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:

Army 365

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

12/17/21

Network Enterprise Technology Command (NETCOM)

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.

The purpose of Army 365 is office automation. In the A365 Impact Level (IL) 5 Software as a Service (SaaS) environment there is a potential for users to download and/or save PII incidental to business processes (chat, email, personal and organizational storage).

Any "user entered" personal information collected, stored, protected, or disseminated within Army365 is the responsibility of the record owner/originator of the information to ensure it's properly protected, categorized, covered under an existing system and maintained in accordance with AR 25-400-2, Army Records Information Management System (ARIMS).

See section 2.a for PII collected.

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)*

Any "user entered" personal identifiable information (PII) collected, stored, protected, or disseminated within Army365 is the responsibility of the record owner/originator of the information to ensure verification, identification, authentication, data matching, mission-related and administrative use.

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.

User information is stored in the Azure Active Directory (AAD) which is a critical component of the system supporting the provisioning process for identification and authentication. The information is necessary to support the establishment of a users email address and maintain their organization affiliation, contact information, etc. There is no opportunity for the users to opt-out.

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.

Standard information is populated as part of the Army365 global user directory. Army standards dictate the information populated based on their milConnect profile (separate system managed by the Defense Manpower Data Center (DMDC)) which ultimately is used to populate information into Army365 as well as the enterprise user directory.

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

Standard Mandatory DoD Notice and Consent

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.

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.	All of Army Active Directory Federation Services (ADFS), Azure Active Directory (AAD),
☒	Other DoD Components	Specify.	Defense Manpower Data Center (DMDC)
☐	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
☒ Existing DoD Information Systems
☐ Other Federal Information Systems
☒ Databases
☐ Commercial Systems

Information is obtained via milConnect, current Army systems, and the enterprise records feeding from the enterprise user directory.

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

☐ E-mail
☐ Face-to-Face Contact
☐ Fax
☒ Information Sharing - System to System
☒ Other *(If Other, enter the information in the box below)*
☐ Official Form (*Enter Form Number(s) in the box below)*
☐ Paper
☐ Telephone Interview
☐ Website/E-Form

Any "user entered" personal information collected, stored, protected, or disseminated within Army365 is the responsibility of the record owner/originator of the information to ensure it's properly protected, categorized, covered under an existing system and maintained in accordance with AR 25-400-2, Army Records Information Management System (ARIMS).

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://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.

Army365 is not the initial point of collection. Records maintained in this system are covered by existing systems of records notices that are published in the Federal Register.

See current approved SORNs at: https://dpcld.defense.gov/

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 3.1 item 010, DAA-GRS-2013-0005-0006

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

(3) Retention Instructions.

Army 365 is not a recordkeeping system. Any data or records collected are required to be maintained in accordance with AR 25-400-2, Army Records Information Management System (ARIMS).

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.

10. U.S.C 7013, Secretary of the Army; AR 25-1, Army Information Technology; AR 25-2 Army Cybersecurity. Department of Defense Directive 8500.01E, Information Assurance (IA); DoD Instruction 8500.2, Information Assurance Implementation; 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.

IAW DODM 8910.01, Vol II, para 8b. (11), Information Collected within the scope of employment (includes tasks to accomplish the job that

are performed) and coupled with the collection of minimal information (name, address, phone number to include email address) that is contained within existing OMB approved collections.