



PRIVACY WORKSHOP



OPENING REMARKS

Mr. Robert Dickerson

Chief

Army Freedom of Information
and Privacy Office

Mr. Gary Evans

Senior Management Analyst
CIO Management Services
Office of the DoD CIO

Defense Privacy Office
Office of the Secretary of
Defense



AGENDA

- Definitions
- Responsibilities:
 - Privacy Officer
 - Systems Manager
 - Information Assurance Official
- How to:
 - Complete a System of Records Notice (SORN)
 - Complete a Privacy Impact Assessment (PIA)
- Other Privacy Initiatives (time permitting)
 - SSN Reduction Plan
 - Forms that contain SSN's
 - Local SORN Compliance
 - Upcoming Privacy training
- Questions



Definitions

- **SYSTEM OF RECORDS:**
 - Group of Records
 - Under the control of the Agency
 - Retrieved by name, SSN, or other personal identifier
 - If records are not retrieved by an individuals name or personal identifier, they are not a PA system of records
- **SYSTEM OF RECORDS NOTICE (SORN):**
 - A description of a group of records that:
 - Is published in the Federal Register
 - Authorizes the collection of Personally Identifiable Information (PII)



Definitions

- **Personally Identifiable Information (PII)**

- PII refers to 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.*

*OMB Memorandum, M-07-16, 22 May 2007

- **Privacy Impact Assessment (PIA)** is an analysis of how information is handled:

- to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
- to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and
- to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.*

*Army CIO/G-6 Memo, Privacy Impact Assessment Guidance, 12 Dec 06



Responsibilities

- **PRIVACY OFFICERS:**
 - A Privacy Official is appointed at Command levels throughout the Army
 - Execute the privacy program in functional areas and activities under their responsibility.
 - Ensure that Privacy Act records collected and maintained within the Command or agency are properly described in a Privacy Act system of records notice.
- **Ensure:**
 - No undeclared systems of records are being maintained.
 - A Privacy Act Statement is provided to individuals when information is collected that will be maintained in a system of records.
 - Each Privacy Act system of records notice within their purview is reviewed biennially.
 - Updated or new System of Records Notices are submitted to the Army Privacy Office



Responsibilities

- **SYSTEM MANAGERS:**
 - Prepare new, amended, or altered Privacy Act system of records notices and submit to Command Privacy Office for review.
- **Ensure:**
 - Appropriate procedures and safeguards are developed, implemented, and maintained.
 - All personnel with access to each system are aware of their responsibilities for protecting personal information being collected and maintained under the Privacy Act.
 - Each Privacy Act system of records notice within their purview is reviewed biennially



Responsibilities

- **Information Assurance Official**

- AR 25-2 para **5–8. Designated approving authority**
 - a. *The DAA is vested with the authority to formally assume responsibility for operating an IS at an acceptable level of risk. The DAA must weigh the operational need for the systems capabilities, **the protection of personal privacy**, the protection of the information being processed, and the protection of the information environment, which includes protection of the other missions and business functions reliant on the shared information environment.*
- Provides a unified approach to protect information stored, processed, accessed, or transmitted by Information Systems
- Consolidates and focus' Army efforts in securing information
- Risk management approach for implementing security safeguards



SORN Review/Update

- Download copy of SORN into word doc from www.defenselink.mil/privacy/notices/army
- Review and edit the 18 categories of the SORN using the track changes feature
- Coordinate SORN within command and obtain authorized signatures on Certification
- Activity Privacy Officer will provide to the Army Privacy Office



SORN Categories

1. System identifier
2. System name
3. System location
4. Categories of individuals covered by the system
5. Categories of records in the system
6. Authority for maintenance of the system
7. Purpose(s)
8. Routine uses
9. Storage
10. Retrievability
11. Safeguards
12. Retention and disposal
13. System manager(s) and address
14. Notification procedures
15. Record access procedures
16. Contesting record procedures
17. Record source categories
18. Exemptions claimed for the system



System of Records Notice

1. **System Identifier: “A0025-55 OAA”**

Already assigned and indicated. If changes are necessary, The Army Privacy Office will assign the notice number. Example: A0025-55 OAA: The first letter “A” indicates “Army”, the next number “25-55” Represents the publication series number related to the subject matter, and the final letter group “OAA” shows the system manager's command, in this case, Office of the Administrative Assistant.

