



DEPARTMENT OF DEFENSE

Department of the Navy

[Docket ID: USN-2021-HQ-0002]

Privacy Act of 1974; System of Records

AGENCY: United States Marine Corps (USMC), Department of Defense (DoD).

ACTION: Notice of a new system of records.

SUMMARY: The Department of the Navy is establishing a new System of Records entitled the Command Individual Risk and Resiliency System (CIRRAS) application. The CIRRAS application will be used by the USMC to enable Commanding Officers and Senior Enlisted Advisors to make informed and timely decisions on Force Preservation Risk Assessments, to optimize individual/unit readiness, and to facilitate enterprise-wide risk management. Individual data will assist commanders by quickly identifying those Marines or Service Members requiring immediate command attention. Trend analysis will assist USMC commanders to implement mitigation strategies to improve overall individual/unit readiness. These records will also be used as a management tool for statistical analysis, tracking, reporting, evaluating program effectiveness, and conducting research.

DATES: This new system of records is effective upon publication; however, comments on the Routine Uses will be accepted on or before **[INSERT 30 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]**. The Routine Uses are effective at the close of the comment period.

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods:

* Federal Rulemaking Portal: <https://www.regulations.gov>.

Follow the instructions for submitting comments.

* Mail: DoD cannot receive written comments at this time due to the COVID-19 pandemic.

Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number for this *Federal Register* document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at <https://www.regulations.gov> as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Sally A. Hughes, FOIA/PA Program Manager (ARSF), Headquarters, U.S. Marine Corps, 3000 Marine Corps Pentagon, Washington, DC 20350-3000, telephone (703) 614-4008.

SUPPLEMENTARY INFORMATION: The “Marine Corps Risk and Resiliency Records” system of records is being established by the USMC to support Force Preservation Risk Assessments. The Marine Corps force preservation process is the formalized method used by commanders to identify individual Marine risk factors and to apply holistic risk management measures to improve individual and unit readiness. Every day, this process assists leaders across the Corps to identify those in need. However, gaps in knowledge have historically limited the effectiveness of the effort. To improve the process, the USMC is developing the CIRRAS application, which compiles individual force preservation data input by small unit leaders, medical officers, and other support staff. By presenting timely, prioritized, actionable information to those who can help Marines, and by protecting unauthorized disclosure through strict access limits and cybersecurity, leaders will be better equipped to reduce destructive behaviors in their units.

Force Preservation Risk Assessments are based on the identification and tracking of individual Service Member behaviors associated with increased risk or resiliency as defined by the Commandant's "Six Fs," as defined in Marine Corps Order 1500.61, 28 July 2017. The Six Fs are Fidelity, Fighter, Fitness, Family, Finances and Future. Force Preservation Risk

Assessments include critical stressors that are environmental factors or experiences that can overtax a Service Member's coping resources. The intensity or accumulation of multiple stressors is linked to a greater likelihood of harmful reactions including death by suicide. The CIRRAS application is a networked, web-based application that captures risk, resiliency and critical stressor factors for all United States Marines and United States Armed Forces Service Members assigned to the USMC to provide Force Preservation information to the unit commander. The CIRRAS will directly support Commanders/Officers in Charge and Senior Enlisted Advisors by providing a tool to enable proactive identification and assessment of individual Marines' or Service Members' risk, resiliency, and critical stressor factors. Also, the system will allow the transfer of the same factors between commands in order to optimize individual/unit readiness and facilitate enterprise-wide risk management of individual Marines' risk status. The CIRRAS will be used by Regimental/Group Commanders through immediate supervisors (Platoon Commander/Officers in Charge) of all United States Marines and United States Armed Forces Service Members assigned to the USMC in accordance with Marine Corps Order 5100.29B, Marine Corps Safety Program; MCO 1500.60, Force Preservation Council (FPC) Program; and other Force Preservation Directives.

The DoD notices for systems of records subject to the Privacy Act of 1974, as amended, have been published in the *Federal Register* and are available from the address in FOR FURTHER INFORMATION CONTACT or at the Defense Privacy, Civil Liberties, and Transparency Division website at <https://dpcl.d.defense.gov>.

