

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:

Enterprise Directory Query Service (EDQS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

02/06/20

milCloud 2 Common Services Virtual Private Cloud

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

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

- | | |
|---|---|
| <input type="checkbox"/> From members of the general public | <input checked="" type="checkbox"/> From Federal employees and/or Federal contractors |
| <input type="checkbox"/> From both members of the general public and Federal employees and/or Federal contractors | <input type="checkbox"/> Not Collected (if checked proceed to Section 4) |

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

- | | |
|--|---|
| <input type="checkbox"/> New DoD Information System | <input type="checkbox"/> New Electronic Collection |
| <input checked="" type="checkbox"/> Existing DoD Information System | <input type="checkbox"/> Existing Electronic Collection |
| <input type="checkbox"/> 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.

In an effort to evolve the DoD IT enterprise, common identity management services to mission applications hosted within the milCloud 2 cloud service enclave. Implementing these common services within a milCloud 2 Virtual Private Cloud (VPC) provides mission owners with reliable authentication and authorization services for their mission applications without the performance degradations of crossing long-haul communications paths. This change will provide a more robust and optimized cloud service environment for mission partners.

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)

DoD ID number replaces EDIPI will be collected in order to identify and authenticate users with mission partner application hosted in DISA milCloud 2 environment.

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.

The common services VPC within milCloud will offer directory data obtained directly from EDQS. The milCloud 2 mission partner applications that leverage this directory common service VPC will be determinative of how data is store according to each mission partner AO (i.e. AMC).

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.

The common services VPC within milCloud will offer directory data obtained directly from EDQS. The milCloud 2 mission partner applications that leverage this directory common service VPC will be determinative of how data is store according to each mission partner AO (i.e. AMC).

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.)

- | | | |
|---|--|---|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input checked="" type="checkbox"/> Privacy Advisory | <input type="checkbox"/> Not Applicable |
|---|--|---|

EASF does not collect PII directly from the individual, but rather obtains data elements from other established systems that are approved to collect these PII data (primarily through the Identity Synchronization Service (IdSS)). An example is DEERS, which is provided by the Defense Manpower Data Center (DMDC), who functions as the DoD Data Wholesaler for data. DMDC data are typically provided directly by the user, or by DoD Component systems that collect data, such as DoD Component Human Resources IT systems. Individuals are provided a Privacy Act Statement and Privacy Advisories at the point where they enter and update their data in accordance with standard procedures for these systems. In addition, Privacy Advisories are provided when users access DoD end-user devices which, in turn, are used to access the applications that use the EASF for access control and to obtain user contact information (Exchange, SharePoint, vOffice, etc.).

Template available: https://disa.deps.mil/disa/cop/privacy_act/SitePages/Privacy%20COP%20homepage.aspx

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

- | | | |
|--|----------|---|
| <input type="checkbox"/> Within the DoD Component | Specify. | <input type="text"/> |
| <input type="checkbox"/> Other DoD Components | Specify. | <input type="text"/> |
| <input type="checkbox"/> Other Federal Agencies | Specify. | <input type="text"/> |
| <input type="checkbox"/> State and Local Agencies | Specify. | <input type="text"/> |
| <input type="checkbox"/> 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. | <input type="text"/> |
| <input checked="" type="checkbox"/> Other (e.g., commercial providers, colleges). | Specify. | N/A: The information will not leave the device and cannot be seen by administrators |

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

- | | |
|--|---|
| <input type="checkbox"/> Individuals | <input type="checkbox"/> Databases |
| <input checked="" type="checkbox"/> Existing DoD Information Systems | <input type="checkbox"/> Commercial Systems |
| <input type="checkbox"/> Other Federal Information Systems | |

Collecting personal biometric data

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

- | | |
|---|--|
| <input type="checkbox"/> E-mail | <input type="checkbox"/> Official Form (Enter Form Number(s) in the box below) |
| <input type="checkbox"/> Face-to-Face Contact | <input type="checkbox"/> Paper |
| <input type="checkbox"/> Fax | <input type="checkbox"/> Telephone Interview |
| <input checked="" type="checkbox"/> Information Sharing - System to System | <input type="checkbox"/> Website/E-Form |
| <input type="checkbox"/> Other (If Other, enter the information in the box below) | |

Information is obtained and maintained on the Mobile device only

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://dpcltd.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

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.

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

(3) Retention Instructions.

Not applicable. Records stored within the cloud should be individually scheduled by the agency/organization who owns the records by utilizing the GRS or their agency's records schedule.

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 following authority allows milCloud 2 Common Services Virtual Private Cloud to collect the following 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 1000.25, DoD Personnel Identity Protection (PIP) Program;
- DoD Enterprise User Data Management Plan for Persons and Personas, August 11, 2010;
- Global Information Grid 2.0 Concept of Operations (GIG 2.0 CONOPS), March 11, 2009.

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 approval is not required in accordance with Section 8.b.11 of Enclosure 3 of DoD Manual 8910.01 - Volume 2