2. **System Name:**

Already assigned and indicated. If changes are needed please ensure that it identifies the system's general purpose. This field is limited to 55 characters.



System of Records Notice

3. System Location:

Specify the address of the primary system and any decentralized elements, including automated data systems with a central computer facility and input or output terminals at separate locations. For geographically or organizationally decentralized system locations, indicate that the official mailing addresses are published as an appendix to the Component's compilation of system of records notices. If no address directory is used, the complete mailing address of each location where a portion of the record system maintained must appear in this caption or give the title and mailing address of the person who can provide a complete listing of locations. Post Office boxes are not locations. Provide the complete mailing address of each location/site maintaining the system of records. Use street address, 2-letter state abbreviations and 9-digit ZIP Codes. Spell out office names. Do not use office symbols.



System of Records Notice

4. Categories of Individuals Covered by the System:

Identify in clear, non-technical terms, individual's records being maintained.

- living person who is a citizen of the U.S.
- alien lawfully admitted for permanent residence.
- Examples: “Department of the Army civilian employees”; “contractors”; “active duty Army personnel”; “civilian employees from other federal agencies”.
- Avoid using broad descriptions like “all Army personnel” unless that is truly accurate.
- Corporations, partnerships, sole proprietorships, professional groups, businesses, and other commercial entities are not “individuals”.



System of Records Notice

5. Categories of Records in the System:

Describe in clear, plain language, all categories of records and items of PII in the system.

- List only documents and forms actually kept in the system.
- Do not identify source documents that are used to collect data and then destroyed.
- Provide the public as much detailed information about the PII.
- If your system of records notice covers a database, it is a good idea to get a print out of the data elements so that you can see all items of PII and records being maintained.
- Do not use overly broad terms or identify forms unless accompanied by a brief explanation.
- The Privacy Impact Assessment may require an update to include PII reflected in the Systems Notice.



System of Records Notice

6. Authority for Maintenance of the System:

A Federal law or Executive order of the President must authorize the collection and maintenance of a system of records. Cite the specific law or Executive Order that Authorizes the maintenance of the system. Whenever possible, cite the specific provisions of the statute or executive order. Cite the DoD directive/instruction or Department of the Army Regulation(s) that authorizes the Privacy Act system of records. This is especially Important when using general statutory grants of authority statute (“internal housekeeping”) as the primary authority. Always include titles with the citations. Note: Executive Order 9397 authorizes using the SSN as a personal identifier. Include this in authority whenever the SSN is used to retrieve records. EO 9397 will never stand alone as an authority to collect and maintain information under the Privacy Act. NOTE: The Privacy Impact Assessment may require an update to include authority reflected in the Systems Notice.

7. Purpose(s):

List the specific purposes for establishing and maintaining the system of records by your activity. Explain: why you collect this information and how the information is used in the course of DoD business.



System of Records Notice

8. Routine Use(s):

List all non-DoD agencies and entities including private sector entities that will routinely provided access to the data or be given the data upon request. List The specific activity or element within the agency/entity to which the record may be disclosed. for example: "To the Veterans Administration" or "To state and local health agencies". For each routine user identified, include a statement as to the purpose or purposes for which the record is to be released to that activity. Do not use general statements, such as "To other federal agencies as required" or "To any other appropriate federal agency". Routine uses shall be written as follows: "To user, to uses, and what they do with the information, and for the purposes of (objective)."



System of Records Notice

9. Storage:

State the medium in which DA maintains the records; for example, in file folders, card files, microfiche, computer, or a combination of those methods. Storage does not refer to the container or facility in which the records are kept. Example: “Maintained in paper files and on electronic storage mediums”.

10. Retrievability:

State how the Army retrieves the records; for example, by name, by Social Security Number, by name and Social Security Number, by fingerprints or by voiceprints. To be subject to the Privacy Act, records within a system of records must be retrieved by a personal identifier.



