

**SYSTEM NAME AND NUMBER:** Employer Support of the Guard and Reserve Member Management System (MMS), DHRA 17 DoD. (November 10, 2020; 85 FR 71636)

**SECURITY CLASSIFICATION:** Unclassified.

**SYSTEM LOCATION:** Defense Information Systems Agency (DISA), Computing Directorate Mechanicsburg, 5450 Carlisle Pike, Mechanicsburg, PA 17050-2411.

**SYSTEM MANAGER(S):** Executive Director, Headquarters, Employer Support of the Guard and Reserve, 4800 Mark Center Drive, Alexandria, VA 22350-1200, Email: OSD.ESGRITSupport@mail.mil.

**AUTHORITY FOR MAINTENANCE OF THE SYSTEM:** 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(S) OF THE SYSTEM:** To maintain a roster of and facilitate communication between Employer Support to the Guard and Reserve (ESGR) members; and track ESGR-related training, awards, and hours donated by ESGR Department of Defense (DoD) volunteer staff. To maintain personnel accountability and ESGR DoD volunteer emergency contact information for accountability during manmade disasters and other emergencies.

**CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM:** DoD-affiliated personnel to include: Military Service members (active duty, Guard/Reserve and the Coast Guard personnel), civilian employees (including non-appropriate fund employees); and other individuals working for or affiliated with ESGR.

**CATEGORIES OF RECORDS IN THE SYSTEM:** Name; home and work address; phone numbers (home, work, and mobile); email addresses (work and personal); position/title; assigned military unit and rank; official report and departure date;

ESGR affiliation (State Committee region or headquarters); military base for volunteer activity; ESGR-related training completed; and emergency contact information to include name, phone number, and relationship.

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).

**RECORD SOURCE CATEGORIES:** The individual.

**ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND PURPOSES OF SUCH USES:** In addition to those disclosures generally permitted under 5 U.S.C. 552a (b) of the Privacy Act of 1974, as amended,

these 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 contractors, grantees, experts, consultants, students, and others responsible for performing or working on contracts for the DoD when necessary to accomplish an agency function related to this System of Records.
- b. 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.
- 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 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 confirms a breach of the System of Records; (2) the DoD determines 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 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.

**POLICIES AND PRACTICES FOR STORAGE OF RECORDS:** Electronic storage media.

**POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS:** Records are retrieved by full name and ESGR affiliation.

## **POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:**

Headquarters Personnel Records. Cut off upon employee separation or transfer. Destroy upon supersession or 1 year after cut off. Volunteer Staff Records: Cut off upon volunteer departure from program. Destroy/delete 4 years after cut off.

**ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS:** All personally identifiable information (PII) is maintained in a secure, password protected electronic system. The system utilizes security hardware and software to include physical controls such as combination locks, cipher locks, key cards, identification badges, closed circuit televisions, and controlled screenings. Technical controls include the use of user identifications and passwords, intrusion detection systems, encryption, Common Access Cards (CAC), 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, visitor registers, and backups secured off-site.

**RECORD ACCESS PROCEDURES:** Individuals seeking access to records about themselves contained in this system should address written inquiries to the Office of the Secretary of Defense/Joint Staff, Freedom of Information Act Requester Service Center, Office of Freedom of Information, 1155 Defense Pentagon, Washington, DC 20301-1155. Signed written requests should contain the individual's full name, personal contact information (home address, phone number, email), and the number and name of this system of records notice. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: "I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature)."

If executed within the United States, its territories, possessions, or commonwealths: "I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature)."

**CONTESTING RECORD PROCEDURES:** The DoD rules for accessing records, contesting contents, and appealing initial agency determinations are contained in 32 CFR part 310 or may be obtained from the system manager.

**NOTIFICATION PROCEDURES:** Individuals seeking to determine whether information about themselves is contained in this system should address written inquiries to the Executive Director, Headquarters, Employer Support of the Guard and Reserve, 4800 Mark Center Drive, Alexandria, VA 22350-1200. Signed written requests should contain the individual's full name, ESGR affiliation, and personal contact information (home address, phone number, and email).

In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746, in the following format:

If executed outside the United States: “I declare (or certify, verify, or state) under penalty of perjury under the laws of the United States of America that the foregoing is true and correct. Executed on (date). (Signature).”

If executed within the United States, its territories, possessions, or commonwealths: “I declare (or certify, verify, or state) under penalty of perjury that the foregoing is true and correct. Executed on (date). (Signature).”

**EXEMPTIONS PROMULGATED FOR THE SYSTEM:** None.

**HISTORY:** 81 FR 37585, June 10, 2016.