



Agenda

- PIA Overview
- Highlights of the DoDI 5400.16 PIA Guidance
- PIA Template
- Summary



PIA Overview

- A PIA is an analysis of whether personally identifiable information (PII) in electronic form is collected, stored, shared, and managed in a manner that protects the privacy of individuals and reduces the risk to their information.
- Section 208 of the E-Government Act of 2002 requires all Federal government agencies to conduct PIAs for all new or substantially changed information systems that collect, maintain, or disseminate PII on the public.
- The new DoD PIA Instruction expands the coverage to include Federal personnel and Federal contractors.



Essential Elements of the PIA

- What privacy information is collected
- Why the information is collected
- What the intended uses are for the information
- With whom the information is shared
- What opportunities individuals have to decline to provide PII
- How information is secured
- Whether a System of Records Notice (SORN) exists
- What privacy risks need to be addressed



When is a PIA Required for DoD?

When PII is collected, a PIA is required for:

- Existing DoD information systems and electronic collections where a PIA has not previously been completed to include systems that collect PII about Federal personnel and contractors.
- New DoD information systems or electronic collections:
 - Prior to developing or purchasing, and
 - When converting paper-based records to electronic systems.



When is a PIA not Required?

When the DoD information system or electronic collection:

- Does not collect, maintain or disseminate personal identifying information
- Is a National Security System (including systems that process classified information)



Highlights of the DoDI 5400.16 PIA Guidance

Formalizes E-Gov Act PIA requirement in DoD for greater visibility and clarity

Enhanced responsibilities and accountability

- Program Manager (PM) or designee starts the assessment
- Required coordination with PM, Information Assurance and Component Privacy
- Expanded signature requirements



Highlights of the DoDI 5400.16 PIA Guidance (continued)

Better coordination with other processes

- Privacy Act SORNs
- Information Collection
- Certification and Accreditation
- Budget

Establishes three year review cycle

Structures privacy risk identification and assessment with new DoD PIA Form (DD 2930)



Highlights of the New PIA Template (DD Form 2930)

More comprehensive tool

- More detailed risk analysis questions
- In-depth PII table for selection
- Technical, administrative and physical control list provided
- Interactive form with check boxes, radio buttons, and tables
- Digital signatures for the PDF form
- MS Word version available also



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enter DoD Information System/Electronic Collection Name

Enter DoD Component Name

SECTION 1: IS A PIA REQUIRED?

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

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

* "Federal personnel" are referred to in the 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) why 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.

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



SECTION 2: PIA SUMMARY INFORMATION

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

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

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
- 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
- No

If "Yes," enter UPI

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

d. Does this DoD information system or electronic collection require 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. PIA and Privacy Act SORN information should be consistent.

- Yes
- No

If "Yes," enter Privacy Act SORN Identifier

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.



UNCLASSIFIED//FOUO

USN Notices - Table of Contents - (notices/usn/index.html) - Microsoft

File Edit View Favorites Tools Help

Back Forward Stop Refresh Home Search Favorites

Address http://www.defenselink.mil/privacy/notices/usn/ Go Links

DEPARTMENT OF THE NAVY

System Identifier	System Name	Exemptions
PREAMBLE		
N01000-2	Naval Discharge Review Board Proceedings	
N01000-3	Navy Individual Service Review Board (ISRB) Proceedings Application File	
N01000-5	Naval Clemency and Parole Board Files	(j)(2)
N01001-1	Database of Reserve/Retired Judge Advocates and Legalmen	
N01070-1	JAG Corps Officer Personnel Information	
N01070-3	Navy Military Personnel Records System	
N01070-5	Database of Retired Navy Flag Officers	
N01070-7	NEXCOM Military Personnel Information System	
N01070-12	NCIS Administrative Files System	
N01070-13	Navy-Marine Corps Mobilization Processing System	
N01080-1	Enlisted Master File Automated Systems	
N01080-2	Officer Master File Automated Systems	
N01080-3	Reserve Command Management Information	
N01131-1	Officer Selection and Appointment System	(k)(1), (k)(5), (k)(6), (k)(7)
N01133-1	NAME/LEAD Processing System	
N01133-2	Recruiting Enlisted Selection System	(k)(1), (k)(5), (k)(6), (k)(7)
N01301-1	Judge Advocate General Reporting Questionnaire	
N01301-2	On-Line Distribution Information System (ODIS)	
N01306-1	Job Advertisement/Career Management/Detailing System	
N01420-1	Enlisted to Officer Commissioning Programs	

Done Internet

Start I.. U.. D.. 6.. N.. S.. M.. D.. P.. 1.. H.. P.. P.. 1:21 PM



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.