System of Records Notice

11. Safeguards:

Identify the system safeguards; for example, storage in safes, vaults, locked cabinets or rooms, use of guards, visitor controls, personnel screening, computer systems software, and so on. Describe safeguards fully without compromising system security. Describe the facility/building safeguards, then the room, then the computer/file cabinet. Then indicate the personnel getting access to the information.

Example: “Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards, and is accessible only to authorized personnel. Access to records is limited to person(s) with an official “need to know” who are responsible for servicing the record in performance of their official duties. Persons are properly screened and cleared for access. Access to computerized data is role-based and further restricted by passwords, which are changed periodically”.



System of Records Notice

12. Retention and Disposal:

State the length of time records are maintained by the activity in an active status, indicate when or if the records may be transferred to a Federal Records Center and how long the record stays there. Specify when the Records Center sends the record to the National Archives or destroys it. If records are eventually to be destroyed, state the method of destruction (e.g., shredding, burning, pulping, etc.). AR 25-400-2, the Army Records Information Management System, should be used as a reference in order to ascertain record disposition. If your activity has sent for NARA approval of the disposition scheduled, we can use the following until the Agency receives an approved disposition: “Disposition pending (treat records as permanent until the National Archives and Records Administration has approved the retention and disposition schedule.”



System of Records Notice

13. System Manager(s) and Address:

List the position title and duty address of the system manager. Please do not include names. For decentralized systems, show the locations, the position, or duty title of each category of officials responsible for any segment of the system.

14. Notification Procedures:

List the title and duty address of the official authorized to tell requesters if their records are in the system. Specify the information a requester must submit; for example, full name, military status, SSN, date of birth, or proof of identity, and so on. Specify the information an individual must provide in order for the Component to respond to the request (address, email address, etc.). The entry should read as follows "Individuals seeking to determine whether information about themselves is contained in this system of records should address written inquiries to...Request should contain individual's..."



System of Records Notice

15. Records Access Procedures:

Explain how individuals may arrange to access their records. This is very similar to the above entry. Describe how an individual can review the record and/or obtain a copy of it. Provide the title and complete mailing address of the official to whom the request for access must be directed; the information the individual must provide in order for the activity to respond to the request; and a description of any proof of identity required. The entry should read as follows "Individuals seeking access to information about themselves contained in this system of records should address written inquiries to...Requests should contain individual's..."

16. Contesting Records Procedures:

The standard language to use is "The Army's rules for accessing records, and for contesting contents and appealing initial agency determinations are contained in Army Regulation 25-71; 32 CFR part 505; or may be obtained from the system manager." Show categories of individuals or other information sources for the system. Do not list confidential sources protected by 5 U.S.C. 552a(k)(2), (k)(5), or (k)(7). Describe where the information maintained in the system is obtained from, (source documents and other agencies). Describe the record sources in general terms.



System of Records Notice

17. Record Source Categories:

Show categories of individuals or other information sources for the system. Do not list confidential sources protected by 5 U.S.C. 552a(k)(2), (k)(5), or (k)(7). Describe where the information maintained in the system is obtained from (source documents and other agencies). Describe the record sources in general terms.

18. Exemptions Claimed for the System

Exemptions: If no exemption has been established for the system indicate "None". If any exemption rule has been established state under which provision(s) of the Privacy Act it was established. Also, state that an exemption rule has been promulgated in accordance with the requirements of 5 U.S.C. 553 (B) (1), (2), (3), (c) and (e). See 5400.11-R, Chapter 5 for detailed exemption information.

**System name:**

Freedom of Information Act Program Files (December 8, 2005, 70 FR 72996).

System location:

Headquarters, Department of the Army, staff and field operating agencies, major commands, installations and activities receiving requests to access records pursuant to the Freedom of Information Act or to declassify documents pursuant to E.O. 12958, National Classified Security Information, as amended. Official mailing addresses are published as an appendix to the Army's compilation of record system notices.

Categories of individuals covered by the system:

Any individual who requests an Army record under the Freedom of Information Act, or requests mandatory review of a classified document pursuant to E.O. 12958, National Classified Security Information, as amended.

Categories of records in the system:

Individual's request, related papers, correspondence between office of receipt and records custodians, Army staff offices and other government agencies; retained copies of classified or other exempt materials; and other selective documents.

