PRIVACY IMPACT ASSESSMENT (PIA)

For the

Personnel, Physical, Information and Communications Security System (PPICSS)
Department of the Navy - United States Marine Corps (USMC)

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

☐ **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 NM05000-2

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 Corps
E.O. 9397 (SSN), as amended

Other authorities:

DoDD 5200.1R, Information Security Program
DoDD 5200.2R, Personnel Security Program
SECNAVINST 5510.30, Department of the Navy Personnel Security Program

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 Personnel, Physical, Information and Communications Security System (PPICSS) provides state of the art security program management and service support to the offices of the Commandant of the Marine Corps, Assistant Commandant of the Marine Corps, Deputy Commandants and Director Marine Corps Staff. PPICSS is a contractor developed government owned security service support and training web application. PPICSS utilizes an encrypted database for the collection and processing of security service support requests. PPICSS will be utilized to process requests for personnel security background investigations, grant access to classified national security information, issue DoD Common Access Card and Badge credentials, conduct inspections, maintain classified information inventories. A full SSN will be collected in order to process requests with DoD systems that require a full SSN to complete the request, i.e., Joint Personnel Adjudication System (JPAS), OPM e-Questionnaire for Investigations Processing, Contractor Verification System, Pentagon Force Protection Agency.

PII collected includes: Name, SSN.

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

The risks to the PPICSS system are identical to the threat facing all networked automated information systems (AIS) or applications whether government or commercial, classified or unclassified. Vulnerabilities exist in hardware and infrastructure, applications and system software, systems and network management, and in the nature of humans and organizations. Several threat agents act without being directed to specific targets and are therefore threats to the PPICSS system regardless of whether it is specifically targeted or not. The following are examples of these threats:

-The human intentional (insider, outsider) threat to the PPICSS system includes system developers, users, and maintainers; it encompasses all phases of the system life cycle. This threat agent can use tactics such as the introduction of malicious logic into the PPICSS software (applications, database, or operating system).
-The human unintentional threats (uninformed users, programmer errors, user errors) are driven primarily by the lack of experience, proper documentation and training.
-Site-specific environmental threats (power failures, outages, spikes, brownouts, loss of communications, water damage from flooding, fire) may pose a significant threat to the PPICSS system.
Intentional or unintentional inappropriate dissemination or unauthorized disclosure of PPICSS PII.

PPICSS has taken steps to mitigate the privacy risks by implementing standardized security controls and minimizing the amount of information collected to the minimum necessary. The PPICSS system has implemented all applicable controls from DoD Instruction 8500.2 based on Mission Assurance Category (MAC) III Sensitive system. PPICSS is also controlled by a Configuration Control Board (CCB), which reviews the impact of changes on the security posture and if risks or vulnerabilities are identified, they are mitigated immediately. Access to the PPICSS system is provided on a need to know basis and via CAC PKI authentication. Access to the PPICSS data is granted at the Security Office level. A PPICSS user only has access to data that they are affiliated with based on assigned roles and permissions.
Connections to the system are secured by 256-bit Secure Socket Layer (SSL).

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. Information will be shared among vetted and appointed USMC account managers, Department of the Navy Central Adjudication Facility, Naval Criminal Investigative Service.

☒ **Other DoD Components.**

Specify. Office of Personnel Management, Pentagon Force Protection Agency, Defense Manpower Data Center

☐ **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.

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

The external DoD applications and agencies the security office utilizes for completion of service does not accept requests without submission of an SSN. In most cases, the SSN is the key necessary to verify identification of the individual, a necessary step in the completion of background investigations and granting access to classified national security information. Individuals may not be granted access to classified information or secure spaces, issued building badges or Common Access Cards without verifying identity. As external agencies migrate to the use of a service number, PPICSS will modify its data collection fields to remove unnecessary collections of PII.

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.

Individuals will read and sign a release letter authorizing the use of their SSN for matters pertaining to Personnel and Information Security service support requests. The original will remain on file with the Security Coordinator through the duration of their stay plus two years after departure. A copy will be provided to the individual.

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

N/A

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.

Individual reads and signs a copy of the privacy act statement upon arrival as part of the check-in process.

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.