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:

2. DOD COMPONENT NAME: Department of the Navy

3. PIA APPROVAL DATE: 01/13/21

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
   - 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
   - Significantly Modified DoD Information System

   New Electronic Collection
   - Existing Electronic Collection

   The purpose of this DoD Information System is to provide an integrated access control and security management solution for the NAS Jacksonville Security Department. The information that is captured will validate legitimate access requirements.

   Personal information collected: Name, Social Security Number, Driver's License Number, Citizenship, Gender, Birth Date, Place of Birth, Personal Cell Telephone Number, Home Telephone Number, Mailing/Home Address, Biometrics, Employment Information.

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)
   - Verification, identification and authentication

   e. Do individuals have the opportunity to object to the collection of their PII? 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.

      But objection would prevent the granting of access.

   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.

      Providing PII is considered consent.

   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 ☐
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
- Other DoD Components
- 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).

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

N/A

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)

N/A

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: NM05512-2

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

1. NARA Job Number or General Records Schedule Authority. See below

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

3. Retention Instructions.

These are TEMPORARY Records. 5530.3a PHYSICAL SECURITY RECORDS. Destroy 5 years after entry or 5 years after date of document, whichever is later. DAA-NU-2015-0005-0064 1630.5 NAVY BASE SECURITY. Retain on board. Destroy after 3 years after final entry. 3512.6a IDENTIFICATION (CREDENTIALS, TAGS, PASSES, AND PERMITS) RECORDS. Destroy 5 years after final entry or 5 years after date of document, whichever is later. DAA-NU-2015-0005-0070

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 PI not collected or maintained in a system of records, the collection or maintenance of the PI 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 PI. (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 PI.
   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.

SORN NM05512-2, Badge and Access Control System Records (April 09, 2014, 79 FR 19593), authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
OPNAVINST 5530.14E, Navy Physical Security and Law Enforcement Program
E.O. 9397 (SSN), as amended.

Other Authorities:

CNRSE INST 5530.1A - Navy Region Southeast Installation Access Control
OPNAVINST 5530.14 (Series), Navy Physical Security and Law Enforcement
OPNAVINST 3440.17, Navy Installation Emergency Management Program
CNICINST 5530.1 (Series) Taxicab, Limousine and Shuttle Access on Navy Installations
DODINST 5200.08-R, Physical Security Program
SECNAVINST 5510.34, Foreign National Access
BUPERSINST 1750.10, Identification Cards for members of the Uniformed Services, their eligible family members, and other eligible personnel
OPNAVINST 11200.5D, Motor Vehicle Traffic Supervision
DODD 5200.8, Security of DOD Installations and Resources
FIPS PUB 201, Personal Identify Verification (PIV) of Federal Employees and Contractors
HSPD-12, Policy for a Common Identification Standard for Federal Employees and Contractors
UFC 4-022-1, Security Engineering: Entry Control
DODD 8190.3, Smart Card Technology Facilities/Access Control Points
Title 10 U.S.C. Section 1072(2), Definitions of Military
NTPP 3-07.2.1, Navy Tactics, Techniques, and Training, Antiterrorism/Force Protection.
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 8510.01, 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.

Note: A Public Information Collection Package has been submitted (December 2, 2020). This PIA will be updated to reflect the OMB control number upon issuance by OMB.