

SYSTEM NAME AND NUMBER: Employer Support of the Guard and Reserve Ombudsman Inquiry and Case Management System (ICMS), DHRA 16. (September 23, 2020; 85 FR 59757)

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, Employer Support of the Guard and Reserve, Suite 05E22, 4800 Mark Center Drive, Alexandria, VA 22350-1200; email: osd.USERRA@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 38 U.S.C. Ch. 43, Employment and Reemployment Rights of Members of the Uniformed Services; 5 U.S.C. 574, Confidentiality; 5 U.S.C. Part I, Chapter 5, Subchapter IV, Alternative Means of Dispute Resolution in the Administrative Process; 42 U.S.C. 300hh-11, National Disaster Medical System, ((d)(3) Employment and reemployment rights); 20 CFR 1002, Regulations Under the Uniformed Services Employment and Reemployment Rights Act of 1994; 5 CFR 353, Restoration to Duty from Uniformed Service or Compensable Injury; DoD Instruction 1205.22, Employer Support of the Guard and Reserve; and DoD Instruction 1205.12, Civilian Employment and Reemployment Rights for Service Members, Former Service Members and Applicants of the Uniformed Services.

PURPOSE(S) OF THE SYSTEM: To record information related to the mediation of disputes and inquiry responses related to the Uniformed Services Employment and Reemployment Rights Act (USERRA); to track case assignments and mediation results of potential conflicts between employers and the National Guard, Reserves, or National Disaster Medical Service (NDMS) members in their employ; and to report statistics related to the Ombudsman Program in aggregate and at the state committee level. These records are also used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness and conducting research.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Members of the National Guard, Reserves, and NDMS submitting inquiries or requesting mediation; Employers (personnel) of the Guard and Reserve (ESGR) personnel; civilian employers; contractors and volunteers handling inquiries and cases; and individuals submitting inquiries.

CATEGORIES OF RECORDS IN THE SYSTEM: Individual's full name, home address, home or work phone number, home or work email address; current Uniformed Service member pay grade; ESGR case number; type of USERRA issue; employer name, employer type, employer's contact name, contact phone, email and address; name, email and state committee/ESGR affiliation of ESGR employee, contractor, or volunteer who handles an inquiry or mediation case; and case notes.

RECORD SOURCE CATEGORIES: Individual Members of the National Guard, Reserves, and National Disaster Medical System (NDMS) who submit inquiries or request mediation, and the Member Management System.

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, 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:

- a. To contractors, grantees, experts, consultants, students, and others performing or working on a contract, service, grant, cooperative agreement, or other assignment for the DoD when necessary to accomplish an agency function related to this system of records.
- b. To Department of Labor for Congressionally-mandated USERRA reporting (38 U.S.C. Employment and Reemployment Rights of Members of the Uniformed Services § 4432, Reports) with consideration of 5 U.S.C. 574, Confidentiality requirements.
- c. 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.
- d. 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.
- e. 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.
- f. 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.
- g. 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.
- h. 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.
- i. 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: Records are maintained in electronic storage media.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records are retrieved by individual's full name and/or case number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Temporary. Destroy 7 years after case is closed.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: Physical controls include combination locks, cipher locks, key cards, security guards, identification badges, closed circuit televisions, and controlled screenings. Technical controls include encryption of data at rest, encryption of data in transit, user identification and password, intrusion detection system, Common Access Card, firewall, virtual private network, role-based access controls, least privilege access, DoD public key infrastructure certificates, 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.

RECORD ACCESS PROCEDURES: Individuals seeking access to records about themselves contained in this system should address 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 include the individual's full name and personal contact information (address, phone number, and email), and the name and number of this system of records notice (SORN). 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, its territories, possessions, or commonwealths: "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 of records 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 and personal contact information (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: April 14, 2006, 71 FR 19486; November 14, 2007, 72 FR 64058; October 23, 2015, 80 FR 64401.