In accordance with 5 U.S.C. sec. 552a(r) and Office of Management and Budget (OMB) Circular No. A-108, the DoD has provided a report of this system of records to the OMB and to Congress.

Dated: February 10, 2021.

Kayyonne T. Marston,

Alternate OSD Federal Register Liaison Officer,

Department of Defense.

SYSTEM NAME AND NUMBER: Marine Corps Risk and Resiliency Records, M05230-1.

SECURITY CLASSIFICATION: Unclassified.

SYSTEM LOCATION: Command Individual Risk and Resiliency Assessment System (CIRRAS) application, AWS GovCloud (US-East), NIWC Atlantic, Charleston, Component Enterprise Data Center (CEDC), P.O. Box 190022, Bldg. 3148, North Charleston, SC 29419-9022.

SYSTEM MANAGER(S): CIRRAS System Manager, Headquarters Marine Corps, Manpower & Reserve Affairs (M&RA), Marine & Family Programs (MF) Division, 3280 Russell Rd, Quantico, VA 22134-5143, 4th Deck, CIRRAS.Support@usmc.mil, 703-432-9294.

AUTHORITY FOR MAINTENANCE OF THE SYSTEM: 10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; Department of Defense (DoD) Instruction 6490.08, Command Notification Requirements to Dispel Stigma in Providing Mental Health Care to Service Members; DoD 6025.18-R, DoD Health Information Privacy Regulation; Marine Corps Order (MCO) 1500.60, Force Preservation Council (FPC) Program; MCO 3500.27C, Risk Management; MCO 1752.5C, Sexual Assault Prevention & Response; MCO 5300.17A, Substance Abuse Program; MCO 5100.29B, Marine Corps Safety Program; MCO 5100.19F, Marine Corps Traffic Safety Program.

PURPOSE(S) OF THE SYSTEM: To capture risk, resiliency, and critical stressor factors for all United States Marines or United States Armed Forces Service Members assigned to a United States Marine Corps (USMC) unit, and to provide Force Preservation information to the USMC Unit Commander; to transfer the same between commands, in order to optimize individual/unit readiness and facilitate enterprise-wide risk management of individual Marines; to help prevent adverse outcomes including the loss of life; to quickly identify those Marines or Service Members requiring immediate command attention; and to provide trend analysis to assist in implementing mitigation strategies to improve individual/unit readiness.

CATEGORIES OF INDIVIDUALS COVERED BY THE SYSTEM: Active duty and Reserve USMC military personnel, and any other United States Armed Forces Service Members assigned to the USMC.

CATEGORIES OF RECORDS IN THE SYSTEM: Biographic information to include: full legal name, DoD ID number/Electronic Data Interchange Personal Identifier (EDIPI), citizenship/legal status, race/ethnicity, date and place of birth, gender/gender identification, home/mailling address, and phone numbers; marital status and divorce date (if any), alleged infidelity, and geographic separation from significant other; name, number of dependents, expecting parent, foster parenting, pending adoption, acting caregiver, family care plan, and housing information; date of entry, age, position/title, rank/grade, duty status, deployments, service member photo, Military Occupational Specialty (MOS), awards, End of Active Service (EAS), Pay Entry Base Date (PEBD), General Technical Score (GT) score, time in service, waivers, performance summary, monitored command code, future monitored command code, Reporting Unit Code (RUC), work email, deployment history, discipline, Non-Judicial Punishment (NJP), loss of rank, loss of pay, security clearance revocation or suspension, law enforcement events identified on military blotter, under investigation by military or civilian commands/agencies, arrested within the last twelve months, and restraining order; Command Stressors information to include: combat exposure, responsible for killing or injury in combat, and combat action ribbons; driver's license, restricted license, and base driving privileges; clubs and spiritual affiliations; fitness test scores and health promotion courses.

