

## 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:**

DISA Storefront (DSF)

**2. DOD COMPONENT NAME:**

Defense Information Systems Agency

**3. PIA APPROVAL DATE:**

### 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  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
- 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.**

DISA Storefront is a suite of web-based applications that allows customers to request telecommunications services from DISA. Mission partners use Storefront to submit service orders for approval and fulfillment. DSF uses routing rules and workflow to route orders for approval. Once orders are approved, a DISA service request (e.g. Telecommunications Service Request (TSR)) data is sent to key stakeholders and finance/fulfillment systems. Storefront is public facing and can be accessed by federal and coalition partners from outside the .mil domain. Storefront directly interfaces with DISA billing and contracting systems (e.g. TIBI, IDEAS, CSS). Storefront uses PKI enabled single sign on authentication services for user authentication. The production, UAT, and QA environments are hosted by MilCloud 2 at the DISA Datacenter Montgomery, AL. The development environment is a standalone environment hosted in the AWS GovCloud Instance. PII is collected in the following ways:

1. Data collected during user registration.
2. The Central Address Directory displays user information and is visible to all users regardless of their agency, but is role restricted.
3. DMUC Subscriber information. This is the data that leverages EDQS and primarily uses EDQS to validate the entered subscriber email address.
4. Mobility Search function allows users to look up DMUC subscribers and view the subscriber details. This is also open to all users with the ARO role regardless of agency.
5. POC information is stored for all circuit based orders and can be viewed when creating orders or by using the POC Management function. These records are also available for viewing by all user and all Agencies.
6. POC information is contained on the actual TSR message, which is emailed out to all addressees on the TSR message. A person doesn't have to be a DSF user to be addressed on a TSR message.

**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)

The PII is gathered by the user entering their own PII (duty location, contact information, CAC certificate information) in the account creation form. POC information for service delivery locations is also entered on service orders by users and stored for reuse on future orders. The use of EDQS is for verifying subscriber email addresses used when requesting DoD Mobility Unclassified Capability (DMUC) service. The validated email addresses are stored in the DSF database and associated with the specific DMUC service order.

**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.

Users can object to the collection of their PII by not utilizing the system. However, the PII collected is used to compare to the data already stored in the EDQS system. DSF conducts a query of the data to validate its accuracy from EDQS. Additionally, users must supply their duty email addresses, names, duty location, CAC certificate information and ranks in order to utilize DSF.

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.

If users do not wish to enter this information, they can exit the account creation process. Note, this data already exists in the GAL and EDQS system. However, to utilize DSF, this information must be entered.

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

You are accessing a U.S. Government (USG) Information System (IS) that is provided for USG-authorized use only.

By using this IS (which includes any device attached to this IS), you consent to the following conditions:

-The USG routinely intercepts and monitors communications on this IS for purposes including, but not limited to, penetration testing, COMSEC monitoring, network operations and defense, personnel misconduct (PM), law enforcement (LE), and counterintelligence (CI) investigations.

-At any time, the USG may inspect and seize data stored on this IS.

-Communications using, or data stored on, this IS are not private, are subject to routine monitoring, interception, and search, and may be disclosed or used for any USG authorized purpose.

-This IS includes security measures (e.g., authentication and access controls) to protect USG interests--not for your personal benefit or privacy.

-Notwithstanding the above, using this IS does not constitute consent to PM, LE or CI investigative searching or monitoring of the content of privileged communications, or work product, related to personal representation or services by attorneys, psychotherapists, or clergy, and their assistants. Such communications and work product are private and confidential. See User Agreement for details.

-This system collects the user's name, duty e-mail address, duty location, duty contact information, and CAC information for account creation.

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. DISA
- Other DoD Components Specify. All DoD Agencies
- Other Federal Agencies Specify. All Federal Agencies
- State and Local Agencies Specify.
- 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. Foreign Mission Partners (NATO, UK, Canada, New Zealand, Australia)

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

Enterprise Directory Query Service (EDQS)

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)

**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 K890.14

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or <http://dpcl.dod.mil/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.

**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. GRS 5.5. Item 020

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

(3) Retention Instructions.

Destroy when 1 year old or when superseded or obsolete, whichever is applicable, but longer retention is authorized if required for business use. Disposition Authority: DAA-GRS2016-0012-0002

**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 statute 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.

The authority allows DISA Storefront (DSF) to collect the data: 5 U.S.C. 301, Departmental Regulation; 10 U.S.C. chapter 8; DoD Directive 5105.19, Defense Information Systems Agency (DISA); DoD Directive 5105.19, Defense Information Systems Agency (DISA); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Enterprise User Data Management Plan for Persons and Personas; and Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS).

**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.

OMB Control Number: 0704-0415; Expiration Date: None