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:

Military OneSource Business Operations (MOS-OPS) Information System

2. DOD COMPONENT NAME:

Office of Secretary of Defense

3. PIA APPROVAL DATE:

11/10/21

Deputy Assistant Secretary of Defense (DASD) for Military Community and Family Policy (MC&FP)

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
- [x] 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
- [x] 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 Under Secretary of Defense for Personnel and Readiness (USD/P&R) Office of the Deputy Assistant Secretary of Defense for Military Community and Family Policy (MC&FP) is directly responsible for programs and policies that establish and support community quality of life and readiness programs for service members, their families, and service providers worldwide. As part of its mission, MC&FP provides for family support policies and programs in areas including family center operations, child care, youth programs, family advocacy, relocation, transition support services and support during mobilization and deployment. In support of these missions, The Military OneSource Business Operations Information System (IS) drives the technological capabilities that deliver the full ecosystem of Military OneSource web-based services and capabilities. The Military OneSource Business Operations IS assists MC&FP with the delivery of relationship counseling resources, non-medical counseling services, financial counseling services and resources, spouse scholarship, education and career benefits, child care options and more. Lastly, the MC&FP CAS (Central Authentication Service) serves as a core component of the Military OneSource Business Operations IS, thereby delivering single-sign on features to the IS.

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)*

Identification, (person) data matching, and mission-related use.

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.

The disclosure of information to MC&FP is voluntary in association with a variety of Military OneSource services, however, if data in the MOS-OPS information system is not up-to-date, the individual's Military OneSource entitlements, privileges, and/or the ability of MC&FP to identify the individual as a DoD affiliated person could be delayed. Any further objections should be directed to the MC&FP Privacy Officer or Chief Information Officer.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [ ] Yes [x] 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 disclosure of information to MC&FP is voluntary in association with a variety of Military OneSource services, however, if data in the MOS-OPS information system is not up-to-date, the individual's Military OneSource entitlements, privileges, and/or the ability of MC&FP to identify the individual as a DoD affiliated person could be delayed.

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

PRIVACY ACT STATEMENT

Authority: 10 U.S.C. § 1788, "Additional Family Assistance," as codified on December 2, 2002, and the legislative mandates/authorities of:
a. Public Law (P.L.) 109–364 National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2007, Sec. 675, "Joint Family Support Assistance Program." October 17, 2006;
b. P.L. 111–84, NDAA for FY 2010, Sec. 561, "Establishment of Online Resources to Provide Information About Benefits and Services Available to Members of the Armed Forces and Their Families." October 28, 2009;
c. P.L. 107-107 NDAA for FY 2002 Sec. 571, "Improved Financial and Other Assistance to Military Spouses for Job Training and Education." December 28, 2001;
d. House Report (H. Rpt.) 114-537, "National Defense Authorization Act for Fiscal Year 2017," p.173, "Network of Support"; and
d. Title 10 U.S.C. 1056, "Relocation Assistance Program," January 2, 2006.

Purpose: The data provided will be used to validate your eligibility for non-public Military OneSource Business Operations information system services and capabilities. This eligibility validation will be executed via 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.

Routine Uses: 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 as a routine use pursuant to 5 U.S.C 552a(b)(3) as follows:
a. To contractors performing/working on a contract for the DoD to accomplish an agency function related to this system of records.
b. To complainants and/or victims to the extent necessary to provide such persons with information and explanations concerning the progress and/or results of an investigation or case arising from the matters of which they complained and/or of which they were a victim.
c. To such recipients and under such circumstances and procedures as are mandated by federal statute or treaty.
d. 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.
e. 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.
f. 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.
g. To the National Archives and Records Administration (NARA) for the purpose of records management inspections conducted under the authority of 44 U.S.C. § 2904 and 2906.
h. 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.
i. 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.
j. 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.

Disclosure: Furnishing this information is voluntary; however, if the data in the MOS-OPS information system is not up-to-date, your Military OneSource entitlements, privileges, and/or the ability of MC&FP to identify you as a DoD affiliated person could be delayed.

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.	DASD MC&FP
☐	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

Defense Manpower Data Center (DMDC) DS Logon Services --- Details: DS Logon was created by DMDC as a secure logon credential for DoD or VA-affiliated individuals to access self-service applications. It consists of a user name and password and was initially created to enable access to applications where a Common Access Card is unavailable.

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 DPR 45

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.

Pending coordination with DPCLTD

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. See below

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

(3) Retention Instructions.

Master database files (DAA-0330-2014-0017-0001): Cut off after 3 years of continuous inactivity or notification of discharge, retirement or separation of the service member. Destroy 10 years after cut off.

Non-medical counseling records (DAA-0330-2014-0017-0002): Cut off after 3 years of continuous inactivity or notification of discharge, retirement or separation of the service member. Destroy 15 years after cut off.

Training records (DAA-0330-2016-0006-0001): Cut off annually upon completion of training. Destroy 5 years after cut off.

Call center recordings (DM-0330-2014-0017-0003): Cut off after referral to non-medical counseling, employee assistance program support, information and referral. Destroy 90 days after cut off."

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 MOS-OPS Information System serves as the IT foundation of the Military OneSource continuum of support that, in totality, provides 24/7/365 centralized assistance, information dissemination and support to Service members, their families and survivors. This information system supports the legislative assistance and welfare mandates of 10 U.S.C. § 1788, "Additional Family Assistance," as codified on December 2, 2002, and the legislative mandates/authorities of:

a. Public Law (P.L.) 109–364 National Defense Authorization Act (NDAA) for Fiscal Year (FY) 2007, Sec. 675, "Joint Family Support Assistance Program." October 17, 2006;
b. P.L. 111–84, NDAA for FY 2010, Sec. 561, "Establishment of Online Resources to Provide Information About Benefits and Services Available to Members of the Armed Forces and Their Families." October 28, 2009;
c. P.L. 107-107 NDAA for FY 2002 Sec. 571, "Improved Financial and Other Assistance to Military Spouses for Job Training and Education." December 28, 2001;
d. House Report (H. Rpt.) 114-537, "National Defense Authorization Act for Fiscal Year 2017," p.173, "Network of Support"; and
e. Title 10 U.S.C. 1056, "Relocation Assistance Program," January 2, 2006; and
f. NDAA 2020 Section 570E, "Pilot program on information sharing between Department of Defense (DoD) and designated relatives and friends of member of the Armed Services regarding the experiences and challenges of military service" which directs DOD to develop a pilot program encouraging new recruits to designate up to ten persons [public] to receive information regarding the military service of that member.

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 No. 0704-0528
Expiration Date: February 28, 2022