**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:

Navy Physical Access Control System (NPACS)

### 2. DOD COMPONENT NAME:

Department of the Navy

### 3. PIA APPROVAL DATE:

03/11/21

Commander, Navy Installations Command (CNIC)

### 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
- [ ] From both members of the general public and Federal employees and/or Federal contractors
- [x] From 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
- [ ] Existing DoD Information System
- [x] 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.

The requirement for NPACS is to provide automated entrance into a naval installation based on two factor authentication leveraging existing authoritative identification sources such as CAC and Telsin cards. The NPACS system collects this information from these cards through proximity sensors and/or barcode.

Personal Information collected: Name, DoD ID nbr, FACS-N, photo, other ID, date of birth, work phone nbr, rank/grade, biometrics, citizenship, drivers license, home/cell phone, mailing/home address, passport information, place of birth, work email.

#### 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)

Authentication and identification. The purpose of this electronic collection is to authorize Department of the Navy civilian, military, and contractor personnel entrance onto the naval installation. NPACS compares CAC and Telsin holder PII information on Federal personnel and Federal contractors from the authoritative data source Defense Enrollment Eligibility Report System (DEERS) database and the Department of Navy Total Workforce Management System (TWMS) via Socket Layer (SSL) as defined in the Enabler System Security Authorization Agreement (SSAA). This provides NACS with the ability to interactively check for authentication, permissions and privileges before any benefit, service or privilege is provided.

#### 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.

Individuals have the opportunity to object to the collection of their PII by following the procedures outlined in the System of Record Notice (SORN) NM05512-2 and by refusing to provide the requested PII information as disclosure is voluntary; however, failure to provide the information may result in refusal to grant access to DoD installations.

#### f. Do individuals have the opportunity to consent to the specific uses of their PII?

- [ ] Yes
- [x] 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.

If an individual provides their PII, consent is assumed.

#### 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.)
No information is provided to the user when requesting PII data. The PII data is resident on the CAC and Teslin card. This information is pulled and verified against the DOD DMDC database for authentication and to allow authorization to enter the Navy base. The system receiving data is fully automated and reads the DOD CAC through the contact-less chip on the CAC as well as bar code on the back of the CAC as a backup or for those individuals that hold Teslin dependent, retired or other federal cards that are able to be authenticated by the DOD DMDC database.

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

- [X] Within the DoD Component
- [X] Other DoD Components
- [X] Other Federal Agencies
- [ ] State and Local Agencies
- [ ] 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.)
- [ ] Other (e.g., commercial providers, colleges).

Specify:
- USN, USMC base access/security personnel
- USAF, USA, CG, PFPA base access/security personnel
- DLA base access/security personnel
- [ ]
- [ ]
- [ ]

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

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

The PII data is resident on the CAC and Teslin card presented at base access points by the individual.

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

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

The PII data is resident on the CAC and Teslin card presented at base access points by the individual. This information is pulled and verified against the DOD DMDC database for authentication and to allow authorization to enter the Navy base. The system receiving data is fully automated and reads the DOD CAC through the contact-less chip on the CAC as well as bar code on the back of the CAC as a backup or for those individuals that hold Teslin dependent, retired or other federal cards that are able to be authenticated by the DOD DMDC database.

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. PII and Privacy Act SORN information must be consistent.

- [X] Yes
- [ ] No

If “Yes,” enter SORN System Identifier: **NM05512-2**

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

I. 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?
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 statute 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.

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.

OMB Control Number, 0703-0061, OMB Control Number 0703-0061, Navy Access Control Management System and USMC Biometric and Automated Access System. The 30 Day Notice was published in the Federal Registry on 1 March 2021 and ends on 31 March 2021. After the closing date, OMB has 30 days to issue the new expiration date.