# 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:**

MILSUITE - MILSUITE

**2. DOD COMPONENT NAME:**

United States Army

**3. PIA APPROVAL DATE:**

Program Executive Office Command, Control, Communications - Tactical (PEO C3T) / Project Lead (PL) Network Enablers (NET E) / Product Lead (PdL) Military Technical Solutions (MilTech)

## 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
- [x] 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
- [x] 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 milSuite is to provide a collection of social business tools for Department of Defense (DoD) personnel (Common Access Card (CAC) enabled approved) that facilitates professional networking, learning, and innovation through knowledge sharing and collaboration. This system connects Military, DoD Civilian, and DoD Contractor personnel from across the DoD enterprise and provides individuals, units, and organizations a platform to quickly and easily build tools and business processes to support execution of the mission. Access is controlled based on individual needs for specific types of information. Statistical data, with all personal identifiers removed, may be used by management for system efficiency, workload calculation, or reporting purposes. milSuite registers users and displays data from Defense Manpower Data Center's (DMDC) Defense Enrollment Eligibility Reporting System (DEERS), e.g. name, basic employment information (work phone, address, email), and allows users to post profile pictures to help build their professional network across the milSuite platform with other DoD users. milSuite collects Personally Identifiable Information (PII) for authentication, access control to the system, information contained in the system, and general identification management.

milSuite is comprised of five major applications behind the firewall: milBook, milSurvey, milTube, milUniversity, milWiki.

milBook provides users the ability to connect with other users and establish a professional network of colleagues and subject matter experts from across the DoD. Users can post status updates, blog posts, and a variety of other content types either in their individual space or as part of a collaboration space.

milSurvey provides an online survey platform, enabling users to develop, publish and collect responses to surveys. Surveys can include everything from simple questionnaires to surveys with conditional branching questions and can provide basic statistical analysis of survey results.

milTube is a media sharing capability that allows users to share video across the DoD. Video content is primarily focused on system and application training, news and event updates, senior leader messages and information-based material from across the services.

milUniversity is an application that allows organizational trainers to post their learning content and training materials to reach a focused or joint audience on milSuite.

milWiki is a knowledge management tool used by the DoD community. It is a powerful tool and a living knowledge bank where experts are encouraged to contribute their experience and update information as it happens. milWiki's mission is to capture the knowledge and information of the DoD community and allow users to easily locate and impact that knowledge through community updates.

**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)*

Name and basic employment information is collected for registration of users into the milSuite platform for verification, authentication, and identification of users and mission-related use of data to allow users to connect with other DoD users and share knowledge across milSuite. Users have the option to upload a profile picture, videos, or other personal information if they desire. milSuite may contain unsolicited PII through user sharing of personal information (education and specialized training; professional and personal interests) using milSuite content types like blog posts, image and video uploads, and profile entries.

**e. Do individuals have the opportunity to object to the collection of their PII?** [X] 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.

A user can object to the collection of their PII by not agreeing to the Privacy Act Statement (PAS) on the milSuite login page. If the user does not agree with the Privacy Act Statement on login then milSuite access is not granted. If a user opts to join milSuite, PII data such as name and email are required to implement and operate the milSuite platform. milSuite displays information from Defense Manpower Data Center's (DMDC) Defense Enrollment Eligibility Reporting System (DEERS). Upon opting to join, a user can upload a profile picture, videos, or other personal information if they desire, but it is not required. If a user objects to a collection after agreeing to the PAS the account will be removed from the system upon request.

**f. Do individuals have the opportunity to consent to the specific uses of their PII?** [X] 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.

A user can consent to the collection of their PII by not agreeing to the Privacy Act Statement (PAS) on the milSuite login page. If the user does not agree with the Privacy Act Statement on login then milSuite access is not granted. If a user opts to join milSuite, PII data such as name and email are required to implement and operate the milSuite platform. milSuite displays information from Defense Manpower Data Center's (DMDC) Defense Enrollment Eligibility Reporting System (DEERS). Upon opting to join, a user can upload a profile picture, videos, or other personal information if they desire, but it is not required. If a user objects to a collection after agreeing to the PAS the account will be removed from the system upon request.

