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:

DoD Enterprise Portal Service (DEPS)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

Center for Operations/Services Directorate

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.

DEPS is the DoD Enterprise Portal Service based off the SharePoint Platform. This service is provided to the DISA DEPS audience (mission partners) in order to facilitate Document Collaboration, Business Process Automation, Content Management, and many other features. The Community of Practice is here to help Site Managers, Content Managers, and End Users interact with each other, helping to foster a sense of unity, collaboration, and good faith in the DISA mission.

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)*

DEPS PMO does not determine how each unique mission partner, who consumes the DEPS service, utilizes PII. The way in which PII will be utilized, collected, stored, and maintained is determined by each distinct mission partner. Further, each mission partner is responsible for data verification, identification, data matching, mission-related use, and administrative use in day-to-day operations.

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.

Each unique mission partner that consumes the DEPS service determines how the PII data is collected, used, and for what purpose. There may be cases in which a mission partner does not provide individuals the opportunity to object to the collection of their PII.

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.

Each unique mission partner that consumes the DEPS service determines how the PII data is collected, used, and for what purpose. There may be cases in which a mission partner does not provide individuals the opportunity to consent to the specific uses of their PII.

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

Individuals are provided a Privacy Act Statement and/or a Privacy Advisory in accordance with each unique mission partners' policies and procedures. These notices will vary based upon how and why the PII is being collected.

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.
☒	Other DoD Components	Specify. Army, Navy, Air Force
☐	Other Federal Agencies	Specify.
☐	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.

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		

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)*		

How the information will be collected will be determined by each unique mission partner utilizing the DEPS service based upon mission need.

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 K890.21

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.

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.

Users of the DEPS service must adhere to the National Archives and Records Administration's (NARA) General Records Schedule (GRS) or their Agency specific schedule to determine retention timelines for the various types of documents stored within DEPS.

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.

5 C.F.R. parts 2, 5, 731, 732, 736, and 1400 establish the requirements for agencies to evaluate relevant covered positions for a position sensitivity and position risk designation commensurate with the duties and responsibilities of those positions. Depending upon the purpose of the particular background investigation, OPM is authorized to collect information under Executive Orders 9397, 10450, 10577, 10865, 12333, 12968, 13467 as amended, 13488, and 13549; 5 U.S.C. §§ 1103, 1302, 1303, 1304, 3301, 7301, 9101, and 11001; 22 U.S.C. §§ 272b, 290a, 2519; 31 U.S.C. §§ 1537; 42 U.S.C. §§1874(b) (3), 2165, 2201, and 20132; 50 U.S.C. § 3341; Public Law 108-136; and Homeland Security Presidential Directive (HSPD) 12.

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