



PRIVACY IMPACT ASSESSMENT (PIA)

For the

Enterprise Mass Notification System (eMNS)

Department of the Navy - 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

DITPR ID: 17768	DITPR DON ID: 23224
-----------------	---------------------
- 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-117?

- Yes
- No

If "Yes," enter UPI

UII: 007-000100936

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 Program Management and Locator System

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

Collects on federal personnel only.

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 NM05000-2, Program Management and Locator System, January 24, 2008 Authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
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.

This system provides pop-up messages to Marine Corps Enterprise Network (MCEN) NIPR workstations attached to the Local Area Network. The Enterprise Mass Notification System (eMNS) is also known as AtHoc IWS Alerts. (AtHoc is the name of the vendor supplying the commercial-off-the-shelf (COTS) eMNS/IWS Alerts application). The eMNS has the capability to send alerts to personnel in its database via electronic mail (email), telephone, Short Message Service (SMS) text messages, and a smart phone application. Alerts provide information pertaining to personnel recalls, real-world and exercise incidents. The nature of the alerts provided makes the eMNS a life-safety system. It is an operational system owned by the US Marine Corps.

PII collected: From MCTFFS: Name, UIC/Command (location), Work Email, and Work Phone. Through the CAC enabled self-service portal personnel can enter: Personal Email Address, Personal Cell Phone Number, Home Phone Number, Dependent Phone Number. Designated Mission Essential Personnel are required to provide Home Phone Number or Personal Cell Phone Number for recall purposes.

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

All reports generated from the Telecommunications Notifications System containing Personally Identifiable Information (PII) will be used for the sole purpose of validating confirmation alert messages. These reports will only be reviewed by the Command Post personnel and applicable leadership authorities and then will be shredded upon completion of need. Access to the Base Local Area Network containing the PII data is limited to Common Access Card users and further restricts Telecommunications Notifications System application access with an additional user identification and password

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.

Non key civilians may elect to object to the collection of this PII. This is identified in the web-based Self Service page where this information is inputted by each individual. Objection can be easily accomplished by simply not inputting their information in the system. When this information is requested by individuals, a Privacy Act Statement (PAS) is provided which informs them that the collection is voluntary not mandatory for non key civilians but mandatory for Military members and key civilians.

(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.

The act of inputting the Personally Identifiable Information data into the Telecommunications Notifications System constitutes the consent for specific use. The Privacy Act Statement gives individuals the option to provide or not provide their Personally Identifiable Information to be used with the system. The instructions given to individuals when they fill it out states that by inputting their information in this system, they are giving their consent for its use as stated in the Privacy Act Statement.

k. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Privacy Act Statement | <input type="checkbox"/> Privacy Advisory |
| <input type="checkbox"/> Other | <input type="checkbox"/> None |

Describe each applicable format.

Provided on the self-service portal.

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.