



PRIVACY IMPACT ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

Defense Retiree and Annuitant Pay System (DRAS)

DoD Component Name:

Defense Finance and Accounting Service

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).

- (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.

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 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
 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.

- 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. PIA and Privacy Act SORN information should be consistent.

- 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

- No Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date.

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

0730-001 **Child Annuitant's School Cert** (exp. 07/2010);
0730-0003 **DFAS Customer Satisfaction Survey - General**
(exp. 12/2010); 0730-0010 **Custodianship Certificate to**
Support Claims on behalf of Minor Children of Deceased
Members of the Armed Forces (exp. 07/2012); 0730-0011
Physician's Certificate for Child Annuitant (exp. 09/2010);
0730-0012 **Trustee Report** (exp. 09/2010); 0730-0013
Application for Trusteeship (exp. 09/2010); 0730-0014
Dependency Statements (exp. 11/2010).

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 provision of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute and/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.

5 U.S.C. 301 Departmental Regulations; 10 U.S.C. Chapters 53, 61, 63, 65, 67, 69, 71, 73, 74; 10 U.S.C. Sec. 1059 and 1408(h); 38 U.S.C. Sec 1311 and 1313; Pub. L.92-425; Pub Law 102-484 sec 653; Pub L. 103-160 sec. 554 and 1058; Pub L. 105-261sec. 570; DODI 1342-24, Transmittal Compensation for Abused Dependents; DoD Financial Management Regulation 7000.14-R, Volume 7B and E.O. 9397 SSN.

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.

DRAS maintains pay and personnel information for use in the computation of military retired pay, survivor annuity pay, and to make payments to retirees, spouses, former spouses and other dependents. The DRAS system supports over 2.5 million customers and has several modules which include Retired and Casualty Pay System (RCPS), Annuitant Pay System (APS), Victim of Abuse (VOA), Voluntary Separation Incentive (VSI), Retired and Annuitant Pay Information (RAPID) system, Interactive Voice Response and Call Center Anywhere (IVR/CCA) system, Combat Related Special Compensation (CRSC), Concurrent Retirement and Disability Payments (CRDP), CRDP-CRSC Processing (CCP), Survivor Benefits Plan (SBP), Dependency and Indemnity Compensation (DIC), Annuities for Certain Military Surviving Spouses (ACMSS), and Retired and Annuitant Pay Policy Automation (RAPPA).

Information collected for retirees and annuitants includes name, social security number, military records, address, etc. PII data is received through a wide range of collection methods with the largest being interfaces with partners at Veterans Administration, Military Services, IRS, etc. PII data is also received from individuals during Retiree Seminars and during conversations with DFAS Call Center Customer Service Representatives. The RAPID system collects PII data from documents that are received from our customer base through the mail or via fax. Customers can send PII data to DFAS via internet capabilities such as direct emails and forms on the DFAS WebSite.

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

Mishandling PII may result in lost, stolen, or compromised data causing at least one of the following negative impacts to the affected individual: identity theft, damage to the individual's reputation, and/or financial hardship. Such incidents could irreparably damage DFAS' credibility casting the agency in an unfavorable light to the public.

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

PII will be shared with internal DFAS organizations that demonstrate a "need to know" (e.g. DFAS Office of General Counsel, DFAS Garnishment Operations, DFAS Disbursing Operations, or other DFAS offices to process pay entitlement related documents and to address customer inquiries).

Other DoD Components. Specify

Data is shared with other DoD components such as active duty and reserve components for the military services (Army, Air Force, Navy and Marine Corps). Other DoD components include the Defense Manpower Data Center (DMDC).

Other Federal Agencies. Specify

Records are provided to the Internal Revenue Service for normal wage and tax withholding. Disclosures are made to the Department of Veterans Affairs (DVA) regarding establishments, changes and discontinuing of DVA compensation to retirees and annuitants; Office of Personnel Management as part of myPay processes; and Social Security Administration for matching purposes.

State and Local Agencies. Specify

Data is provided to State Income Tax authorities.

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

All contracts listed below include the specific narrative text from DFAS 52.224-9000 "INFORMATION ASSURANCE (July 2009)" paragraphs 'a' through 'e' which provides language stating requirement for contractor to safeguard all PII data:

ACS - In-bound Mail contract (contractor receives R&A Operations incoming mail and faxes from wide range of customers and scans and indexes the documents into RAPID).

Anthony Wayne Rehabilitation Center - Outbound Mail contract (contractor manages the processing of outgoing R&A mail).

KeyPoint Government Solutions, Inc. - Certificate of Death (COD) contractor (Contractor obtains CODs from state and local offices as requested by DFAS).

NOTE: DRAS was recently in-sourced (effective February 1, 2010) from Lockheed Martin who had provided processing support under a contract for Military Retiree and Annuitant Pay Performance (MDA220-01-C-0002). Lockheed Martin still provides software development support for RAPID.

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

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, records may be disclosed outside the DoD as a routine use as follows: to individuals authorized to receive retired and annuitant payments on behalf of retirees or annuitants; to former spouses for purposes of providing information regarding Survivor Benefit Plan coverage; the Army and Air Force Mutual Aid Association (AAFMAA) and Navy-Marine Corps Relief Society (NMCRS) to process allotments for repayment of interest-free loans from the society; and to process retiree charitable allotments in support of fund drives initiated by Secretaries of the Army, Navy and Air Force.

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.

Privacy Act Statements appear on all Forms used to collect the information from retirees, annuitants, and other eligible payees or authorized payee representatives. When collecting PII via telephone the Privacy Act statement is included as part of the Interactive Voice Response System's script. When receiving information via web-site electronic form submission, a privacy policy advisory is included.

(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.

Individuals can review the Privacy Act Statement on forms and have the opportunity to decline to provide the information. Likewise, individuals may withhold consent for use by not providing information requested.

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