General Education Development (GED), vocational training, college level, degrees, and certifications, military career qualifications, military career progression, and military career administration status; factors affecting personal finance status, wage garnishments, past-due bills, bankruptcy collection agency action, and gambling debt or issues; Force Preservation Risk and Resiliency Level; Individual Service Member Risk, Resiliency and Critical Stressor life events to include: high-risk hobbies, exposure to suicide, non-suicidal self-injury, witness/victim

exposure to crime or violence, hazing, sexual harassment, sexual assault, violence, child abuse, domestic abuse, neglect, behavioral and mental health information, traumatic brain injury, accidental death, alleged offender of crime or violence; Comments by commanders and command leadership Force Preservation Council members; alcohol/drug treatment, inpatient/outpatient, inpatient location, alcohol screening and use/misuse, drug screening and use/misuse, drug or alcohol related incident(s), history of substance abuse, duty-limiting diagnosis, under care for chronic treatment, prescription drugs (duty restricting), history of substance abuse, pending medical board decision, psychotropic or narcotic drugs prescribed, hospitalization, and critical illness/injury.

RECORD SOURCE CATEGORIES: Records and information stored in this system of records are obtained from: Service Individuals, Service Member's first-line leader, command staff, commanding officer, small unit leaders, medical officers, other support staff, and their assigned Force Preservation Council Members as well as authoritative data from Marine Corps Total Force System (MCTFS). Future iterations of the system may also include information from Department of Defense Tricare Pharmacy Tracking, Defense Enrollment Eligibility Reporting System, Marine Corps Recruiting Information Support System, Armed Forces Health Longitudinal Technology Application/GENESIS, and Manpower and Reserve Affairs Marine and Family Programs.

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING

CATEGORIES OF USERS AND THE 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 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 that 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 that 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.

i. To such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty.

POLICIES AND PRACTICES FOR STORAGE OF RECORDS: Records in this system are stored in electronic format in accordance with the safeguards mentioned below.

POLICIES AND PRACTICES FOR RETRIEVAL OF RECORDS: Records may be retrieved by name or EDIPI/DoD ID number.

POLICIES AND PRACTICES FOR RETENTION AND DISPOSAL OF RECORDS:

Records are permanent and maintained by USMC for 25 years, then transferred to the National Archives and Records Administration.

ADMINISTRATIVE, PHYSICAL, AND TECHNICAL SAFEGUARDS: Access is limited to authorized personnel with a need to know to perform their official assigned responsibilities.

Users are granted only those privileges that are necessary for their job requirements. Access is controlled through use of Common Access Cards, DoD Public Key Infrastructure certificates, user identification and passwords, firewall, and role-based access controls. Personally

Identifiable Information (PII) and Health Insurance Portability and Accountability Act (HIPAA) training is required for all users. Physical access to AWS data centers is logged and monitored.

The physical access points to server rooms are monitored using Closed Circuit Television

Camera (CCTV). Physical access is controlled at building ingress points by professional security staff utilizing surveillance, detection systems, and other electronic means. Authorized staff

utilize multi-factor authentication mechanisms to access and exit data centers and server rooms.

Entrances to server rooms are secured with devices that sound alarms to initiate an incident

response if the door is forced or held open. Electronic intrusion detection systems are installed

within the data layer to monitor, detect, and automatically alert appropriate personnel of security

incidents. Data at Rest Encryption and Risk Management Framework security controls, which include security controls for the PII and Protected Health Information (PHI) overlays, are utilized.

RECORDS ACCESS PROCEDURES: Individuals seeking access to information about themselves contained in this system of records should address written requests to the commanding officer where assigned or to the system manager at Headquarters Marine Corps, Manpower & Reserve Affairs (M&RA), Marine & Family Programs (MF) Division, 3280 Russell Rd, Quantico, VA 22134-5143, 4th Deck. Signed, written requests should include the individual's full name, EDIPI/DoD ID number, telephone number, street address, email address, and name and number of this System of Records Notice (SORN). In addition, the requestor must provide either a notarized statement or a declaration made in accordance with 28 U.S.C. 1746, in the appropriate 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 if information about themselves is contained in this system should address written requests to the commanding officer where assigned or to the system manager at Headquarters Marine Corps, Manpower & Reserve Affairs (M&RA), Marine & Family Programs (MF) Division, 3280 Russell Rd, Quantico, VA 22134-5143, 4th Deck. Signed written requests should include the individual's full name,

telephone number, street address, email address, and name and number of this SORN. In addition, the requestor must provide either a notarized statement or a declaration made in accordance with 28 U.S.C. 1746, using 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: None.

[FR Doc. 2021-03453 Filed: 2/19/2021 8:45 am; Publication Date: 2/22/2021]