PRIVACY IMPACT ASSESSMENT (PIA)

For the

Spanish Payroll Management System (SPMS)

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: 94359

☐ 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.

Spanish Fiscal Laws.
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 Spanish Payroll Management System (SPMS) application is used as the Spanish Local National payroll and accounting system. All data captured in the application pertains to CNIC Spanish direct hire employees. Access is limited to authorized users by the Comptroller, N8 Department.

PII collected: Name, Bank account for foreign national payrolls electronic bank transfers (EFTs), Law Enforcement Background Investigation "Certificado de Penales", DNI - Documento Nacional de Identidad, Driver's License, DoD ID Number, Citizenship, Legal Status, Gender, Race/Ethnicity, Birthdate, Personal Cell Phone Number, Home Phone Number, mailing/Home address, Spouse and Child Information: Name, Date of Birth (DOB), Address if needed; Martial Status, Previous employment information; Emergency contact: Name, Address, Telephone number; and Education information. Additionally, Occupational health evaluation information - personnel employment qualification/disqualification based on physical evaluations; and, disability status/level for disability pay and social security entitlements.

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

To mitigate these risks, various layers of security controls have been implemented within SPMS to achieve a defense-in-depth security strategy. Technical and procedural access controls have been implemented to restrict access to the data processed/stored in SPMS 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 the SPMS application. SPMS is protected from network attacks via a series of boundary protection devices located at various layers of the DoN enterprise network on which SPMS resides.

ISSMs/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 the SPMS unless they have been vetted through background investigations and have explicit approval by the command security manager, supervisor, information owner and ISSM.

Physical Security measures have been implemented to protect the servers hosting SPMS. SPMS 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 SPMS 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 N8 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.  SP Navy Pagaduria; SP Hacienda (Treasury) and Soc. Sec. Agencies

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.

All data captured are required by Spanish Fiscal Laws.

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.

All data captured are required by Spanish Fiscal Laws.
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.

- T1 & T2 Formats for Spanish Hacienda and Seguridad Social (SP Tax Agency and Social Security)
- Relacion nominal (Leave and Earning Statement) to SP Pagaduria (Disbursing)
- Certificados Instituto Nacional de Empleo (INEM) -SP Nat. Employment certificates-
- All other certificates requested by SP ministry of Defense (MOD)

The initial collection of personnel information is conducted by the Human Resources Office for the Spanish Navy (Non-US personnel). All Spanish Employees are employed by the Spanish Ministry of Defense (MOD) and indirect support to the US Navy; therefore, the information that is collected within the SPMS Application is provided to the US Navy by the Spanish MOD HRO, and not by the individual.

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.