



PRIVACY IMPACT ASSESSMENT (PIA)

For the

MANPOWER .NET VER 1.0.x.x

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
- 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

M01040-3

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
10 U.S.C. 1074f, Medical Tracking System for Members Deployed Overseas
32 CFR 64.4, Management and Mobilization
DoDD 1215.13, Reserve Component Member Participation Policy
DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural and Manmade Disasters
CJCSM 3150.13B, Joint Reporting Structure Personnel Manual
DoD Instruction 6490.03, Deployment Health
MCMEDS: SECNAVINST 1770.3D, Management and Disposition of Incapacitation Benefits for Members of the Navy and Marine Corps Reserve Components (Renamed Line of Duty(LOD))
MCO 7220.50, Marine Corps Policy for paying Reserve Marines
E.O. 9397 (SSN), as amended

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 Manpower .NET environment provides the platform upon which the Deputy Commandant for Manpower & Reserve Affairs Department (DC M&RA) can develop, test, and deploy manpower-specific applications and data. Based upon Microsoft .NET Framework, the Manpower .NET environment allows users to customize their browsing experience within the Manpower .NET environment - drilling through to applications and information that is important to them as individuals.

If personally identifiable information (PII) were allowed in the site collection, this could include names, addresses, birth dates, and social security numbers. It could be stored in SharePoint lists and document libraries, with permission groups used to control access to the information.

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

Risk: Records are retrieved by name and/or Social Security Number.

Safeguards: Login to systems and network requires use of the DoD Common Access Card (CAC). Public Key Infrastructure (PKI) network login may be required to allow for documents to be digitally signed and encrypted and/or the receiving of encrypted mail. All official users use the CAC and PKI to login to their computer, digitally sign and encrypt email and other documents used to establish secure internet sessions.

Access to server rooms, are strictly controlled by the hosting facility personnel in accordance with established Navy/Marine Corps security and access procedures. At a minimum, cipher locks, access rosters, sign-in sign-out procedures, escort and supervision of all maintenance personnel and physical security checks are provided on a routine basis. Physical security of buildings after normal working hours, are provided by independent security guards or military police. Periodic and unannounced audits to ensure compliance of security procedures are conducted at least quarterly.

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.

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

The "Gold Source" of data is the Operational Data Store Enterprise (ODSE), which in accordance with the USMC rules for contesting contents and appealing initial agency determinations are published in Secretary of the Navy Instruction 5211.5E; 32 CFR part 701; or may be obtained from the system manager

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.

As data is shared from the centralized manpower databases (ODSE and MCTFS), individuals are not provided the opportunity to object to the data collection. Although Marines do not have the opportunity to object to PII within MANPOWER .NET, they do have the opportunity to object to information in ODSE and MCTFS at anytime. A Marine can also view their individual record through the Total Force Administration System (TFAS) Marine OnLine (MOL) application which is a self-service personnel portal.

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.

PII is not collected directly from 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.

SECTION 3: PIA QUESTIONNAIRE and RISK REVIEW

a. For the questions in subparagraphs 3.a.(1) through 3.a.(5), indicate what PII (a data element alone or in combination that can uniquely identify an individual) will be collected and describe the source, collection method, purpose, and intended use of the PII.

(1) What PII will be collected? Indicate all individual PII or PII groupings that apply below.

- | | | |
|--|--|--|
| <input checked="" type="checkbox"/> Name | <input type="checkbox"/> Other Names Used | <input checked="" type="checkbox"/> Social Security Number (SSN) |
| <input checked="" type="checkbox"/> Truncated SSN | <input type="checkbox"/> Driver's License | <input checked="" type="checkbox"/> Other ID Number |
| <input checked="" type="checkbox"/> Citizenship | <input checked="" type="checkbox"/> Legal Status | <input checked="" type="checkbox"/> Gender |
| <input checked="" type="checkbox"/> Race/Ethnicity | <input checked="" type="checkbox"/> Birth Date | <input checked="" type="checkbox"/> Place of Birth |
| <input checked="" type="checkbox"/> Personal Cell Telephone Number | <input checked="" type="checkbox"/> Home Telephone Number | <input checked="" type="checkbox"/> Personal Email Address |
| <input checked="" type="checkbox"/> Mailing/Home Address | <input checked="" type="checkbox"/> Religious Preference | <input type="checkbox"/> Security Clearance |
| <input checked="" type="checkbox"/> Mother's Maiden Name | <input type="checkbox"/> Mother's Middle Name | <input checked="" type="checkbox"/> Spouse Information |
| <input checked="" type="checkbox"/> Marital Status | <input type="checkbox"/> Biometrics | <input checked="" type="checkbox"/> Child Information |
| <input checked="" type="checkbox"/> Financial Information | <input checked="" type="checkbox"/> Medical Information | <input checked="" type="checkbox"/> Disability Information |
| <input type="checkbox"/> Law Enforcement Information | <input checked="" type="checkbox"/> Employment Information | <input checked="" type="checkbox"/> Military Records |
| <input checked="" type="checkbox"/> Emergency Contact | <input checked="" type="checkbox"/> Education Information | <input checked="" type="checkbox"/> Other |

If "Other," specify or explain any PII grouping selected.

Personnel record or enlistment or reenlistment document recording original expiration of service date;

All ODSE and MCTFS data elements

(2) What is the source for the PII collected (e.g., individual, existing DoD information systems, other Federal information systems or databases, commercial systems)?

PII through system-to-system (ODSE and MCTFS) as well as interfaces with Manpower .Net via a web service over Secure Hyper Text Protocol.