PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

MIRARS-PEO CS&CSS - MANPOWER INFORMATION REPORTING AND RETRIEVAL SYSTEM-

2. DOD COMPONENT NAME:

United States Army

3. PIA APPROVAL DATE:

09/09/20

Program Executive Office Combat Support & Combat Service Support (PEO CS&CSS)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: foreign nationals are included in general public.)*

- [ ] From members of the general public
- [x] From Federal employees and/or Federal contractors
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [ ] Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one)*

- [ ] New DoD Information System
- [ ] New Electronic Collection
- [ ] Existing DoD Information System
- [x] Existing Electronic Collection
- [ ] Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

Manpower Information Retrieval and Reporting System (MIRARS) PEO CS&CSS is an Embedded Technology Component (child application) of TCAN - Team C4ISR Acquisition Network, APMS AITR# DA65056 and RMF ID# 889.

MIRARS PEO CS&CSS PIA is submitted to document the specific PII collected as the MIRARS Base subcomponent discussed in the below paragraph

MIRARS is a fast, modern, mobile-ready Personnel Accountability web application that provides Leadership with the ability to quickly locate and account for their Personnel with full visibility into the current locations of its workforce and with a two-way communication capability via email, phone calls, and/or text messaging. A self-service web interface provides the workforce the ability to keep their location information current via a daily roll call process. In short, MIRARS combines location information with contact information allowing Leadership to quickly account for their personnel in a location and have two-way communications with them. MIRARS contains the location of employees/contractors/military personnel on duty location for emergency notification purposes and home and contact information. MIRARS can also provide emergency notification and two-way communication to personnel on non-duty status if the employee chooses to provide this optional information.

MIRARS Base collects PII related to military, personal, employment and work related information. Product Lead Military Technical Solutions is the network provider with overall responsibility for establishing and maintaining certification and accreditation security controls for the MIRARS Base application. The MIRARS Base application hosts various data collections from multiple data owners using MIRARS and each Command or Command Component will submit a separate PIA for their specific PII collection requirements.

MIRARS, as a role-based application, limits access to PII data to specific users within each organization with the need-to-know. There is no cross-organizational sharing of PII data.

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The PII is collected to sustain the mission. Accounting for personnel in emergency situations allows the Command to effectively report readiness and personnel status up the chain of command.

e. Do individuals have the opportunity to object to the collection of their PII? [x] Yes [ ] No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

Command Leadership can leverage MIRARS to support their requirement to account for and communicate with their workforce when disasters and/or emergency situations arise. Individuals that object to the collection of their PII will not enter it into the system. As a result, these individuals will not receive notifications based on their work location outside of their normal duty station.

f. 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.

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

The individuals' information is only being used for the communication process with the workforce when disasters and/or emergency situations arise, and therefore no other uses apply.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. *(Check as appropriate and provide the actual wording.)*

☒ Privacy Act Statement ☐ Privacy Advisory ☐ Not Applicable

AUTHORITY: 10 U.S.C. 3013, Secretary of the Army and Department of Defense Directive 3020.23, The Defense Continuity Program.

PURPOSE: To document personnel location information, contact information and names and phone numbers of persons to be notified in emergency situations.

ROUTINE USE:
Law Enforcement (Investigations): To the appropriate federal, state, local, territorial, tribal, or 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.

Department of Justice for Litigation: A record from a system of records maintained by a DoD Component may be disclosed as a routine use to any component of the Department of Justice for the purpose of representing the Department of Defense, or any officer, employee or member of the Department in pending or potential litigation to which the record is pertinent.

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.

Breach Mitigation and Notification: A record from a system of records maintained by a Component may be disclosed to appropriate agencies, entities, and persons when (1) The Component suspects or has confirmed that the security or confidentiality of the information in the system of records has been compromised; (2) the Component has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by the Component or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with the Components efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm.

Breach Mitigation and Notification: To another Federal agency or Federal entity, when the Department of Defense (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.

DISCLOSURE: Voluntary. Failure to supply this information may result in not being notified of a potential emergency to include acts of nature, accidents and technological and/or attack related emergencies. While disclosure of personal contact information is voluntary, providing work related information and participating in the daily Roll Call process to provide on-duty location is mandatory.

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? *(Check all that apply)*

☒ Within the DoD Component	Specify.	Command component G1 Offices, G3/5 and individuals' own HR/Admin Office, supervisors and command
☐ Other DoD Components	Specify.	
☐ Other Federal Agencies	Specify.	
☐ State and Local Agencies	Specify.	

[X]	Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)*	Specify.	Data Systems Analysts, Inc. (DSA) - The Contractor System Administrators will be required to design, develop, or operate a system of records on individuals, to accomplish an agency function subject to the Privacy Act of 1974, Public Law 93-579, December 31, 1974 (5 U.S.C. 552a) and applicable agency regulations. Violation of the Act may involve the imposition of criminal penalties.
[X]	Other *(e.g., commercial providers, colleges)*.	Specify.	MIRARS has an instant alert capability designed to provide instant communication across various geographic locations. The Twilio service provides this functionality. Twilio Inc. - A commercially provided product, the Twilio Messaging product is a service that provides instant communication across various geographical locations.

i. Source of the PII collected is: *(Check all that apply and list all information systems if applicable)*

- [X] Individuals
- [X] Existing DoD Information Systems
- [ ] Other Federal Information Systems
- [ ] Databases
- [ ] Commercial Systems

Essential employee data will be entered by organizational system administrators. Employees will be asked to complete the data collection themselves. Essential contractor information will be collected from each individual organization, and those workers would be asked to complete data in the system as well. Some users are able to self register in the system and information provided by DEERS is pulled directly from the CAC.

j. How will the information be collected? *(Check all that apply and list all Official Form Numbers if applicable)*

- [ ] E-mail
- [ ] Face-to-Face Contact
- [ ] Fax
- [ ] Information Sharing - System to System
- [ ] Other *(If Other, enter the information in the box below)*
- [ ] Official Form (*Enter Form Number(s) in the box below)*
- [ ] Paper
- [ ] Telephone Interview
- [X] Website/E-Form

k. 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 must be consistent.

[X] Yes [ ] No

If "Yes," enter SORN System Identifier A0500-3c G3/5/7, for Department of the A

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/

or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority. DAA-GRS-2016-0004-00

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

The transfer and/or separation process is considered concluded 14 days after personnel are made not active in the system and PII is removed at that time.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

AUTHORITY: 10 U.S.C. 3013, Secretary of the Army and Department of Defense Directive 3020.23, The Defense Continuity Program.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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 ☒ No ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

No data is being collected from the members of the general public.