# PRIVACY IMPACT ASSESSMENT (PIA)

**PRESCRIBING AUTHORITY**: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

**1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:**

DFAS Portal SharePoint

**2. DOD COMPONENT NAME:**

Defense Finance and Accounting Service

**3. PIA APPROVAL DATE:**

06/27/18

## SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

**a. The PII is:** *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

**b. The PII is in a:** *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [x] Existing DoD Information System
- [ ] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

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

The DFAS Portal is the Agency's integrated tool for accessing information, conducting business, and managing operations. The DFAS Portal components consist of an information store of over 15 Terabytes (TB) of data on Servers including Microsoft SharePoint, Microsoft Structured Query Language (SQL) in Always-On Configuration with 5 TB capacity, Microsoft Active Directory (AD), Microsoft Active Directory Federated Services, Microsoft Active Directory Rights Management Services and Microsoft Forefront Identity Manager. These servers are configured in a virtualized environment hosted at the Defense Information Systems Agency (DISA) Computing Ecosystem, in Ogden Utah. While the DFAS Portal does not collect, retain or use Personally Identifiable Information (PII) for its own use, the DFAS Portal user (with elevated site collection privileges) may determine that using the DFAS Portal is a method that facilitates the performance of their duties in supporting critical agency mission(s). The Site Collection Manager may provide limited access to documents for their sites, or to DFAS as a whole, based upon a need-to-know. They are responsible for ensuring their content does not contain any Personally Identifiable Information (PII), as the dissemination of PII is strictly prohibited. Site Collection Managers have an ability to create sites, 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 DFAS Portal only serves as a gateway to operations-based systems and has no direct external interface, 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 operational owner per agency and Department of Defense (DoD) guidance.

**d. Why is the PII collected and/or what is the intended use of the PII?** *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

While the DFAS Portal does not collect, retain or use PII for its own use, the DFAS Portal user (with elevated site collection privileges) may determine that using the DFAS Portal is a method that facilitates the performance of their duties in supporting critical agency mission(s). The Site Collection Manager may provide limited access to documents for their sites, or to 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. Site Collection Managers have an ability to create sites, 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 DFAS Portal 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 and has no direct external interface; the PIA requirements for these operations-based systems are the responsibility of the operational owner per agency and DoD guidance.

**e. 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 to the collection of PII.

DFAS Portal does not collect PII directly from individuals.

**f. 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.

DFAS Portal does not collect PII directly from individuals.

**g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided.** *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

DFAS Portal does not collect PII directly from individuals.

**h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component?** *(Check all that apply)*

| | | |
|---|---|---|
| ☒ Within the DoD Component | Specify. | All Non-classified Internet Protocol (IP) Router Network (NIPRNet) agency employees may access documents to which they have been granted access, and maintain a valid Common Access Card (CAC) that has been approved. |
| ☒ Other DoD Components | Specify. | Any NIPRNet State or Local agency with a valid CAC that has been approved. |
| ☒ Other Federal Agencies | Specify. | Any NIPRNet State or Local agency with a valid CAC that has been approved. |
| ☒ State and Local Agencies | Specify. | Any NIPRNet State or Local agency with a valid CAC that has been approved. |
| ☐ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)* | Specify. | |
| ☐ Other *(e.g., commercial providers, colleges).* | Specify. | |

**i. Source of the PII collected is**: *(Check all that apply and list all information systems if applicable)*

☒ Individuals ☐ Databases

☐ Existing DoD Information Systems ☐ Commercial Systems

☐ Other Federal Information Systems

The DFAS Portal does not collect PII.

**j. How will the information be collected?** *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail ☐ Official Form (*Enter Form Number(s) in the box below)*

☐ Face-to-Face Contact ☐ Paper

☐ Fax ☐ Telephone Interview

☐ Information Sharing - System to System ☐ Website/E-Form

☒ Other *(If Other, enter the information in the box below)*

It is possible for individuals to upload PII to the DFAS Portal. However, the DFAS Portal does not collect PII. DFAS Portal isn't used to retrieve/collect info on individuals & doesn't assign the Electronic Data Interchange Personal Identifier (EDIPI)/UserPrincipalName to any of the user accounts. It is not the system of record. Its internal users are retrieved from Active Directory. AD is DISA Computing Ecosystem Ogden's responsibility; DISA is responsible for any AD SORN. Defense Civilian Personnel Data System (DCPDS) is used to load external users, and the DCPDS system is responsible for any SORN.

**k. 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 must be consistent.

☐ Yes ☒ No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

*or*

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

DFAS Portal isn't used to retrieve/collect info on individuals & doesn't assign the EDIPI/UserPrincipalName to any of the user accounts. It is not the system of record. Its internal users are retrieved from Active Directory. AD is DISA Computing Ecosystem Ogden's responsibility; DISA is responsible for any AD SORN. DCPDS is used to load external users, and the DCPDS system is responsible for any SORN.

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

(1) NARA Job Number or General Records Schedule Authority. DFAS 5015.2-M vols 1,2

(2) If pending, provide the date the SF-115 was submitted to NARA. N/A

(3) Retention Instructions.

In accordance with Volume 1 and 2 of DFAS 5015.2-M: Cutoff is at the end of the fiscal year and destroy 10 years after cutoff.
*Information is determined by the subject of the records retained.

**m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.**

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

N/A. The DFAS Portal does not collect PII. The DFAS employs a system called DFAS Portal. Its primary function is to enable collaboration and information sharing. This data contains Social Security Number (SSN) and Taxpayer Identification Number (TIN) required for validation of payments and vouchers and for audit. The last Privacy Impact Assessment performed as part of the accreditation process was completed on July 18, 2016.

The justification for the use of the SSNs and/or TINs is Department of Defense (DoD) Instruction 1000.30, Enclosure 2, Paragraphs 2.c. (4) "Interactions with Financial Institutions", (7) "Federal Taxpayer Identification Number", and (8) "Computer Matching". Financial institutions may require that individuals provide the SSN as part of the process to open accounts. It may therefore be required to provide the SSN for systems, processes, or forms that interface with or act on behalf of individuals or organizations in transactions with financial. institutions.

**n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

N/A. The DFAS Portal does not collect PII.