Authority for maintenance of the system:

5 U.S.C. 552, Freedom of Information Act, as amended by Pub.L. 93-502; 5 U.S.C. 301, Departmental Regulations, 10 U.S.C. 3013, Secretary of the Army; Army Regulation 25-55, The Department of the Army Freedom of Information Act Program; and E.O. 12958, National Classified Security Information, as amended.

Purpose(s):

To control administrative processing of requests for information either pursuant to the Freedom of Information Act or to E.O. 12958, National Classified Security Information, as amended, including appeals from denials.

Routine uses of records maintained in the system, including categories of users and the purposes of such uses:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, these records or information contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

The DoD 'Blanket Routine Uses' set forth at the beginning of the Army's compilation of systems of records notices also apply to this system.

Policies and practices for storing, retrieving, accessing, retaining, and disposing of records in the system:**Storage:**

Paper records in file folders and electronic storage media.

Retrievability:

By requester's surname.

Safeguards:

All records are maintained in areas accessible only to authorized personnel who have official need in the performance of their assigned duties. Automated records are further protected by assignment of users identification and password to protect the system from unauthorized access. User identification and passwords are changed at random times.

Retention and disposal:

Records reflecting granted requests are destroyed after 2 years. When requests have been denied, records are retained for 6 years; and if appealed, records are retained 6 years after final denial by the Army or 3 years after final adjudication by the courts, whichever is later.

System manager(s) and address:

Director, U.S. Army Records Management and Declassification Agency, Freedom of Information/Privacy Division, 7701 Telegraph Road, Casey Building, Suite 144, Alexandria, VA 22315-3905.

Notification procedure:

Individuals seeking to determine if information about themselves is contained in this record system should address written inquiries to the Director, U.S. Army Records Management and Declassification Agency, Freedom of Information/Privacy Division, 7701 Telegraph Road, Casey Building, Suite 144, Alexandria, VA 22315-3905.

For verification purposes, individual should provide enough information to permit locating the record.

Record access procedures:

Individuals seeking access to records about themselves contained in this record system should address written inquiries to the Director, U.S. Army Records Management and Declassification Agency, Freedom of Information/Privacy Division, 7701 Telegraph Road, Casey Building, Suite 144, Alexandria, VA 22315-3905.

For verification purposes, individual should provide enough information to permit locating the record.

