight agency responsible for appraising all Federal records[12], approving their disposition, providing program assistance and storage, evaluating records management programs, and serving as the final custodian of permanent records. Disposition refers to actions taken with regard to Federal records that are no longer needed for current government business as determined by their appraisal pursuant to legislation, regulation, or administrative procedure.

NARA assigns Job Numbers and uses GRS, issued by the Archivist of the United States, to provide mandatory instructions for the disposition of records (including the transfer of permanent records and disposal of temporary records) when the agency no longer needs the records. The Standard Form (SF) 115, *Disposition of Federal Records*, is used to obtain authority for the disposition of records.

To search for Army Consolidated Record Schedules see https://www.arims.army.mil/ARIMS/RRSA/Search.aspx. Also, consult with your local Command Records Management Officer. The PIA will not be approved if the records in the information system or electronic collection are not scheduled and do not have an approved retention schedule.

[11] Under the Privacy Act of 1974, the term "record" means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print.

[12] Records include all books, papers, maps, photographs, machine-readable materials, or other documentary materials, regardless of physical form or characteristics, made or received by an agency of the United States Government under Federal law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of the data in them. See 44 U.S.C. 3301.

m) What is the authority to collect information?

List all statutory and regulatory authorities that permit the collection of information. Authorities listed here should be specific to the collection and **included in the authorities provided in the SORN**. Be sure to include the citation **and** its title. Authorities provided must be current and specific to the Army or DOD-Wide. SORNs are **not** acceptable authorities for collection. Acceptable authorities include, but are not limited to, DoD Directives and Instructions, Army Regulations (AR), EOs, Unites State Code (USC), Public Law (Pub. L.), etc.

Examples: 10 United States Code (USC) 612-646, 3013, Secretary of the Army, or
DODD 1300.19, Joint Officer Management Program

n) Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (OMB) Control Number?

Pursuant to the Paperwork Reduction Act (PRA) of 1995[13], agencies are required to obtain OMB approval and a Control Number[14] before collecting most types of information from ten (10) or more members of the public regardless of whether the collection is mandatory, voluntary, or required to obtain or retain a benefit. See Section 1(a) for categories of individuals included in members of the public. Public information collection request come in a variety of formats (e.g., surveys, forms, or collections). The instrument and method used for collection will require a PAS and/or a Privacy Advisory/Notice. See Section 1(g) for more information regarding a PAS and Privacy Advisory/Notice.

Where applicable, list all OMB Control Numbers, collection titles, and expiration dates. If the collection does not have an OMB Control Number, explain why the OMB Control Number is not required. If the approval is pending, provide the date for the 60 and/or 30-day notice and the FR citation. For more information visit the RMDA PRA website at https://www.rmda.army.mil/records-management/PRA/index.html, and consult with your local Command Army Information Management Control Officer (IMCO).

[13] Pubic Law No. 96-511.

[14] OMB assigns a Control Number to approved information collection request that the agency must display on the information collection. OMB Control Numbers are formatted NNNN-XXXX, where the 'N' is the agency code and the 'X' is the number that uniquely identifies the collection.

SECTION 2: PII RISK REVIEW

Responses provided in this section will **not** be available to the public.

a) What PII will be collected?

Select all the data elements collected, maintained, used, or disseminated by the information system or electronic collection. If the data elements being collected, maintained, used, or disseminated is not listed or you are unsure about its category or PII grouping, select the other box and enter the data element(s). Be as specific as possible.

Eliminate any use of SSNs that is not justified through appropriate authorities and use alternatives to the SSN whenever possible. Examples of SSN alternatives include, but not limited to, DoD ID Numbers, system-specific identifiers, net centric environment, and biometrics. **If** a SSN (in any form) is collected, maintained, used, and/or disseminated by the information system or electronic collection, a SSN Justification Memo is **required**. If the information system or electronic collection does not collect, maintain, use or disseminate a SSN in any form, a Justification Memo is not required.

