# 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:**

Employer Support of the Guard and Reserve Member Management System (MMS)

**2. DOD COMPONENT NAME:**

Defense Human Resources Activity

**3. PIA APPROVAL DATE:**

09/12/19

Defense Personnel and Family Support Center/Employer Support of the Guard and Reserve

## 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 the Member Management System (MMS) is to maintain a roster of and facilitate communication between Employer Support to the Guard and Reserve (ESGR) members, and to track ESGR-related training, awards, and hours donated by ESGR DoD volunteer staff. Additionally, the system is used to identify federal employee and ESGR DoD volunteer emergency contact information for accountability during manmade disasters and other emergencies.

Types of personal information collected include: Full name; role/position and ESGR affiliation (State Committee region or headquarters); military base for volunteer activity; home address, home and/or mobile phone number, and personal email address; ESGR-related training completed; affiliated Service (if applicable); and emergency contact name, phone number, and relationship.

Additional information collected on federal employees include: work address, work phone number, and work email; assigned military unit and rank (where applicable); and official report and departure date.

Additional information collected on DoD volunteers include: volunteer hours performed; awards; mentor/mentee assignments; military experience (component, rank, status, and years of service); civilian work experience (industry and position type); special skills or qualifications; shirt size; and form of DoD identification (where applicable).

**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)*

Mission-related use; identification

**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 provide information voluntarily and are presented with a Privacy Act Statement at the point of collection. Failure to provide information, however, may inhibit participation as a Employer Support to the Guard and Reserve (ESGR) volunteer.

**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 provide information voluntarily and are presented with a Privacy Act Statement at the point of collection. By providing the information the individual is consenting to the specific use outlined in the Privacy Act Statement and System of Records Notice. Failure to provide information, however, may inhibit participation as a Employer Support to the Guard and Reserve (ESGR) volunteer.

**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

Authorities: 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1588, Authority to accept certain voluntary services; DoD Instruction (DoDI) 1205.22, Employer Support of the Guard and Reserve; DoDI 1100.21, Voluntary Services in the Department of Defense; and DoDI 3001.02, Personnel Accountability in Conjunction With Natural or Manmade Disasters.

Purpose: To maintain a roster of and facilitate communication between Employer Support to the Guard and Reserve (ESGR) members, and to track ESGR-related training, awards, and hours donated by ESGR DoD volunteer staff. Additionally, the system is used to identify federal employee and ESGR DoD volunteer emergency contact information for accountability during manmade disasters and other emergencies.

Routine Use(s): Routine uses may be found in the applicable system of records notice DHRA 17, Employer Support of the Guard and Reserve Member Management System (MMS) at: https://dpcld.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/608082/ingb-004/

Disclosure: Voluntary, however, failure to provide information may inhibit participation as a Employer Support to the Guard and Reserve (ESGR) volunteer.

**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. | |
| □ 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. | DSF FEDERAL, INC. Perform offsite work with Personally Identifiable Information (PII) only on systems and platform information technology systems (PIT) that meet Risk Management Framework (RMF) for DoD Information Technology (IT) requirements. FAR privacy clauses 52.224-1 and 52.224-2, and FAR 39.105 are not included. |
| □ 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)*
☒ 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 DHRA 17

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. OSD 202-07 and 202-17

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

(3) Retention Instructions.

202-07, Office Personnel Information Files, Temporary. Review annually at the end of each year and destroy superseded documents. Cut off file when employee separation or transfer and destroy remaining documents 1 year after cutoff.
202-17, Volunteer Service Case Files, Temporary. Cut off when volunteer departs service. Destroy 4 years after cutoff.

**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. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 1588, Authority to accept certain voluntary services; DoD Instruction (DoDI) 1205.22, Employer Support of the Guard and Reserve; DoDI 1100.21, Voluntary Services in the Department of Defense; and DoDI 3001.02, Personnel Accountability in Conjunction With Natural or Manmade Disasters.

**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.

Volunteers are legally considered DoD employees when providing volunteer services to the Department.

## SECTION 2: PII RISK REVIEW

**a. What PII will be collected** *(a data element alone or in combination that can uniquely identify an individual)? (Check all that apply)*

□ Biometrics
□ Citizenship
□ Driver's License
☒ Employment Information
☒ Home/Cell Phone
☒ Mailing/Home Address
☒ Military Records
☒ Official Duty Address
□ Passport Information
□ Place of Birth
□ Race/Ethnicity
□ Records
☒ Work E-mail Address

□ Birth Date
□ Disability Information
□ Education Information
□ Financial Information
□ Law Enforcement Information
□ Marital Status
□ Mother's Middle/Maiden Name
☒ Official Duty Telephone Phone
☒ Personal E-mail Address
☒ Position/Title
□ Rank/Grade
□ Security Information
□ If Other, enter the information in the box below

□ Child Information
□ DoD ID Number
☒ Emergency Contact
□ Gender/Gender Identification
□ Legal Status
□ Medical Information
☒ Name(s)
□ Other ID Number
□ Photo
□ Protected Health Information (PHI)[1]
□ Religious Preference
□ Social Security Number (SSN) *(Full or in any form)*

Role/position and ESGR affiliation (State Committee region or headquarters); military base for volunteer activity; ESGR-related training completed; official report and departure date; volunteer hours performed; awards; mentor/mentee assignments; special skills or qualifications; and shirt size.

If the SSN is collected, complete the following questions.

*(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

(1) Is there a current (dated within two (2) years) DPCLTD approved SSN Justification on Memo in place?

□ Yes □ No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

(2) Describe the approved acceptable use in accordance with DoD Instruction 1000.30 "Reduction of Social Security Number (SSN) Use within DoD".

(3) Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instructoin 1000.30, "Reduction of Social Security Number (SSN) Use within DoD".

(4) Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

□ Yes □ No

**b. What is the PII confidentiality impact level[2]?** ☒ Low □ Moderate □ High

[1] The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

[2] Guidance on determining the PII confidentiality impact level, see Section 2.5 "Categorization of PII Using NIST SP 800-122." Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is

most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

**c. How will the PII be secured?**

(1) Physical Controls. *(Check all that apply)*

☒ Cipher Locks
☒ Combination Locks
☒ Key Cards
□ Security Guards
☒ Closed Circuit TV (CCTV)
☒ Identification Badges
□ Safes
☒ If Other, enter the information in the box below

Controlled screenings

(2) Administrative Controls. *(Check all that apply)*

☒ Backups Secured Off-site
☒ Encryption of Backups
☒ Methods to Ensure Only Authorized Personnel Access to PII
☒ Periodic Security Audits
☒ Regular Monitoring of Users' Security Practices
☒ If Other, enter the information in the box below

Visitor registers

(3) Technical Controls. *(Check all that apply)*

□ Biometrics
☒ Encryption of Data at Rest
☒ Firewall
☒ Role-Based Access Controls
☒ Virtual Private Network (VPN)
☒ Common Access Card (CAC)
□ Encryption of Data in Transit
☒ Intrusion Detection System (IDS)
□ Used Only for Privileged (Elevated Roles)
□ If Other, enter the information in the box below
□ DoD Public Key Infrastructure Certificates
□ External Certificate Authority Certificates
□ Least Privilege Access
☒ User Identification and Password

Two-factor authentication

**d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?**