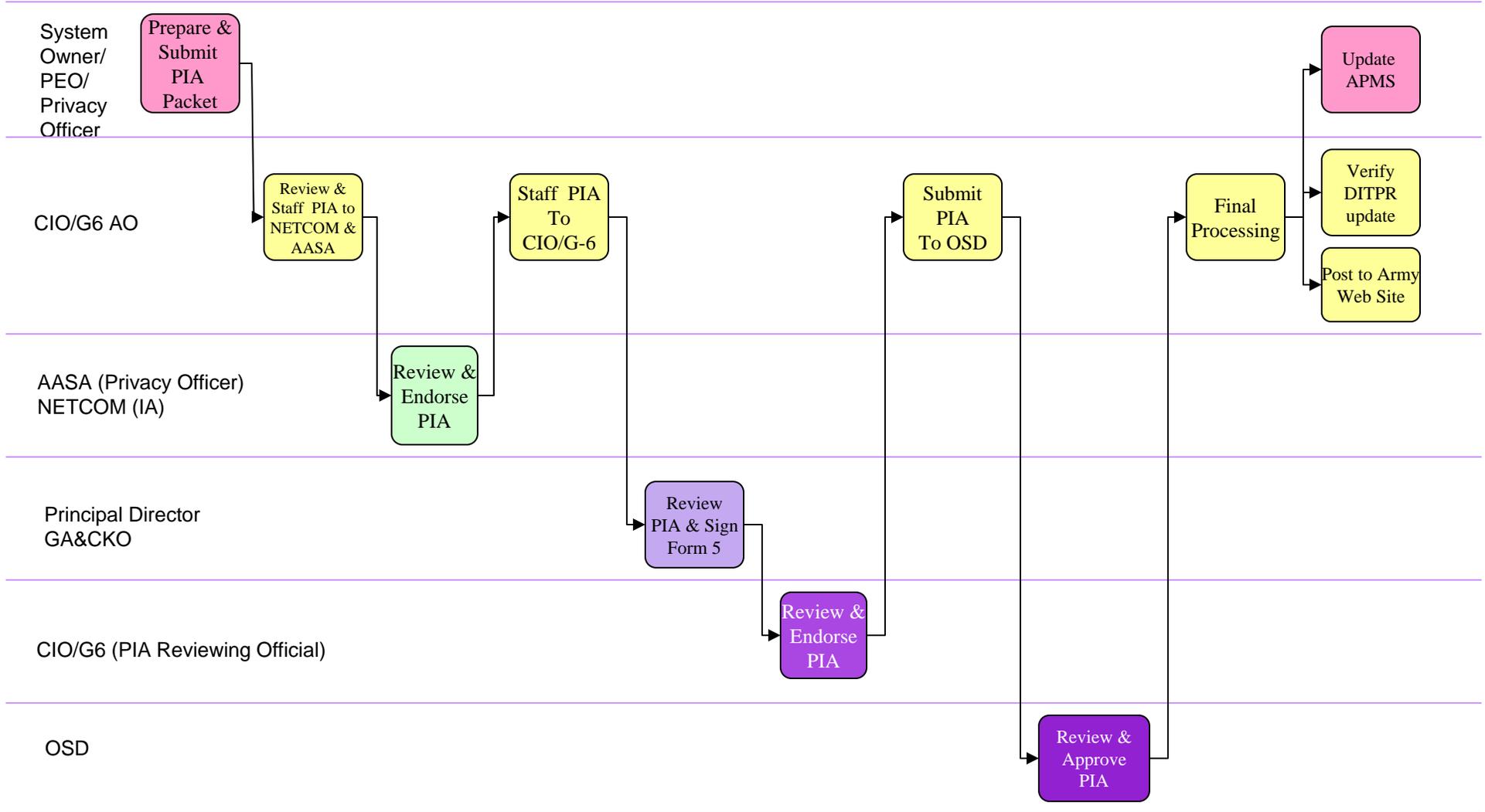


PIA Process

- Examples of completed PIA's can be found at
<http://www.army.mil/CIOG6/links/privacyimpact.html>
- Complete Certification and obtain authorized signatures
- Ensure that your APMS records are current
- Submit to CIO G-6



Army PIA Approval Process¹ Level Ø



¹The process is documented as if it worked properly at every step. It is implied at every



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

1. Department of Defense Component.

Entry should always begin with U. S. Army, then add the name of the system owner's organization. Don't go into too much detail, because your audience is the general public and they may not recognize the finer details of Army Organization. It is very important to identify the system correctly. This is why we ask for so many different identifiers.

2. Name of Information Technology System.

Enter the full name of the system, with acronym in parentheses, follow APMS name.

3. Budget System Identification Number (SNAP-IT Initiative Number)

If you don't know the BIN number, or can't find it in APMS, a PM or finance officer should be able to help.



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

4. System Identification Number(s) (IT Registry/Defense IT Portfolio Repository (DITPR)):

Should find this in APMS. Budget System Identification Number is a 4 digit number located in the DITPR database or IT_Registry.

5. IT Investment (OMB Circular A-11) Unique Identifier (from IT-43/FOIT Database -- if applicable):

Not all systems have this identifier. We will post a spreadsheet on the Website that lists all the Army systems that have this number. If your system has such a number enter the number as the answer to this question. Otherwise enter N/A. For most systems the answer will be N/A



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

6. Privacy Act System of Records Notice Identifier:

If this is a Privacy Act System of Records (i.e. information is retrieved by personal identifiers specific to an individual such as name, SSN, or other unique designator) consult the listing of System of Records Notices at

<http://www.defenselink.mil/privacy/notices/> in order to determine the notice that applies. Army notices begin with AAFES or AO followed by the prescribing regulation number and activity. **EXAMPLE: AO 600-8-14, Uniformed Services Identification Card.** NOTE: Some Army systems operate under a DoD or Government-wide Systems Notice and those should also be reviewed if an Army notice is not apparent. If the system does not retrieve information through personal identifiers, indicate “N/A – this is not a Privacy Act System of Records.”



