# PRIVACY IMPACT ASSESSMENT (PIA)

## For the

IPP Network Alerting System (NAS) 1.0

Emergency Management Modernization Program (EM2P)

## 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: 15698 /DA207858
- ☐ **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**: A0500-3c G3/5/7

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.

5 U.S.C. 301, Departmental Regulation; DoD Directive 5105.19, Defense Information Systems Agency (DISA).

**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 Network Alerting System (NAS) is designed to provide timely and accurate warning and notification of Chemical, Biological, Radiological, and Nuclear (CBRN) events and incidents to installation personnel, particular emphasis placed on warning and notification of critical mission personnel. NAS shall be interoperable with the existing installation systems and operate within their intended environments. NAS permits a distributed organization to alert different groups using different alerting devices, including desktop pop-ups, voice telephony, text messages to mobile devices, e-mail, Giant Voice and other devices. NAS tracks alert distribution and responses, and provides its operators with online reports showing progress of alert dissemination. NAS operators connect via a secure and permission-based web User Interface (UI) to perform alert creation, initiation and administration tasks. NAS end-users can use its secure web based self-service to view past and current alerts, and view and update their personal details. The PII collected for NAS consists of the following:
*Name
*Other names used
*Personal cell telephone number
*Personal email address
*Home telephone number

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

The privacy risks associated with NAS are minimal. The only PII collected by NAS consists of installation personnel's names and the various telephone numbers by which they may be contacted during a CBRN incident.

**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. NAS information is only shared within the within the military installation to which NAS is deployed.

☐ **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.

Each military installation with NAS has authority to enact its own privacy policies, presumably consistent with service requirements. Any given individual on a NAS deployed installation may elect to not provide their telephone contact numbers, and thus this information would not be captured by NAS.

The only exception is Emergency Essential Personnel as they are required to provide such information per condition of their employment.

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

**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.

The specific use of this NAS is for notifications to be sent during emergencies, and a user cannot opt out of certain notifications.

**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. | If you wish to furnish personal information requested as part of the MWN is registration, you may do so. Personal information includes non-government furnished e-mail addresses, home and personal cell phone numbers, personal pager numbers, and other personally owned or furnished devices. If you choose NOT to furnish personal information, the system will be unable to contact you on these devices. |

**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.**