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:

Command and Control Incident Management Emergency Response Application (C2IMERA)

2. DOD COMPONENT NAME:

United States Air Force

3. PIA APPROVAL DATE:

05/15/20

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
- [x] Existing DoD Information System
- [ ] 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.

C2IMERA is an IL-5 National Security System providing a standardized enterprise C2 capability through a vertically and horizontally interoperable system supporting the full range of military operations, to include disaster/emergency response and combat operations. The primary purpose of C2IMERA is to conduct Command and Control, allowing Commander's to issue directives, plan and coordinate operations, conduct and track personnel recalls, accountability and status, and rapidly communicate to C2 personnel through a live-fed Common Operating Picture (COP). The software has been secured according to the Risk Management Framework (RMF) within NIST.

Types of PII: Required - Name, managing unit, and duty status (dead, injured, missing, isolated, quarantined, isolated, hospitalized, recovered), Service Branch, Building Number, Flight, Job Type, Address, Office Symbol, leave, PCS Date, EDIPI, Personnel Type (Mil/ Civ), Rank, Remarks, personal Contact Phone Number and email address

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 use of the PII is for personnel accounting during disaster/emergency and incident response, used to improve the process of identifying, validating, and accounting for personnel and their current status in an integrated multi-echelon C2 tool.

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.

Requested information is required to ensure commanders maintain 100% accountability of personnel assigned. Individuals who fail to provide required information will hinder commanders from maintaining 100% accountability. Data is pulled from external source systems. Objection to collection of PII is handled by the external source systems.

f. Do individuals have the opportunity to consent to the specific uses of their PII? [x] 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.

Requested information is required to ensure commanders maintain 100% accountability of personnel assigned. Individuals who fail to provide required information will hinder commanders from maintaining 100% accountability. Data is pulled from external source systems. Collection of PII is handled by the external source systems.

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., Armed Forces, DoD Directive 5124.02, USD Personnel and Readiness, DoD Instruction 3001.02, Personnel Accountability in Conjunction With Natural or Manmade Disasters, AF Policy Directive 13-1, Command and Control Enterprise (C2 Enterprise); AF Instruction (AFI) 36-3802, Personnel Readiness Operations

Purpose: C2IMERA collects PII to track and report recalls, accountability and personnel status via electronic means, providing Wing and MAJCOM Commander's and staff's critical data that is housed in a collaborative C2 tool and common operating picture. C2IMERA works synergistically with, and fills gaps in, systems like Personnel Accountability and Assessment System and Enterprise Mass Warning and Notification Systems (ref: At Hoc). Critical reporting updates can be provided to and by C2 nodes and first responders anywhere, at anytime through mobile devices, significantly reducing the data-to-decision and emergency response timelines.

Routine Use: 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 a domestic or foreign entity that has entered into a public-private partnership with the Defense POW/MIA Accounting Agency (DPAA) as authorized by 10 U.S.C. 1501a, when DPAA determines that such disclosure is necessary to the performance of services DPAA has agreed shall be performed by the partner.
b. 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.
c. To appropriate Federal, State, local, territorial, tribal, foreign, or international agencies for the purpose of counterintelligence activities authorized by U.S. law or Executive Order, or for the purpose of executing or enforcing laws designed to protect the national security or homeland security of the United States, including those relating to the sharing of records or information concerning terrorism, homeland security, or law enforcement.
d. 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.
e. 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.
f. 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.
g. 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.
h. 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.
i. To appropriate agencies, entities, and persons when (1) The Department of Defense (DoD) suspects or has confirmed that the security or confidentiality of the information in the system of records; (2) the DoD has determined that 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.
j. 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.

Voluntary/Involuntary: Voluntary. However, individuals who fail to provide required information will hinder commanders from maintaining 100% accountability

SORN Identifier/Name: DPR 39 DOD SORN

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.	Unit, installation, and MAJCOM Manager's, Commander's and Director's
☒ Other DoD Components	Specify.	US Army, US Navy, Coast Guard
☐ Other Federal Agencies	Specify.	

☐ State and Local Agencies — Specify.

☐ 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.

☐ Other *(e.g., commercial providers, colleges).* — Specify.

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

☒ Individuals
☒ Existing DoD Information Systems
☐ Other Federal Information Systems
☒ Databases
☐ Commercial Systems

C2IMERA will predominantly import PII from the Military Personnel Data System (MilPDS) and Defense Civilian Personnel Data System (DCPDS), some data may be captured or input by authorized unit personnel (Commander, First Sergeant, Superintendent, or other approved authority). This also ensures data is removed from the system upon moving or separation.

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
☐ Website/E-Form

C2IMERA will predominantly import PII from the Military Personnel Data System (MilPDS) and Defense Civilian Personnel Data System (DCPDS), some data may be captured or input by authorized unit personnel (Commander, First Sergeant, Superintendent, or other approved authority). This also ensures data is removed from the system upon moving or separation.

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.

☒ Yes ☐ No

If "Yes," enter SORN System Identifier: DPR 39 DOD SORN

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-2016-0004-0002

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

(3) Retention Instructions.

Records are deleted from the C2IMERA application upon permanent change of station to a location where the system is not in use, separation from military or civil service, or when no longer required based on routine updates. Records are routinely checked by the unit manager at each base/location. Personnel information is added, deleted or modified as appropriate by the base appointed C2IMERA system administrator.

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.

10 U.S.C. , Armed Forces, DoD Directive 5124.02, USD Personnel and Readiness, DoD Instruction 3001.02, Personnel Accountability in Conjunction With Natural or Manmade Disasters, AF Policy Directive 13-1, Command and Control Enterprise (C2 Enterprise); AF Instruction (AFI) 36-3802, Personnel Readiness Operations

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.

Information is not being collected from individuals of the general public.

NOTE: Sections 1 above is to be posted to the Component's Web site. Posting of these Sections indicates that the PIA has been reviewed to ensure that appropriate safeguards are in place to protect privacy. A Component may restrict the publication of Sections 1 if they contain information that would reveal sensitive information or raise security concerns.