



PRIVACY IMPACT ASSESSMENT (PIA)

DoD Information System/Electronic Collection Name:

DFAS Enterprise Portal (ePortal)

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?

- X 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

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

- No

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

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 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.

The ePortal does not collect PII. The authority to collect PII would lie within the business owners who utilize the ePortal to collect PII, and conduct their operations.

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.

The ePortal is the Agency's integrated tool for accessing information, conducting business, and managing operations. The ePortal components consists of a web layer (portal), authentication for single sign-on (SSO) gateway to a variety of back-end systems, Collaboration Projects for sharing and exchange of information, Documentum for dissemination of DFAS corporate communications, access to HR applications for DFAS employees (e.g., e-Biz Timekeeping), access to DoD HR information for personnel across the DoD (i.e., TSP), and automated Business Process Management through the use of electronic workflows.

While the ePortal does not collect, retain or use PII for its own use, the ePortal user (with elevated privileges) may determine that using the ePortal is a method that facilitates the performance of their duties in supporting critical agency mission(s). The Content or Community Manager may use Documentum to provide limited access to documents for their communities, or DFAS as a whole, based upon a need-to-know. They are responsible for ensuring their content does not contain any PII, as the dissemination of PII is strictly prohibited. Collaboration Project Leaders have an ability to create projects, and share content (including PII) to a limited number of users on a need-to-know basis, in the performance of their duties.

Since the ePortal only serves as a gateway to operations-based systems, note that this PIA does not consider or include PII data collected or exchanged via operations-based systems; the PIA requirements for these operations-based systems are the responsibility of the operation owner per agency and DoD guidance.

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

The result of mishandling personal data may lead to lost, stolen or compromised PII which could be harmful to the individual in many ways (e.g., identity theft, damage to an individual's reputation and/or financial hardship). Additionally, such incidents could cast DFAS in an unfavorable light to the public. DFAS adheres to physical protections of PII as described in accordance with DFAS 5200.1-R while IA policy (DFAS 8400.1-R) prescribes protection requirements for sensitive data for all DFAS systems. Management responsibilities are maintained in DFAS 8500.1

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

All agency employees may access documents which are 'published' while documents contained in ePortal 'projects' are made available through project manager approval and granting of access.

Other DoD Components. Specify

Any '.mil' domain account, with a valid CAC that has been approved.

Other Federal Agencies. Specify

Any '.gov' domain account, with a valid CAC that has been approved.

State and Local Agencies. Specify

Any State or Local agency with a valid CAC that has been approved

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

Any '*.com' , with a valid CAC that has been approved

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

Any '.edu' domain accounts, with a valid CAC that has been approved.

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.

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

ePortal does not collect PII directly from individuals.

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