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:

milDrive

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.

milDrive is DISA's core cloud storage service that provides a personal desktop, web, and mobile application client that enhances traditional file services and extend user's self service capability to store, share, synchronize, backup and recover their data. With milDrive, user data is stored and protected in the cloud, synchronized locally and available offline on any DOD-approved device.

The milDrive system collects a very limited set of PII. This limited set of PII is consists of a persona-based user objects such as users first name, last name, middle initial, persona type code (PTC), work email address, and DOD ID number. These data are pulled from an existing DOD systems (e.g. Identity Synchronization Service (IdSS), Defense Enrollment Eligibility Reporting System (DEERS)) solely for the purpose of creating milDrive accounts. Without this information a milDrive user account cannot be created. These data elements are required for DOD CAC authentication auditing requirements. These PII data are required to implement and operate DoD information technology (IT). If these data were not available for a specific individual, then that individual would not be able to access milDrive.

milDrive is a storage platform and is authorized to store all forms of Controlled Unclassified Information (CUI) data. Organizations who collect privacy data must consult with their privacy officer if using/intend to use milDrive to store privacy data from existing electronic collections.

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 username, work email, PTC and DOD ID number are necessary in the account creation process for user verification, identification and authentication as well as auditing requirements.

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 milDrive system 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. For example, milDrive gets persona data (DOD ID number, PTC, and work email address) from IdSS, which pulls from DEERS (i.e milConnect). The milConnect/DEERS system is managed by the Defense Manpower Data Center (DMDC), who functions as the DoD Data Wholesaler for these data. milConnect provides individuals the capability to review and update their data where users can review their data, enter or provide certain data, and be directed to other organizations and systems to update other data (such as in local DoD Component Human Resources (HR) systems).

Without this information the milDrive could not create user accounts or meet it's requirements for secure user verification, identification and authentication as well as auditing requirements. These PII data are required to implement and operate DoD information technology (IT). If

these data were not available for a specific individual, then that individual would not be able to access milDrive or key new components of DoD IT, such as Enterprise E-Mail, which are required for individuals to do their work.

Individuals seeking to determine whether information about themselves is contained in this system of records can e-mail disa.meade.esd.list.idam-eds@mail.mil or address written inquiries to Defense Information Systems Agency (DISA), Enterprise Services Directorate, PO Box 549, Fort George G Meade, MD 20755-0549.

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 milDrive system 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. For example, milDrive gets persona data (DOD ID number, PTC, and email address) from IdSS, which pulls from DEERS (i.e milConnect). The milConnect/DEERS system is managed by the Defense Manpower Data Center (DMDC), who functions as the DoD Data Wholesaler for these data.

milConnect provides the following Privacy Act Statement:

Authority: 5 U.S.C. App. 3, Inspector General Act of 1978; 5 U.S.C. Chapter 90, Federal Long-Term Care Insurance; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 53, Miscellaneous Rights and Benefits; 10 U.S.C. Chapter 54, Commissary and Exchange Benefits;

10 U.S.C. Chapter 55 Medical and Dental Care; 10 U.S.C. Chapter 58, Benefits and Services for Members being Separated or Recently Separated; 10 U.S.C.

Chapter 75, Deceased Personnel; 10 U.S.C. 2358, Research and Development Projects; 20 U.S.C. 1070a (f)(4), Higher Education Opportunity Act; 31 U.S.C. 3512(c), Executive Agency Accounting and Other Financial Management;

42 U.S.C. 1973ff, Federal Responsibilities; 50 U.S.C. Chapter 23, Internal Security; DoD Directive 1000.4, Federal Voting Assistance Program (FVAP); DoD Instruction 1341.2, DEERS Procedures; Homeland Security Presidential Directive 12, Policy for a common Identification Standard for Federal Employees and Contractors; 38 CFR part 9.20, Traumatic injury protection; 38 U.S.C. Chapter 19, Subchapter III, Servicemembers's Group Life Insurance; DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural or Manmade Disasters, and E.O. 9397 (SSN), as amended.

Purpose: The data provided will be used to update your Defense Eligibility and Enrollment Reporting System (DEERS) record. The DEERS data is used for determining eligibility for DoD entitlements and privileges. It is also used to authenticate and identify DoD affiliated personnel. For a complete listing of the uses of the DEERS data see System of Record Notice "DMDC 02 DoD". (http://dpclo.defense.gov/privacy/SORNs/component/osd/DMDC02.html)

Routine Uses: Data is shared with other Federal/State agencies and contractors for the purpose of determining eligibility of benefits, fraud, and documented studies dealing with the health and well-being of DoD personnel. For a complete listing of the routine uses see System of Record Notice "DMDC 02 DoD".

Disclosure: Voluntary. However, if data in DEERS is not up-to-date, your DoD entitlements/privileges and the ability of DEERS to identify you as a DoD affiliated person could be delayed or inaccurate. Home addresses will be used for mustering in the event of an officially declared manmade or natural disaster (DoDI 3001.02) and for notification of a Privacy compromise, loss or stolen (breached) personally identifiable information (PII). If addresses are not correct these two requirements will not be performed with accuracy as to your location.

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 exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	The sharing of the data is for internal DISA milDrive PMO reporting purposes only and for mission partner billing.
☐ Other DoD Components	Specify.	
☐ 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

IdSS

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)*

The account information is collected automatically when the milDrive account is associated with the IdSS record.

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 DOD

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.

Records maintained within milDrive are managed by the individual users/organizations. Personnel who utilize milDrive to store records should adhere to either federal records disposition authorities or DISA's records retention authorities since the cloud will house various types of federal records. Unscheduled records (records types not listed within these documents) should be maintained as permanent until the records are scheduled. Coordination of unscheduled records can be started by contacting the Agency Records Officer.

NARA General Records Schedule: https://www.archives.gov/records-mgmt/grs.html

DISA Records Disposition Schedule: https://disa.deps.mil/disa/cop/rm/Pages/RecordManagementCoP.aspx

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 U.S.C. 301, Departmental Regulations
- Pub. L. 106-229, Electronic Signatures in Global and National Commerce, July 1, 1997
- OASD(C3I) Policy Memorandum dated August 12, 2000, subject: Department of Defense (DoD) Public Key Infrastructure (PKI).
- OASD (C3I) Memorandum dated Jan 2001, subject: Common Access Card (CAC), and Government Paperwork Elimination Act.

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 #l0704-0415 Expiration Date: None