# PRIVACY IMPACT ASSESSMENT (PIA)

## For the

| Computer Desktop Notification System (CDNS) |
| --- |
| 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

☐ **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** N01754-4 NFAAS

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.

Internal housekeeping - DODI 8500.1 Information Assurance, October 24, 2002, DODI 8510.01 Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Instruction.

Indirect Authority -
10 U.S.C. 5013, Secretary of the Navy and E.O. 9397 (SSN) as amended,
DODINST 6055.17 DoD Installation Emergency Management (IEM) Program,
OPNAVINST 3440.17 Navy Installation Emergency Management Program,
CNICINST 3440.17 Navy Installation Emergency Management Program,
UFC 4-021-01 Design and O&M: Mass Notification Systems.

**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.

Computer Desktop Notification System (CDNS) (vendor: AtHoc, product: IWSAlerts) provides Navy installations with the ability to rapidly and effectively disseminate emergency alerts and notification information to installation personnel. To assess disaster-related needs of Navy personnel and their families who are involved in a natural or other man-made major disaster or catastrophic event. Region and Installation Emergency Management personnel are required to notify all installations within a 10 minute period from the time of emergency event determination. CDNS utilizes various communication mediums such as workstation pop-ups, telephone (work, mobile, home), e-mail (work, home), pagers, and SMS (text messaging) in order to achieve a high rate of notification success. Utilization of various communications mediums allows for alerts and notifications to occur in a 24/7 mixed work environment on Navy installations. CDNS can target all base personnel or targeted groups of personnel by name, role, and/or location. PII elements collected: First Name, Last Name, Email - Work - Primary, Phone - Work, Email - Work - Secondary, Phone - Mobile, SMS, TTY/TTD Phone, Email - Home, Phone - Home, Pager (Numeric), Pager (One Way), Pager (Two Way). User name is passed to CDNS system via NMCI or One-Net workstation login.

(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 CDNS 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 region and installation emergency management personnel and applicable leadership authorities with a need to know and then will be shredded upon completion of need. Access to the NMCI/One-Net Networks containing the PII data is limited to Common Access Card users and further restricts CDNS system users as designated by the region and installation authorities. CDNS application access utilizes user identification and password with user based permissions to restrict access.

**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. Navy region and installation emergency management personnel and applicable leadership authorities

☐ **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.

Alert recipients are supplied with a Self Service web page entry for their data submission. Work e-mail and work telephone number are utilized notifications during working hours where home phone and home e-mail data is optional for the user to enter but allows for notification during off hours. 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 home telephone information in the system. When this information is requested from 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.

**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 act of inputting the Personally Identifiable Information data into the CDNS 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. Only the areas with provided information will be activated.

**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.

AUTHORITY: DODINST 6055.17, OPNAVINST 3440.17, CNICINST 3440.17 , UFC 4-021-01, 10 U. S.C. 5013 and E.O. 9397 (SSN), as amended.

PRINCIPAL PURPOSE(S): Computer Desktop Notification System (CDNS) serves as part of the Navy Region and Installation Mass Notification System (MNS). CDNS provides pop-up messages to the workstations attached to the NCMI/One-Net Networks. In addition, CDNS has the capability to notify members in the database, via electronic mail and telephone, of real-world and exercise threat conditions.

ROUTINE USE(S): Emergency Operations teams and System Administrators have routine access to the PII information. This information will be used during emergency operations to contact individuals.

DISCLOSURE: Disclosure is required for military and key-civilians and voluntary for non-key civilians. Failure to disclose information would result in not being notified of mission or natural disaster alert notifications.

**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.**