

SYSTEM NAME AND NUMBER: Commander's Risk Reduction Dashboard (CRRD), A0600-63 DAPE G-1. (June 11, 2020; 85 FR 35638)

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Regional Network Enterprise Center-Redstone (RNEC-R), Building 5301-B, Sparkman Center, Redstone Arsenal, AL 35898

SYSTEM MANAGER(S): SHARP, Ready and Resilient Directorate, Deputy Chief of Staff, G-1, Headquarters, Department of the Army, 300 Army Pentagon, Washington, DC 20320-3000, usarmy.pentagon.hqda-dcs-g-1.list.crrd-army-g1@mail.mil.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 5 U.S.C. 7902, Safety Programs; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 7013, Secretary of the Army; 18 U.S.C. 3771, Crime victims' rights; 29 U.S.C. Chapter 15, Occupational Safety and Health; 34 U.S.C. 41303, Uniform Federal Crime Reporting Act of 1988; 42 U.S.C. 290dd-2, Confidentiality of records; E.O. 12564, Drug Free Federal Workplace DoD Directive (DoDD) 1030.01, Victim and Witness Assistance; DoDD 6490.02E, Comprehensive Health Surveillance; DoD Instruction (DoDI) 1030.2, Victim and Witness Assistance Procedures; DoDI 6055.01, DoD Safety and Occupational Health Program; DoDI 6495.02, Sexual Assault Prevention and Response Program Procedures; Army Regulation (AR) 190-45, Military Police Law Enforcement Reporting; AR 195-2, Criminal Investigation Activities; AR 385-10, Army Safety Program; AR 600-63, Army Health Promotion; AR 600-85, Army Substance Abuse Program; AR 608-18, Family Advocacy Program; and E.O. 9397 (SSN), as amended.

PURPOSE(S) OF THE SYSTEM: The CRRD will provide command teams (battalion commanders, company commanders, Command Sergeants Major, First Sergeants) with the necessary information to recognize early warning signs of high-risk behaviors and proactively engage in intervention activities to help reduce soldier suicides, risk-related deaths, and other negative outcomes of high-risk behavior. The command teams at battalion and company levels will be able to access information to help identify soldiers in the unit with high-risk profiles. The Command Teams at brigade and higher levels will only be provided aggregated data pertaining to their command level and its subordinate commands to identify high risk units. De-identified, aggregate data from the CRRD may also be used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness and conducting research.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: All Active duty Army, United States Army Reserve, and Army National Guard Soldiers.

CATEGORIES OF RECORDS IN THE SYSTEM: Full name, social security number (SSN), DoD Identification (DoD ID) number, date of birth, photograph, height, weight, marital status, and number of dependent family members.

Military service data to include: Rank, Military Occupational Specialty, unit identification code, unit of assignment and assignment date, Exceptional Family Member Program enrollment, promotion dates, security clearance, deployment history, awards, education level, training attendance, and physical fitness test and body fat composition results.

Personal health and wellness information to include: Date of last health assessments, drug test results, substance abuse screenings/enrollments, pending medical boards dates, date of last psychotropic or opiate prescription, documented incidents related to suicide, and Family Advocacy Program interactions.

Other adverse information to include: Record of courts-martial, referred charges and case disposition, administrative disciplinary actions, criminal history, substantiated domestic and child abuse complaints, bars/flags to reenlistment, sex offender identifier code, financial problems, and substance use disorder history.

RECORD SOURCE CATEGORIES: Individual, Command Teams, CRRD Local/Regional Administrators, Army Central Registry, Army Safety Management Information System, Army Law Enforcement Reporting and Tracking System, Army Training Management System, Defense Casualty Information Processing System, Drug and Alcohol Management Information System, Defense Finance and Accounting System, Army Organization Server, Army Training Requirements And Resource System, Army Training Management System, Defense Readiness Reporting System—Army, Deployed Theater Accountability System, Integrated Disability Evaluation System, Digital Training Management System, Master Resilience Trainer—Database of Record, Medical Occupational Data System, Military Justice Online, Official Military Personnel File, Risk Reduction Program, Military Health System Mart, Pharmacy Data Transaction Services, Theater Medical Data Store, US Military Entrance Processing Command Integrated Resource System, U.S. Army Recruiting Command, Army Waiver Data, Department of Defense Suicide Event Report, Defense Sexual Assault Incident Database, Army Leader Unit Risk Readiness Tool, Inspector General Action Request System, TRANSCOM Reference Data Management.

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. 552 a(b) of the Privacy Act of 1974, as amended, the records contained therein 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 performing or working on a contract, service, grant, cooperative agreement, or other assignment for the Federal Government 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 determined 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: Full name and DoD ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS: Disposition pending. Treat records as permanent until the National Archives and Records Administration approves the proposed retention and disposition schedule.

ADMINISTRATIVE, TECHNICAL, AND PHYSICAL SAFEGUARDS: In-depth physical, technical, and administrative controls have been established to safeguard electronic data. Records are protected in accordance with policies in DoDI 8510.01, DoD Risk Management Framework for DoD Information Technology. The system is maintained in controlled facilities that employ physical restrictions and safeguards such as security guards, identification badges, key cards, and locks. The facilities are accessible only to authorized personnel with a need-to-know. The CRRD utilizes a layered network security approach including, firewalls, host based intrusion detection, data in transit encryption, and encryption for data at rest. Access to personal data is limited to person(s) responsible for maintaining and servicing data in performance of their official duties and are properly trained, screened and cleared for a need-to-know. Access to personal data is further restricted by encryption and the use of Common Access Card. Users are required to successfully undergo and complete a National Agency Check with Inquiries along with a credit check. Role-based access to the system is managed by Army G-1 access control

procedures and policies. All aspects of privacy, security, configuration, operations, data retention, and disposal are documented to ensure privacy and security are consistently enforced and maintained.

RECORD ACCESS PROCEDURES: Individuals seeking access to information about themselves, contained in this system should address written inquiries to the SHARP, Ready and Resilient Directorate, 2530 Crystal Drive, 6th Floor, Arlington, VA 22202. Individuals must provide their full name, date of birth, and DoD ID Number. 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 SHARP, Ready and Resilient Directorate, 2530 Crystal Drive, 6th Floor, Arlington, VA 22202. Individuals must provide their full name, date of birth, and DoD ID Number. In addition, the requester must provide either a notarized statement or an unsworn declaration made in accordance with 28 U.S.C. 1746 to declare that the information provided in the request for notification is true and correct, 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: May 1, 2014, 79 FR 24690.