Tip: The data elements selected should be similar to the data types listed in the SORN's *Categories of Records in the System*.

SSN JUSTIFICATION

The DA is required to minimize the collection and use of SSNs as a unique personal identifier. Use of SSNs, in any form – **including truncated**, on forms and IT systems, requires a **current** SSN Justification Memo. The PIA will be rejected if the information system or electronic collection collects or uses SSNs, and there is no accompanying Justification Memo.

Justification Memos should be prepared in accordance with DoDI 1000.30, *Reduction of Social Security Number Use within DOD*. The Memo should identify an explanation why the SSN is necessary, the appropriate acceptable use from DoDI 1000.30-Enclosure 2, the applicable SORN, authorities (should be consistent with the SORN, if applicable), and safeguards implemented to protect the SSN. Send all draft SSN Justification Memos to the APO for approval **before** staffing it to the Senior Executive Service (SES) or General Officer for approval and signature. Justification Memos expire two (2) years after the signed approval date.

For additional information, see the *Social Security Number (SSN) Justification Guide* at https://www.rmda.army.mil/privacy/docs/SSNjustification%20Guide20170620.pdf. If you do not have a SES or General Officer, contact the APO at usarmy.belvoir.hqda-oaa-ahs.mbx.army-privacy-sorn-ssn-reduction@mail.mil.

b) What is the PII confidentiality impact level?

Confidentially is preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information[15]. The PII confidentiality impact level—low, moderate, or high—indicates the potential harm that could result to individuals and/or the organization if the PII is inappropriately accessed, used, or disclosed[16]. The PII confidentiality impact is **not always the same as the** Federal Information Processing Standard (FIPS) 199 impact level.

[15] 44 U.S.C., Sec. 3542.
[16] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

Factors in Determining Confidentiality Impact Levels[17]:

Identifiability	Consider how easily PII could identify specific individuals. PII data composed of individuals' names, fingerprints, or SSNs uniquely and *directly* identify individuals, whereas PII data composed of individuals' ZIP codes and dates of birth can *indirectly* identify individuals or can significantly narrow large datasets.
Quantity of the PII	Consider how many individuals are identified in the information (e.g., number of records). For example, breaches of 25 records and 25 million records may have different impacts. However, a low impact level should not be assigned for a PII dataset simply because it contains a small number of records.
Sensitivity	Consider the sensitivity of each individual PII data field, as well as the sensitivity of the PII data fields together. For example, an individual's SSN, medical history, or financial account information is generally considered more sensitive than an individual's phone number or ZIP code.
Context of Use	Consider the purpose for which PII is collected, stored, used, processed, disclosed, or disseminated. Examples of context include, but are not limited to, statistical analysis, eligibility for benefits, administration of benefits, research, etc. For example, law enforcement investigations could be compromised if the mere fact that information is being collected about a particular individual is disclosed.
Location of the PII	Consider the nature of authorized access to PII. When PII is accessed more often or by more people and systems, there are more opportunities for the confidentiality of the PII to be compromised. Another aspect of the nature of access to PII - is the PII being stored on or accessed from teleworkers' devices or other systems, such as web applications, outside the direct control of the organization.
Legal Obligations	Consider obligations to protect the PII and if it is subject to laws, regulations, or other mandates governing the obligation to protect personal information, such as the Privacy Act of 1974, OMB memoranda, and the Health Insurance Portability and Accountability Act of 1996 (HIPAA).

[17] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

Impact Levels[18]:

- Low - The loss of confidentiality could be expected to have a limited adverse effect on the individual(s) affected. Adverse effect result in minor financial loss; or result in minor harm to individuals.
- Moderate - The loss of confidentiality could be expected to have a serious adverse effect on the individual(s) affected. Serious adverse effect could be result in significant harm to individuals that does not involve loss of life or serious life threatening injuries.
- High - The loss of confidentiality could be expected to have a severe or catastrophic adverse effect on individual(s) affected. Severe or catastrophic adverse effects results in major financial loss; or result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.

c) How will the PII be secured?