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

7. OMB Information Collection Requirement Number and Expiration Date:

If your system collects PII using an OMB-approved form, the form will have an identifying number in the upper right corner of the form. (For an example, see your recent IRS form 1040). Few, if any, Army systems will use data collection forms with these numbers on them. Again, we have a list to post on the website of Army forms which contain an OMB Collection Requirement Number. If your system uses such a form, enter the number as the answer to this question. Otherwise, enter NA.

8. Type of authority to collect information (statutory or otherwise)

Indicate the statutory and/or Executive Order authority that allows the Army to collect the information and conduct this business practice. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation, use statute names or regulations in addition to citations. If this is a Privacy Act System of Records, the citations must match the authority that has been published in the Systems Notice. Also list any prescribing Army Regulations, DoD Directives or Instructions. As an example, Executive Order 9397 allows the Army to use the SSN as the primary identifier for individuals and should be listed on most systems. NOTE: The Systems Notice may require an update to include any additional authority reflected in the PIA.



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

9. Provide a brief summary or overview of the IT system (activity/purpose, present life-cycle phase, system owner, system boundaries and interconnections, location of system and components, and system backup)

Identify whether this is a new IT system, an existing system with no PIA, a Significantly modified IT System, or other. Identify whether the system contains information on members of the public (i.e. not agency employees or contractors). Part of the response to this question should address business requirements, practices and procedures that relate directly to an individual and the use(s) of their PII. A generic technical description of the system often does not provide enough information to evaluate the PIA. Be sure to describe: (1) The system purpose; (2) A description of a primary transaction conducted on or by the system; (3) A general overview of the modules and subsystems, and their functions.



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

10. **Identifiable Information to be Collected, its Nature and Source.**

List all data elements in the system linked to an individual in detail. This must include all data elements listed in the System of Records Notice under the section “Categories of records in the system”. Also indicate the source, who or what is providing the information, where this information will be provided from, (e.g., the individual, existing DoD IT system (specify), other Federal database (specify), etc). It is suggested the table of data elements in the system be reviewed to ensure complete PII is described. NOTE: The Systems Notice may require an update to include any additional PII reflected in the PIA.

(1) Examples of PII: Name Other Names Used, Social Security Number, Truncated SSN, Drivers License, Other ID Number, Citizenship Legal Status, Gender Race/Ethnicity, Birth Date, Place of Birth, Personal Cell Telephone Home Telephone Numbers, Personal Email Address Mailing/Home Address, Religious Preference, Security Clearance, Mother's Maiden Name, Mother's Middle Name, Spouse Information, Marital Status, Biometrics, Child Information, Vehicle Identifiers, Medical Data Disability Information, Financial Information Employment Information, Military Records, Law Enforcement Data, Emergency Contact, Education Information

(*Electronic Data Interchange Personal Identifier (DEERS Record Locator)



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

11. Method of Information Collection.

Indicate how the information will be collected. Methods that may apply are: Paper Form, Face to Face Contact, Telephone Interview, Fax, Email, Web, Information Sharing from System to System, Others.

Example: Personal information is provided by the individual record subject through completion of forms and via personal interview. Some information (Specify) is acquired from other Army/DoD personnel database systems (Specify).

12. Purpose of Collection and How Identifiable Information/Data will be used.

Describe why you are collecting the PII and state the intended use (e.g. Verification, Identification, Authentication, Data Matching; along with description of Intended Use - e.g., Mission related use (define), Administrative use (define). This should include a description from an individual record subject's standpoint. State the Army requirements and business practices to be accomplished.



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

13. Does system create new data about individuals through aggregation?

Will data from two or more systems be combined to derive new data or Create previously unavailable data about an individual. In most cases the answer to this question is “No”. If “Yes”, describe what data elements from which systems are combined and describe the new data that is developed.



