PRIVACY IMPACT ASSESSMENT (PIA)

For the

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

SECTION 1: IS A PIA REQUIRED?

a. Will this Department of Defense (DoD) information system or electronic collection of information (referred to as an "electronic collection" for the purpose of this form) collect, maintain, use, and/or disseminate PII about members of the public, Federal personnel, contractors or foreign nationals employed at U.S. military facilities internationally? Choose one option from the choices below. (Choose (3) for foreign nationals).

☐ (1) Yes, from members of the general public.

☒ (2) Yes, from Federal personnel* and/or Federal contractors.

☐ (3) Yes, from both members of the general public and Federal personnel and/or Federal contractors.

☐ (4) No

* "Federal personnel" are referred to in the DoD IT Portfolio Repository (DITPR) as "Federal employees."

b. If "No," ensure that DITPR or the authoritative database that updates DITPR is annotated for the reason(s) why a PIA is not required. If the DoD information system or electronic collection is not in DITPR, ensure that the reason(s) are recorded in appropriate documentation.

c. If "Yes," then a PIA is required. Proceed to Section 2.

SECTION 2: PIA SUMMARY INFORMATION

a. Why is this PIA being created or updated? Choose one:

- ☐ **New DoD Information System**
- ☐ **New Electronic Collection**
- ☒ **Existing DoD Information System**
- ☐ **Existing Electronic Collection**
- ☐ **Significantly Modified DoD Information System**

b. Is this DoD information system registered in the DITPR or the DoD Secret Internet Protocol Router Network (SIPRNET) IT Registry?

- ☒ **Yes, DITPR** Enter DITPR System Identification Number: 10314
- ☐ **Yes, SIPRNET** Enter SIPRNET Identification Number:
- ☐ **No**

c. Does this DoD information system have an IT investment Unique Project Identifier (UPI), required by section 53 of Office of Management and Budget (OMB) Circular A-11?

- ☒ **Yes**
- ☐ **No**

If "Yes," enter UPI 1344

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

d. 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 should be consistent.

- ☒ **Yes**
- ☐ **No**

If "Yes," enter Privacy Act SORN Identifier DHRA 17

DoD Component-assigned designator, not the Federal Register number.
Consult the Component Privacy Office for additional information or
access DoD Privacy Act SORNs at: http://www.defenselink.mil/privacy/notices/

or

Date of submission for approval to Defense Privacy Office
Consult the Component Privacy Office for this date. Pending

e. Does this DoD information system or electronic collection have an 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**

Enter OMB Control Number

Enter Expiration Date

☒ **No**

f. Authority to collect information. A Federal law, Executive Order of the President (EO), or DoD requirement must authorize the collection and maintenance of a system of records.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be the same.

(2) 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) Whenever possible, cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If a specific statute or EO does not exist, determine if an indirect statutory authority can be cited. An indirect 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) 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 should be identified.

10 U.S.C. 1588, Authority to accept certain voluntary services; DoD Directive 1250.01, National Committee for Employer Support of the Guard and Reserve (NCESGR); DoD Instruction 1205.22, Employer Support of the Guard and Reserve; DoD Instruction 1100.21, Voluntary Services in the Department of Defense; and DoD Instruction 3001.02, Personnel Accountability in Conjunction With Natural or Manmade Disasters.

g. Summary of DoD information system or electronic collection. Answers to these questions should be consistent with security guidelines for release of information to the public.

(1) Describe the purpose of this DoD information system or electronic collection and briefly describe the types of personal information about individuals collected in the system.

To maintain a roster of and facilitate communication between ESGR members; to track ESGR-related training, awards, and hours donated by ESGR DoD volunteer staff; and to identify federal employee and ESGR DoD volunteer staff emergency contact information in the event of an emergency.

Full name; role/position and ESGR affiliation (State Committee region or Headquarters); home address, home and/or mobile phone number, personal email address; ESGR-related training completed; affiliated Service (if applicable); emergency contact name, phone number, and relationship.

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

Additional information collected on DoD volunteers, includes: 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; and form of DoD identification (where applicable).

(2) Briefly describe the privacy risks associated with the PII collected and how these risks are addressed to safeguard privacy.

