PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy-Marine Corps Mobilization Processing System (NMCMPS)
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: DITPR ID: 809 DITPR-DON ID: 20830
- ☐ **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 UII: 007-000000371

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 N01070-13

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 N01070-13 authorities:

5 U.S.C. 301, Departmental Regulations
10 U.S.C. 5013, Secretary of the Navy
OPNAVINST 3060.7B, Navy Manpower Mobilization/Demobilization Guide (Appendix D)
OPNAVINST 1001.24, Individual Augmentation (IA) Policy and Procedures
DoD 6025.18-R, DoD Health Information Privacy Regulation
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.

NMCMPS provides peacetime and wartime manpower and personnel mission-critical web-based system for Navy augmentation execution, coordination and management. This system is used for non-routine, emergent requirements, and its function is critical to the direct fulfillment of military missions and task forces.

NMCMPS provides end-to-end command visibility and control of integrated augmentation processes and automated work-flow. This includes: initial operational planning, requesting of manpower requirements, approving and sourcing of requirements, centralized distribution and order writing, tracking and accountability, data collection, and coordination during activation and recall processing of the people temporarily assigned to the critical wartime billets at intermediate bases. The scope also includes the mobilization and demobilization of reservists and the temporary reassignment of active duty personnel for emergent manpower requirements. It allows administrative, operational and ad-hoc task force based chain-of-command duty stations direct access via the web to monitor from start to finish the status of their manpower requests and personnel augmenting to their command.

Collection of data is used to support the above mentioned initiative. NMCMPS on the low-side processes unclassified data, which contains Privacy Act and Health Insurance Portability and Accountability Act (HIPAA) information.

PII collected: Name, SSN (full and truncated), DoD ID, citizenship, legal status, gender, race/ethnicity, birth date, place of birth, personal cell telephone number, home telephone number, personal email address, mailing/home address, marital status, religious preference, security clearance, medical information: Last physical date, on medical hold and if so reason code, on dental hold and if so reason code, DNAFlag, glasses, earplugs, hearing aids, medical and dental appointment dates, TRICARE eligible, and blood type; military records: a member's personnel record, order information, command address, phone numbers, rate/ rank, race, dependant ID, legal hold/assistance/or brief, legal activity, training and completion date, and dependants (name, age, birth date, and number of dependents); emergency contact.

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

Privacy risk is unauthorized personnel viewing or gaining PII. Safeguards in place to protect PII include the following:

1) Security Guards, Identification Badge,s and Electronic Key Cards access to building where system server infrastructure is located.
2) ID Badge, Electronic Key Cards, Security Guards, and Closed Circuit TV (in most cases) are implemented in buildings were personnel who utilize the applications on CCES have their work spaces.
3) Administrators and users have User Accounts to log into the appropriate applications they have authorized access to. Additionally, users are logged into their NMCI with their CAC.
4) DoD PII annual training is required for all Administrators of the servers and NMCI users.

Privacy Risks could include access to individual's pay data, personal identifying information such as SSN and name, place of deployment, age, home of record, etc. Currently only NMCMPS support personnel and system administrators have access to information that can identify individuals. System administrators and support personnel are bound by non-disclosure and privacy statements, are subject to DoD, and DoN, and N1's privacy policies, and are required to have no less than "SECRET" level clearance. Data is stored in a DADMS approved system operating on a fully accredited (DIACAP) Navy (SPAWAR) facility. Two levels of security are required before someone can gain access to NMCMPS. Users must have a valid PKI certification (CAC) to login and must be authorized for specific NMCMPS areas. NMCMPS also imposes authorization expiration to assist in assuring only appropriate personnel have access to the data. PII data is

masked in the system by associating SSN with an encrypted representation.

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. OPNAV, U.S. Fleet Forces Command (USFFC), Navy Personnel Command (NPC)

☐ **Other DoD Components.**

Specify.

☐ **Other Federal Agencies.**

Specify.

☐ **State and Local Agencies.**

Specify.

☒ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify. All contracts contain the required FAR privacy clauses regarding the protection of PII.

☐ **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.

PII data in use is derived from inheritable systems that maintain the systems of records for individual's information within the Navy.

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.

PII data in use is derived from inheritable systems that maintain the systems of records for individual's information within the Navy.

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.

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.