Yes

Enter OMB Control Number

Enter Expiration Date

No

f. Authority to collect information. A Federal law, Executive Order of the President (EO), 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. (If multiple authorities are cited, provide all that apply.)

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

(b) If a specific statute or EO 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.

(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.



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.

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

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.

Other DoD Components.

Specify.

Other Federal Agencies.

Specify.

State and Local Agencies.

Specify.

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 method by which individuals can object to the collection of PII.

(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.

(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. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

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



SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

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.

- Name
- Other Names Used
- Social Security Number (SSN)
- Truncated SSN
- Driver's License
- Other ID Number
- Citizenship
- Legal Status
- Gender
- Race/Ethnicity
- Birth Date
- Place of Birth
- Personal Cell Telephone Number
- Home Telephone Number
- 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
- Financial Information
- Medical Information
- Disability Information
- Law Enforcement Information
- Employment Information
- Military Records
- Emergency Contact
- Education Information
- Other

If "Other," specify or explain any PII grouping selected.

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

Describe here.



(3) How will the information be collected? Indicate all that apply.

- | | |
|---|---|
| <input type="checkbox"/> Paper Form | <input type="checkbox"/> Face-to-Face Contact |
| <input type="checkbox"/> Telephone Interview | <input type="checkbox"/> Fax |
| <input type="checkbox"/> Email | <input type="checkbox"/> Web Site |
| <input type="checkbox"/> Information Sharing - System to System | |
| <input type="checkbox"/> Other | |

If "Other," describe here.

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

Describe here.

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

Describe here.

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.)

- 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 this DoD information system or electronic collection? Indicate all that apply.

- Users
- Developers
- System Administrators
- Contractors
- Other

If "Other," specify here.

d. How will the PII be secured?

(1) Physical controls. Indicate all that apply.

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

If "Other," specify here.

(2) Technical Controls. Indicate all that apply.

- User Identification
- Password
- Intrusion Detection System (IDS)
- Encryption
- External Certificate Authority (CA) Certificate
- Other
- Biometrics
- Firewall
- Virtual Private Network (VPN)
- DoD Public Key Infrastructure Certificates
- Common Access Card (CAC)

If "Other," specify here.



(3) Administrative Controls. Indicate all that apply.

- 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**

If "Other," specify here.

e. Does this DoD information system require certification and accreditation under the DoD Information Assurance Certification and Accreditation Process (DIACAP)?

Yes. Indicate the certification and accreditation status:

- | | | | |
|--------------------------|--|----------------------|----------------------|
| <input type="checkbox"/> | Authorization to Operate (ATO) | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> | Interim Authorization to Operate (IATO) | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> | Denial of Authorization to Operate (DATO) | Date Granted: | <input type="text"/> |
| <input type="checkbox"/> | Interim Authorization to Test (IATT) | Date Granted: | <input type="text"/> |

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 here.



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

Describe here.

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

Describe here.



**Other Official Signature
(to be used at Component
discretion)**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component Senior
Information Assurance
Officer Signature or
Designee**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

**Component Privacy Officer
Signature**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:



**Component CIO Signature
(Reviewing Official)**

Name:

Title:

Organization:

Work Telephone Number:

DSN:

Email Address:

Date of Review:

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. 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 (PII). Information about an individual that identifies, links, relates or is unique to, or describes him or her (e.g., a social security number; age; marital status; race; salary; home telephone number; other demographic, biometric, personnel, medical, and financial information). Also, 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 any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. The Privacy Act of 1974 requires this notice to be published in the Federal Register upon establishment or substantive revision of the system, and establishes what information about the system must be included.



Forward in PIA Process

- Increased awareness of PII and need for adequate protection
- Increase in compliancy rates
- Identification of areas for enhanced communication and collaboration to enhance privacy