# PRIVACY IMPACT ASSESSMENT (PIA)

## For the

| Admin Management Information System (AMIS) |
| --- |
| Department of the Navy - CNIC |

## 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: 94932
- ☐ **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**: NM05512-1

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** | Package submitted to OPNAV DNS-15.(Pending) |
| **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 NM05512-1 authorities:

10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN).

Other authorities:

Per Status of Force Agreement with host Country Spain (SOFA); Agreement of Defense Cooperation (ADC) (Annex 8); DOD Directive 5530.3 "International Agreements"

NATO Status of Forces Agreement (SOFA). The SOFA of 19 June 1951 states that, "It is the duty of a force...to respect the law of the receiving State.

US-Spain Agreement of Defense Cooperation (ADC). The Agreement of 1 December 1988, Amended by Protocol of 10 April 2002 (NATO SOFA and ADC)

**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.

Shore Application: The Admin Management Information System (AMIS) is Government off the shelf (GOTS) application locally developed, customized for Naval Station Rota,Spain (NAVSTA Rota) for its specific requirements. It is a window environment with progress database backend. It contains various modules to support Security Housing and Admin department such as Pass & ID, Vehicle registration, Incident/Complaint Reports, Spanish Police/Court appearance, Firearms registration, Spanish traffic tickets, On-Base traffic tickets, Base-access passes and Base locator.

In order to comply with Host Nation regulations the US Security Department records and manages the information of all Members of the US Forces with regards to: passports, ID's, vehicles, spanish drivers licenses, firearms, spanish and On-base traffic tickets, base passes, incidents and complaints, spanish police/Court appearances.

AMIS does not collect information on Foreign Nationals.

Personal information collected: Name, SSN, Other ID Number, Gender, Race/Ethnicity, Birth Date, Place of Birth, Personal Cell Telephone Number, Home Telephone Number, Mailing/Home Address, Spouse Information, Marital Status, Child Information, Disability Information, Employment Information, Military Records, Emergency Contact Information, Education Information (details in Section 3).

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

The access, storage, and transmission of the PII collected by AMIS is subject to various privacy risks. The primary privacy risks to the PII collected by AMIS include: "insider threats" including intentional/unintentional compromise of privacy data by privileged users and application administrators; and physical compromise of the AMIS database.

To mitigate these risks, various layers of security controls have been implemented within AMIS to achieve a defense-in-depth security strategy. Technical and procedural access controls have been implemented to restrict access to the data processed/stored is AMIS to authorized users or processes acting on behalf of users. Auditing has been implemented to provide accountability of actions performed by general and privileged users of AMIS application.
AMIS is protected from network attacks via a series of boundary protection devices located at various layers of the DoN enterprise network on which AMIS resides.
Information System Security Managers (ISSMS) and Information Systems Security Officers (ISSOS) are vigilant to limiting insider threat by restricting system access to those individuals who have a defined "need to know".
Personnel may not access AMIS unless they have explicit approval by the command security manager, supervisor, information owner and ISSM.
Physical Security measures have been implemented to protect the servers hosting AMIS. AMIS database components are located in a secure military base, with strict personnel access controls.
Security training is provided on a continuous basis to keep users aware of their responsibilities with regard to protection of the AMIS application and the PII processed/stored within the application.

**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. CNIC ROTA Human Resource personnel.

☐ **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. Spanish Ministry of Defense (MOD)

**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.

Every individual who checks into NAVSTA ROTA must provide the requested information as it is required by NATO Status of Forces Agreement (SOFA). The SOFA of 19 June 1951 and US-Spain Agreement of Defense Cooperation (ADC). The Agreement of 1 December 1988, Amended by Protocol of 10 April 2002 (NATO SOFA and ADC), Local National employees working for the U.S. are employees of the Spanish Ministry of Defense (MOD). MOD must approve all actions affecting employees.

**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.

Every individual who checks into NAVSTA ROTA must provide the requested information as it is required by NATO Status of Forces Agreement (SOFA). The SOFA of 19 June 1951 and US-Spain Agreement of Defense Cooperation (ADC). The Agreement of 1 December 1988, Amended by Protocol of 10 April 2002 (NATO SOFA and ADC), Local National employees working for the U.S. are employees of the Spanish Ministry of Defense (MOD). MOD must approve all actions affecting employees.

**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 is provided on NAVEUR Forms 5512/1 and 5512/12. Form that collects on minors does not have a PAS. All three forms are being reviewed to ensure compliance with the DON Forms manual.

**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.**