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

14. Internal and External Information/Data Sharing

List all Army activities followed by all other (DoD, Federal/State/Local/Foreign government, private organizations, etc.) that receive information or data from the system. NOTE: If this is a Privacy Act System of Records, disclosures outside DoD must include those published under the System of Records Notice under the section “Routine Uses”. Agencies identified Under Internal and External Information/Data Sharing should be accompanied by a brief description of the purpose for disclosing the information to the agency. NOTE: The Systems Notice may require an update to include any additional external data sharing outside DoD reflected in the PIA. Please ensure that all sharing within the Army; with other DoD components; with other Federal Agencies; with State and Local Agencies; with Contractors (specify contractor’s name and describe the language in the contract that safeguards PII); and other (e.g., colleges) are specified. As a standard entry, we are using the following for all systems: “Information will be available to authorized users with a need to know in order to perform official government duties. Internal DoD agencies that would obtain access to PII in this system, on request in support of an authorized investigation or audit, may include DOD IG, DCIS, Army Staff Principals in the chain of command, DAIG, AAA, USACIDC, INSCOM, PMG and ASA FM&C. In addition, the DoD blanket routine uses apply to this system.”



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

15. Opportunities individuals will have to object to the collection of information in identifiable form about themselves or to consent to the specific uses and how consent is granted.

This response should describe Privacy Act Statements provided to individuals on forms (hardcopy or electronic) on system applications or on websites.

Example: See attached Privacy Act Statement.

16. Information Provided to the Individual, the Format, and the Means of Delivery.

This response is similar to Item 15 and should describe that Privacy Advisory Statements are provided to individuals as information is collected.

Example: See attached Privacy Advisory Statement.



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

17. Describe the administrative/business, physical, and technical processes and data controls adopted to secure, protect, and preserve the confidentiality of the information in identifiable form.

Indicate in great detail all physical, business and automation safeguards in place to ensure the data is protected from unauthorized access. Also indicate the authorized users of the system.

Identify:

- Who will have access to PII system- Users, Developers, System Administrators, Contractors or any others
- Type of Physical Controls-Security Guards, Cipher Locks, Identification Badges, Biometrics, Key Cards
- Technical Controls-User ID, Biometrics, Password, Firewall, Intrusion Detection System, Encryption, DoD PKI Cert
- Administrative Controls-Perform periodic security audits (frequency), monitoring of user's security practices, limited access of users to equipment and information
- Has your system undergone a certification and accreditation process and if so, what is the current status? ATO-Authorization to Operate; IATO-Interim ATO; IATT-Interim Authorization to test; DATO- Denial of Auth to Operate; None-Not yet Accredited; Not Required



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

18. Potential privacy risks regarding the collection, use, and sharing of the information, dangers in providing notices or opportunities to object/consent to individuals; risks posed by the adopted security measures.

If there are issues with safeguarding the data, they should be outlined here. For most systems it would most likely be correct to state that appropriate safeguards are in place for the collection, use, and sharing of information. Also indicate the problems (if any) that might arise if individuals are afforded an opportunity to object to the collection of information. An example might be advising a person that we are collecting information when conducting an undercover criminal investigation. For most instances, we should model after the Privacy Act Advisory Statement. Example: Individuals who object to providing required information may be unable to enter the Armed Forces. In most cases we should also state if appropriate that security measures are adequate and risk is minimal. Information is protected by user passwords, firewalls, antivirus software, CAC access, and data-at-rest protection software on portable laptops. **Example:** Due to the level of safeguarding, we believe the risk to individuals' privacy to be minimal. There are no risks in providing the individual the opportunity to object or consent



EXAMPLE GUIDANCE FOR PRIVACY IMPACT ASSESSMENT (PIA)

19. Classification and Publication of Privacy Impact Assessment.

Indicate the classification of the system and whether the Privacy Impact Assessment may be published in its entirety, or identify specific portions not recommended for publication. In most cases, it is appropriate to indicate:

Example: The data in the system is For Official Use Only. The PIA may be published in full.



PRIVACY INITIATIVES

- SSN Reduction Plan
 - DTM 07-015-USD
 - Requires all federal agencies to develop and implement a plan to reduce the unnecessary use of SSN's.
 - Plan includes a review and subsequent approval of all forms and IT systems currently in use within DoD
- Local SORN Compliance
- Upcoming Privacy training



PRIVACY INITIATIVES

QUESTIONS?