PRIVACY IMPACT ASSESSMENT (PIA)

For the

CRRD INC I - COMMANDERS RISK REDUCTION DASHBOARD

HQDA G1 Deputy Under Secretary of the Army (DUSA)

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: 16539 DA300406
- ☐ **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

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 A0600-63 DAPE G-1

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://dpcld.defense.gov/Privacy/SORNs.aspx

or

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

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. 136, Under Secretary of Defense for Personnel and Readiness;
10 U.S.C. 3013, Secretary of the Army;
10 U.S.C. 3013, Secretary of the Army; DoD Instruction 6490.2E, Comprehensive Health Surveillance;
10 U.S.C. Chapter 55, Medical and Dental Care;
29 C.F.R. Part 1960, Occupational Illness/Injury Reporting Guidelines for Federal Agencies;
42 U.S.C. 290dd-2, Substance Abuse and Mental Health Services;
45 C.F.R. Parts 160 and 164, Health Insurance Portability and Accountability Act, General Administrative Requirements and Privacy and Security Rules;
DoD Instruction 1300.18, Personnel Casualty Matters, Policies, and Procedures; Army Regulation 40-66, Medical Record Administration and Health Care Documentation;
DoD Instruction 6015.23, Delivery of Healthcare at Military Treatment Facilities (MTFs);
DoDD 6490.02, Comprehensive Health Surveillance; AR 600-63, Army Health Promotion, Rapid Action Revision 20 Sep 09, Paragraph 4-4 Suicide Prevention and Surveillance;
OPNAV Instruction 1720.4A, Suicide Prevention Program, 5.d, Reporting;
AFI 44-154, Suicide and Violence Prevention Education and Training;
AFPAM 44-160, The Air Force Suicide Prevention Program, XI, Epidemiological Database and Surveillance System;
Army Regulation 195-2, Criminal Investigation Activities;
Army Regulation 600-85, Army Substance Abuse Program;
Army Regulation 600-8-104, Military Personnel Information Management/Records;

Army Regulation 608-18, The Family Advocacy Program;
E.O. 9397 (SSN), as amended.

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.

The purpose of CRRD is to provide Commanders the ability to detect, measure and track unit-level risk behavior and to identify Soldiers who are high risk in order to engage in prevention and intervention activities.

CRRD data is stored in the Person-Event Data Environment (PDE) within the Army Data Center Fairfield Enclave at the Army Analytics Group (AAG). Data in PDE is maintained, transformed, and used in accord with all applicable laws, regulations, and Department of Defense and Department of Army policies for the security of individually-identifiable data. All users/teams using non-PII data derived from PDE must agree that such information will be secured as required by law, regulation, and Army policy.

CRRD collects individual Soldier data associated with the following risk factors:
• Accidents/Injuries
• Alcohol offenses
• Drug offenses
• Crimes against property
• Crimes against persons
• Crimes against society
• Domestic violence
• Child abuse
• Screened at the Alcohol Substance Abuse Program (ASAP)
• Illicit drug positive tests
• Enrolled in the ASAP
• Readiness Limiting Behavioral Health Profiles

Specific data elements to be collected for the above risk factors is detailed in Data Use Agreements (DUA) duly executed with the data source systems.

Data indicating the Unit Identification Code (UIC) to which Soldiers are assigned, and data indicating the UIC for which a Commander maintains command authority is also collected.

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

CRRD collects, computer links and transforms personally identifiable information (PII). SSN is transformed into a PDE-unique identifier so that SSNs are not stored in the application database, only on the secure server that receives the data from the data owners.

The data risks are addressed by restricted areas accessible only to authorized personnel with documented security clearances. Physical access is controlled by dual access controls, alarm system, surveillance system, properly cleared and trained personnel with approved need-to-know, and computer hardware and software security features. Records are restricted to designated personnel and protected by a layered architecture and data encryption. Protection is commensurate with the sensitivity level of the data.

CRRD displays a soldier's first name, last name, and last four of the SSN on the screen to authorized commanders. Authorized commanders access the CRRD application with a CAC card that is cross referenced with DEERS and an internal SharePoint list to limit the commander's access to a list of soldiers within his/her command.

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. All DoD components (military, civilian, and contractors) which include but are not limited to the Army and reserve and National Guard personnel major commands and components, as well as administrative support.

☒ **Other DoD Components.**

Specify. As Requested;
Defense Criminal Investigative Service, Defense Integrated Military Human Resources System, Defense Manpower Data Center, Defense Security Service, Department of Veterans Affairs, DoD Inspector General, National Guard Bureau, Office of the DoD Inspector General, Office of the Secretary of Defense, Office of the Secretary of Defense Personnel and Readiness.

☐ **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.

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

The individual does not have the ability to object at CRRD since this system doesn't collect the initial data directly. The individual would have to opt out at the source system for their PII data not to be collected by CRRD.

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.

The individual does not control the specific uses of the PII data once collected into the CRRD system. All data within CRRD is captured in other systems of record

(2) If "No," state the reason why individuals cannot give or withhold their consent.

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.

CRRD does not directly collect PII information from individual users.