PRIVACY IMPACT ASSESSMENT (PIA)

For the

CAC PIN RESET - WORKSTATION SERVICE (CPR-WS)
Department of the Navy - BUPERS

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: DADMS ID: 83488
- ☐ **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: DMDC 02 (Defense Enrollment Eligibility Reporting System)

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://www.defenselink.mil/privacy/notices/

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.

SORN DMDC 02 authorities:

5 U.S.C. App. 3, Inspector General Act of 1978; 5 U.S.C. Chapter 90, Federal Long-Term Care Insurance; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 53, Miscellaneous Rights and Benefits; 10 U.S.C. Chapter 54, Commissary and Exchange Benefits; 10 U.S.C. Chapter 55 Medical and Dental Care; 10 U.S.C. Chapter 58, Benefits and Services for Members being Separated or Recently Separated; 10 U.S.C. Chapter 75, Deceased Personnel; 10 U.S.C. 2358, Research and Development Projects; 20 U.S.C. 1070a (f)(4), Higher Education Opportunity Act; 31 U.S. C. 3512(c), Executive Agency Accounting and Other Financial Management; 42 U.S.C. 18001 note, Patient Protection and Affordable Care Act (Public Law 111-148); 42 U.S.C. 1973ff, Federal Responsibilities; 50 U.S.C. Chapter 23, Internal Security; DoD Directive 1000.04, Federal Voting Assistance Program (FVAP); DoD Instruction 1100.13, Surveys of DoD Personnel; DoD Instruction 1341.2, DEERS Procedures; DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural or Manmade Disasters; Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors; 38 CFR part 9.20, Traumatic injury protection; 38 U.S.C. Chapter 19, Subchapter III, Service members' Group Life Insurance; 42 U.S.C. 18001 note, Patient Protection and Affordable Care Act (Public Law 111-148); and 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 Common Access Card (CAC) is a "smart" card that is the standard identification for active duty uniformed service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel. It is also the principal card used to enable physical access to buildings and controlled spaces, and it provides access to DoD computer networks and systems

The Defense Enrollment Eligibility Reporting System (DEERS) is a Department of Defense system/ database of United States Service members, retirees, dependents, federal employees, DoD active Contractors, and others, worldwide, who are entitled to a DoD identification card, Public Key Infrastructure (PKI), and other eligibilities.

The Real-Time Automated Personnel Identification System (RAPIDS), also a Department of Defense system, is used in conjunction with DEERS to verify the eligibility for, and to issue the CAC. Used together, these two systems are commonly referred to as a DEERS/RAPIDS system or DEERS/RAPIDS infrastructure. The DEERS/RAPIDS is hosted by the Defense Manpower Data Center (DMDC).

RAPIDS issuing stations (clients) are available in over 700 locations worldwide. RAPIDS ensures that DoD identification credentials are provided only to personnel with a current and appropriate affiliation with the DoD. RAPIDS captures identifying characteristics that are unique and are used to bind an individual to the information maintained in DEERS and in line with the identifying credentials issued by RAPIDS. These include, but are not limited to: Photographs and Fingerprints. The information is stored solely in the DEERS System.

The Common Access Card (CAC) requires a PIN number. The RAPIDS stations allow users the capability to reset the CAC PIN when necessary. But, in many cases, access to a RAPIDS issuing station is not available or is inconvenient.

The CAC PIN Reset (CPR) system was developed by the DMDC to work with the DEERS/RAPIDS to provide a means for a Common Access Card (CAC) holder to reset the CAC PIN. The CPR resets the PIN by using a biometric match on the DEERS server.

The CAC PIN Reset - Work Station (CPR-WS) is a client portion of the CPR system that provides the capability to reset the CAC PIN without having to go to a RAPIDS issuance site. The CPR system is hosted on DMDC servers and the CPR-WS is installed on remote workstations at multiple sites.

The CPR-WS has an operator that verifies the identity of the PIN reset requestor via the CAC and the picture on the CAC before starting the CPR-WS process. CPR-WS collects the DoD ID number data via a card reader and biometric data via a fingerprint reader. The CPR-WS process connects to the CPR portal, The fingerprints and the DOD ID number are transmitted from the CPR-WS to the CPR system. The transmitted data is encrypted via FIPS 140-2 compliant technologies. The CPR system uses the DEERS/ RAPIDS to identify and authenticate both the operator and the CAC holder via their submitted Dod ID number and their fingerprints. Once verified by the DEERS/RAPIDS, the system returns a picture of the CAC holder/requestor to the CPR-WS for further authentication. If the CPR-WS operator verifies the picture, the PIN reset request is processed. When the process is successfully completed, the new PIN is transmitted back to the CPR-WS computer and recorded on the CAC. The CPR-WS does not store any Personally Identifiable Information (PII).

PII collected: Name, DoD ID number, fingerprints.

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

The CPR-WS does not store any PII. It transmits DoD ID numbers and fingerprints of the operator and the PIN reset requester. The transmitted data is encrypted via FIPS 140-2 compliant technologies.

The DoD ID number transmitted via CPR-WS is only one factor in a multi-factor authentication process. Knowledge of the DoD ID number alone does not grant access to records unless accompanied by another factor such as a pin number or biometric data. The transmission by CPR-WS of the operator and requester fingerprints cannot be easily duplicated, and the DoD ID number is of no use to an attacker without it.

The loss or disclosure of the DoD ID number is considered low risk in conjunction with identity theft or fraud. The CPR-WS does not share the DoD ID number with organizations, agencies or corporations outside of DoD.

The DoD ID number, by itself or with an associated name, is considered internal government operations-related PII. Since the loss, theft or compromise of the DoD ID number is low risk for possible identity theft or fraud, a PII breach report is not required unless accompanied by other PII elements, such as date of birth, birthplace or mother's maiden name, which would normally require a report to be submitted. The CPR-WS does not transmit anything other than DoD ID numbers and fingerprints.

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. The PII will be available to the CPR-WS operator. The CPR-WS operator acts as the first line of authentication. The CPR-WS process cannot work without the operator.

☒ **Other DoD Components.**

Specify. The PII will be shared with the DMDC CPR and DEERS/RAPIDS. The process is used to authenticate the operator and requestor by matching data collected by the CPR-WS to the data already stored in the DEERS/RAPIDS.

☐ **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.

Yes, they can decline to use the CPR-WS system

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

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.

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

Once their information is provided to reset their pin they have consented.

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.	The CPR-WS operator explains that the DoD ID number and the fingerprint are transmitted to DEERS/RAPIDS for authentication.

NOTE:

Sections 1 and 2 above are 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 and/or 2 if they contain information that would reveal sensitive information or raise security concerns.