Select **all** the Physical, Administrative, and Technical controls used to safeguard and secure the PII collected, maintained, used, or disseminated by the information system.

Physical controls are physical measures put in place to protect an information system, related buildings, and equipment, from natural and environmental hazards, and unauthorized intrusion.

Administrative controls are actions, policies, and procedures in place to protect information and to manage the conduct of the Army's employees and contractors in relation to the protection of the information.

Technical controls are the technology-based controls used as a basis for controlling the access and usage of the information.

d) What additional measures/safeguards have been put in place to address privacy risk for this information system or electronic collection?

Discuss any additional safeguards pertaining to the information system or electronic collection that would reduce the risk to privacy.

[18] NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII).

SECTION 3: RELATED COMPLIANCE INFORMATION

Responses provided in this section are **not** available to the public.

a) Is this DOD Information System registered in the DOD IT Portfolio Repository (DITPR) or DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) or Risk management Framework (RMF) Tool?

The DITPR was designated as the Enterprise Shared Space for IT Portfolio Management data for all DoD business IT systems. SIPRNET is for classified information systems. Each system on the Army network should have a DIPTR number or an AITR number. All systems must be registered in APMS. Once a system is registered in APMS it will be assigned a AITR number. Note the PIA will not be approved by CIO-G6 if the system does not have an ATO.

b) DoD information systems require assessment and authorization under the DoD Instruction 8510.01, "Risk Management Framework for DOD Information Technology".

DoDI 8510.01, *RMF for DoD IT*, March 12, 2014, cancels the previous DoD Information Assurance Certification and Accreditation Process (DIACAP) and institutes a new, risk-based approach to cybersecurity policy, and assigning responsibilities for executing and maintaining the RMF. Cybersecurity requirements for DA information technologies will be managed through the RMF consistent with the principals established in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems*. Provide the status of the assessment and authorization.

NOTE: If a system's ATO is expiring within 60-days the PIA will NOT be reviewed or approved by the CIO. Systems with a pending accreditation or re-accreditation will NOT be reviewed or approved by the CIO. PIAs submitted to CIO for systems with a pending accreditation or in the re-accreditation process will be held by the CIO for 60 days before the PIA is rejected, cancelled and removed from the PIA review process.

Parent/Child/Dependencies: Child/dependent systems can leverage the Parent ATO if the child system is registered under the Parent in APMS. The Parent must have the child dependent listed in APMS.

c) Does this DOD Information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

As part of the budget process, OMB Circular A-11, requires Federal agencies to analyze, track, and evaluate the risk, including information security risk, for all major capital investments of information systems. All new and existing investments identified in the DoD IT portfolio are assigned a number called a UII, formerly Unique Project Identifiers (UPIs). Each investment has a UII for identification and tracking purposes. For more information, consult with your local Command IT Budget point of contact.

SECTION 4: REVIEW AND APPROVAL SIGNATURES

Responses provided in this section are **not** available to the public.

Each signature block must be completed before the PIA is finalized.

Section a requires a signature from the Program Manager.

Section b requires a signature from another Official.

Section c requires a signature from the local Command Privacy Official.

Section d requires a signature from the Chief of APO.*

Section e requires a signature from the Chief of RM.*

Section f requires a signature from the Senior Information Security Officer.**

Section g requires a signature from the Senior Component Official for Privacy (SCOP)*

Section h requires a signature from the Component CIO Reviewing Official.**

*Indicates actions coordinated through the APO.
**Indicates actions coordinated through CIO-G6.

Note: Review and approval times of the PIA vary based on the complexity of the system, the timeliness of responses for additional information and the development of additional artifacts, where applicable (e.g., SORN, SSN Justification Memo, retention schedule, etc.).