



PRIVACY IMPACT ASSESSMENT (PIA)

For the

AMAG HOMELAND SECURITY MANAGEMENT SOFTWARE ENTERPRISE
EDITION (AMAG HSMS ENT)

Department of the Navy - CNIC - NAS Jacksonville

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
- Existing DoD Information System
- Significantly Modified DoD Information System
- New Electronic Collection
- Existing Electronic Collection

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
- 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

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 Authorities:

10 U.S.C. 5013, Secretary of the Navy

10 U.S.C. 5041, Headquarters, Marine Corp

OPNAVINST 5530.14C, Navy Physical Security

Marine Corps Order P5530.14, Marine Corps Physical Security Program Manual

E.O. 9397 (SSN), as amended

Other Authorities:

CNRSE INST 5530.1 - 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, 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
NTTP 3-07.2.1, Navy Tactics, Techniques, and Training. Antiterrorism/Force Protection.

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 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 includes Name, Social Security Number, date of birth, driver's license, place of birth, citizenship, gender, personal cell phone, home phone, mailing/home address, biometrics, employment information.

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

The privacy risks associated with the PII collected are the unauthorized release of PII data. These risks are addressed by protecting the data collection resource with strong SSL encryption, programmatically restricting the system from releasing PII data through its interfaces, through strong SSL encryption with CAC of PII released to partner agencies under the routine use guidelines authorized in the Privacy Act SORN, through periodic Information Assurance certification of personnel with access to the PII, and through access control restricted by CAC to internal network personnel whose job functions require access to PII.

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.

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.

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.

Individuals can object by not providing the PII however, those individuals will not be allowed access onto the base since the PII is used to determine access eligibility.

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

N/A.

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.

N/A.

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

PII will be sent to federal, state and local law enforcement agencies to determine access eligibility. As stated previously, individuals have the option to not provide their PII however, they will not be permitted to access the base.

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.

Privacy Act Statement -
Authority: Privacy Act of 1974 (5 USC SECTION 552(A)(7)) 41 USC Section 423, SCFR Section 2635.602, AR 340-21 Title 10 and 37 USC.
Principal Purpose(s): To enable military security and/or law enforcement personnel to conduct Citizenship and Criminal Background investigations for civilians requesting access to DOD Facilities.
Routine Use(s): To authorize access to DOD Facilities. Information may be reported to federal, state and local law enforcement agencies with jurisdictional interest.
Disclosure: Voluntary. Failure to provide requested information will result in denial of access to DOD facilities.

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.