The privacy risks associated with the PII collected are information mishandling and improper release to personnel without a need to know. To safeguard such information, MMS and the PII it holds is maintained in a secure, password protected electronic system that utilizes security hardware and software. Physical controls include combination locks, cipher locks, key cards, identification badges, closed circuit televisions, and controlled screenings. Technical controls include use of user identification and password, intrusion detection systems, encryption, Common Access Card, firewalls, virtual private networks, role-based access controls, and two-factor authentication. Administrative controls include periodic security audits, regular monitoring of users' security practices, methods to ensure only authorized personnel access information, encryption of backups containing sensitive data, backups secured off-site, and use of visitor registers.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component (e.g., other DoD Components, Federal Agencies)? Indicate all that apply.

☐ **Within the DoD Component.**

Specify.

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☐ **Other** (e.g., commercial providers, colleges).

Specify.

i. Do individuals have the opportunity to object to the collection of their PII?

☒ **Yes** ☐ **No**

(1) If "Yes," describe method by which individuals can object to the collection of PII.

Individuals may object to the collection of their PII by not providing their information to ESGR; however, failure to provide accurate contact information and other solicited information may delay or prevent ESGR from facilitating communications between ESGR members.

(2) If "No," state the reason why individuals cannot object.

j. 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 may not consent to specific uses of their PII as the information provided is required for proper employee and volunteer management, as well as emergency response.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ **Privacy Act Statement** ☐ **Privacy Advisory**

☒ **Other** ☐ **None**

Describe each applicable format.

ESGR Volunteer Information Form (Local form)
Authority:
10 U.S.C. 1588, Authority to accept certain voluntary services; DoD Directive 1250.01, National Committee for Employer Support of the Guard and Reserve (NCESGR); DoD Instruction 1205.22, Employer Support of the Guard and Reserve; DoD Instruction 1100.21, Voluntary Services in the Department of Defense; and DoD Instruction 3001.02, Personnel Accountability in Conjunction With Natural or Manmade Disasters.

Purpose:
To maintain a roster of and facilitate communication between ESGR members; to track ESGR-related training, awards, hours donated by ESGR DoD volunteer staff, and ESGR DoD volunteer staff demographics; and to identify federal employee and ESGR DoD volunteer emergency contact information in the event of an emergency.

Routine Use(s):
Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: Law Enforcement Routine Use, Congressional Inquiries, Disclosure to the Department of Justice for Litigation Routine Use, Disclosure of Information to the National Archives and Records Administration Routine Use, and Data Breach Remediation Purposes Routine Use. The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

Disclosure:
Voluntary; however, failure to provide accurate contact information and other solicited information may delay or prevent ESGR from processing the request.

ESGR Personal Emergency Data Form (Local form)
Authority:
10 U.S.C. 1588, Authority to accept certain voluntary services; DoD Directive 1250.01, National Committee for Employer Support of the Guard and Reserve (NCESGR); DoD Instruction 1205.22, Employer Support of the Guard and Reserve; DoD Instruction 1100.21, Voluntary Services in the Department of Defense; and DoD Instruction 3001.02, Personnel Accountability in Conjunction With Natural or Manmade Disasters.

Purpose:
To identify federal employee and ESGR DoD volunteer emergency contact information in the event of an emergency.

Routine Use(s):
Disclosure of records are generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, as amended, the records contained herein may be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: Law Enforcement Routine Use, Congressional Inquiries, Disclosure to the Department of Justice for Litigation Routine Use, Disclosure of Information to the National Archives and Records Administration Routine Use, and Data Breach Remediation Purposes

Routine Use. The DoD Blanket Routine Uses set forth at the beginning of the Office of the Secretary of Defense (OSD) compilation of systems of records notices apply to this system. The complete list of DoD Blanket Routine Uses can be found Online at: http://dpcld.defense.gov/Privacy/SORNsIndex/BlanketRoutineUses.aspx.

Disclosure:
Voluntary; however, failure to provide accurate contact information and other solicited information may delay or prevent ESGR from processing the request.

NOTE:

Sections 1 and 2 above are to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy.

A Component may restrict the publication of Sections 1 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.