**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.)*

[X] Privacy Act Statement [ ] Privacy Advisory [ ] Not Applicable

The following Privacy Act Statement is presented to users on the milSuite login page with every user login:

Authority: 10 U.S.C. 3013, Secretary of the Army; Department of Defense Instruction 8500.01, Cybersecurity; AR 25-1, Army Information Technology; Army Regulation 25-2, Information Assurance.

Principal Purpose(s): The purpose of milSuite is to provide a collection of social business tools for Department of Defense (DoD) personnel (Common Access Card (CAC) enabled approved) that facilitates professional networking, learning, and innovation through knowledge sharing and collaboration. This system connects Military, DoD Civilian, and DoD Contractor personnel from across the DoD enterprise and provides individuals, units, and organizations a platform to quickly and easily build tools and business processes to support execution of the mission. Access is controlled based on individual needs for specific types of information. Statistical data, with all personal identifiers removed, may be used by management for system efficiency, workload calculation, or reporting purposes. milSuite registers users and displays data from Defense Manpower Data Center's (DMDC) Defense Enrollment Eligibility Reporting System (DEERS), e.g. name, basic employment information (work phone, address, email), and allows users to post profile pictures to help build their professional network across the milSuite platform with other DoD users. milSuite collects Personally Identifiable Information (PII) for authentication, access control to the system, information contained in the system, and general identity management.

Routine Use(s): In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To the appropriate Federal, State, local, territorial, tribal, foreign, or international law enforcement authority or other appropriate entity where a record, either alone or in conjunction with other information, indicates a violation or potential violation of law, whether criminal, civil, or regulatory in nature.
b. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government when necessary to accomplish an agency function related to this system of records.
c. To any component of the Department of Justice for the purpose of representing the DoD, or its components, officers, employees, or members in pending or potential litigation to which the record is pertinent.
d. In an appropriate proceeding before a court, grand jury, or administrative or adjudicative body or official, when the DoD or other Agency representing the DoD determines that the records are relevant and necessary to the proceeding; or in an appropriate proceeding before an administrative or adjudicative body when the adjudicator determines the records to be relevant to the proceeding.
e. To the National Archives and Records Administration for the purpose of records management inspections conducted under the authority of 44 U.S.C. §§ 2904 and 2906.
f. To a Member of Congress or staff acting upon the Member's behalf when the Member or staff requests the information on behalf of, and at the request of, the individual who is the subject of the record.
g. To appropriate agencies, entities, and persons when (1) the DoD suspects or has confirmed that there has been a breach of the system of records; (2) the DoD has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, the DoD (including its information systems, programs, and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the DoD's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.
h. To another Federal agency or Federal entity, when the DoD determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

Disclosures: Voluntary. If a user decides to join milSuite, PII data such as name and email are required to implement and operate the milSuite platform. milSuite displays information from Defense Manpower Data Center's (DMDC) Defense Enrollment Eligibility Reporting System (DEERS). Upon joining a user has the option to upload a profile picture, videos, or other personal information if they desire, but it is not required.

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

| | | | |
|---|---|---|---|
| [x] | Within the DoD Component | Specify. | milSuite users (with DoD CAC) have access to the provided PII. |
| [x] | Other DoD Components | Specify. | milSuite users (with DoD CAC) have access to the provided PII. |
| [x] | Other Federal Agencies | Specify. | milSuite users (with DoD CAC) have access to the provided PII. As specified in the routine uses of the SORN. |
| [x] | State and Local Agencies | Specify. | milSuite users (with DoD CAC) have access to the provided PII. As specified in the routine uses of the SORN. |

☒ 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. Data Systems Analysts, Inc. (DSA) - The Contractor System Administrators will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.

☐ 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

DMDC DEERS is used to display the profile data within milSuite. An individual has the option to upload a profile picture, videos, or other personal information if they desire.

**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)*

**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 A0025-1 CIO G6

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.

milSuite plans to leverage and modify AKO SORN A0025-1 CIO G6 to include both milSuite and AKO. A draft SORN amendment is being submitted with the PIA.

**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-2016-0013-00

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

(3) Retention Instructions.

K5. Destroy when 5 years old, but longer retention is authorized if needed for business use.

**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. 3013, Secretary of the Army; Department of Defense Instruction 8500.01, Cybersecurity; AR 25-1, Army Information Technology; Army Regulation 25-2, Information Assurance.

**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 applicable per DoD Manual 8910.01, Volume 2, as it is a DOD internal information collection, and does not collect information from members of the public.