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:

Defense Enterprise Office Solution-Unclassified (DEOS-U)

2. DOD COMPONENT NAME:

Defense Information Systems Agency

3. PIA APPROVAL DATE:

03/19/2025

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

- ☐ From members of the general public
- ☐ From Federal employees
- ☒ from both members of the general public and Federal employees
- ☐ 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.

DEOS-U is a logically integrated cloud infrastructure hosted within Microsoft's authorized Azure Government Impact Level 5 (IL5) environment. It has the ability to host data migration and monitoring capabilities supporting the DoD's use of subscriptions to Microsoft's separately authorized Office 365 Software-as-a-Service (SaaS). DEOS-U uses Azure Infrastructure-as-a-Service (IaaS) and Platform-as-a-Service (PaaS) services to host the network infrastructure components and security tools, including MS Sentinel Security Event and Incident Management (SIEM), required to provide required boundary protection and support continuous monitoring & incident response, respectively. The Assured Compliance Assessment Solution (ACAS) is also deployed within the environment to perform vulnerability and compliance scanning on all hosts within boundary. In addition, DEOS-U hosts the ISEC7 Sphere Endpoint and Digital Workspace Management application which allows DISA to monitor and manage the DEOS Digital Workspace and Mobile Infrastructure and network to quickly identify and resolve potential issues through a single dashboard.

There is no organized collection of PII/PHI as part of the DEOS-U system beyond the data in transit of user email, name, user data, phone number, and service/Agency affiliation for the specific purpose of email address lookup and user authentication. Any "user entered" personal information stored within DEOS-U is the responsibility of the user/user's organization to ensure it's properly protected, categorized, reported, etc.

All data is encrypted in transit (TLS) and at rest (DAR) within the Microsoft Azure IL-5 (IaaS/PaaS) environment. The user maintains the responsibility for the classification and handling of the PII/PHI.

The types of personal information that is collected includes: Name(s), Official Duty Telephone Phone Number, DoD ID Number, Position/ Title, and Work Email Address.

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)*

There is no collection of PII within DEOS-U beyond identity information that is required for authentication.

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.

Individuals can object to the collection of their PII by not completing and submitting the information required.

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.

Individuals can object to the collection of their PII by not completing and submitting the information required.

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

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

☒	Within the DoD Component	Specify. DISA DEOS
☐	Other DoD Components *(i.e. Army, Navy, Air Force)*	Specify.
☐	Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)*	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)*

☐ In-Person 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 DMDC.02 DoD/ DoD-0019

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. DAA-GRS-2013-0006-0003

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

(3) Retention Instructions.

Temporary. Destroy when business use ceases.

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.

The following authority allows DEOS-U to collect the following data:
Public Law 113-283, The Federal Information Security Modernization Act of 2014, as amended (44 U.S.C. Chapter 35, Subch. II); 10 U.S.C. 113, Secretary of Defense; 10 U.S.C. 142, Chief Information Officer; 5 U.S.C. 301, Departmental Regulations; 10 U.S.C Section 164, Commanders of Combatant Commands: Assignment; Powers and Duties; 18 U.S.C. 1029, Fraud and Related Activity in Connection with Access Devices; 18 U.S.C. 1030, Fraud and Related Activity in Connection with Computers; Section 922 of the National Defense Authorization Act for FY 2012 (Pub. L. 112-81), "Insider Threat Detection"; Executive Order (E.O.) 10450, Security Requirements for Government Employees, as amended; E.O. 14028, Improving the Nation's Cybersecurity; E.O. 13526, "Classified National Security Information"; E.O. 13587, "Structural Reforms To Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information"; DoD Directive 5205.16, "The DoD Insider Threat Program"; DoD Instruction (DoDI) 8500.01, "Cybersecurity,"; DoDI 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," and E.O. 9397 (SSN), as amended.

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: 1845–0114; Expiration Date: None.