PRIVACY IMPACT ASSESSMENT (PIA)

For the

Emergency Notification System (ENS)

Department of the Navy - NAVSUP - NEXCOM

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

Non-Appropriated Fund (NAF)

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

If "Yes," enter UPI

NAF

If unsure, consult the Component IT Budget Point of Contact to obtain the UPI.

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

NAF

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

N04066-5

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

ENS does not collect information from members of the public.

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 N04066-5 NEXCOM Direct Mail List/Patron Profile  (September 09, 1996,  61 FR 47483)

Authorities:

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 system's purpose is to alert NEXCOM associates of emergency events that affect their personnel or local NEXCOM operating structure.

PII collected: The information within the ENS is pulled from active directory. This information includes: Name, Work Email, Work Phone, DoD ID number, and Work location.

Associates have the option to enter their home phone, mobile phone, home address, and personal email to receive alerts from the system through the desktop client software.

(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 PII are limited to the Navy Exchange Emergency Notification System operators who create and manage alerts for associates. Risks are limited, as this information is safeguarded with logical and physical access controls that include system access and authentication, physical access, systems monitoring, and physical monitoring. System values are set: user profile expiration, system inactivity, password validation. Only administrators have database accessibility. Vulnerability scans are generated and executed continuously in search of system and application vulnerabilities. System controls are tested annually and through maintaining RMF ATO accreditation.

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. NEXCOM personnel - system administrators

- **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. AtHoc - All data will be transmitted securely using HTTPS/ TLS to their alert system for the purposes of sending alert notifications only. Contract Clause 252.204-7012 - Safeguarding Covered Defense Information and Cyber Incident Reporting, DEC 2015. Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology (IT) Systems or Protected Health Information Homeland Security Presidential Directive (HSPD)-12, requires government agencies
to develop and implement Federal security standards for Federal employees and contractors. The Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006 – “DoD Implementation of Homeland Security Presidential Directive – 12 (HSPD-12)” dated November 26, 2008 (or its subsequent DoD instruction) directs implementation of HSPD-12. This clause is in accordance with HSPD-12 and its implementing directives. This clause applies to contractor employees requiring physical access to any area of a federally controlled base, facility or activity and/or requiring access to a DoN or DoD computer/network/system to perform certain unclassified sensitive duties. This clause also applies to contractor employees who access Privacy Act and Protected Health Information, provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Position, as advised by the command security manager. It is the responsibility of the responsible security officer of the command/facility where the work is performed to ensure compliance.

In accordance with SECNAV M-5510.30, contractor employees who require access to DoN or DoD networks are categorized as IT-I, IT-II, or IT-III. The IT-II level, defined in detail in SECNAV M-5510.30, includes positions which require access to information protected under the Privacy Act, to include Protected Health Information (PHI). All contractor employees under this contract who require access to Privacy Act protected information are therefore categorized no lower than IT-II. IT Levels are determined by the requiring activity’s Command Information Assurance Manager.

Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Navy recognizes contractor employees under this contract as Non-Critical Sensitive [ADP/IT-II] when the contract scope of work require physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and Protected Health Information (PHI), provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLC to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position.

Privacy FAR clauses are not included in the contract with AtHoc because of NEXCOMs’ Non-Appropriated status.

☐ 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.

The information within the ENS is pulled from active directory. This information includes: Name, Work Email, Work Phone, DoD ID number, and Work location.

Associates have the option to enter their home phone, mobile phone, home address, and personal email to receive alerts from the system through the desktop client software. Not entering this information could affect the government’s ability to contact the individual in case of an emergency.

(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.

By providing their personal contact information via the Desktop Portal, the individual consents to allowing NEXCOM to use the information for the sole purpose of alerting them when an emergency event occurs.

The individual cannot consent to the use of the PII pulled from the active directory.

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

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.

All users will be notified via email prior to the Desktop client roll-out of their privacy. The text will be as follows:

Any private contact information (PII) you provide in the Emergency Notification System will be used for emergency notification purposes only. By providing such information you consent to the use of your information for the sole purpose of emergency notification. Your information will not be shared with any other systems or entity.

Privacy Act Statement (PAS)

We do not rent, sell, or exchange your name with other organizations. We protect our databases with various physical, technical and procedural measures and we restrict access to your information by unauthorized persons. Our information systems are maintained behind a software firewall to isolate them from access by other networks connected to the internet.
All information transmitted through our emergency notification system is stored on our secure server. We use Transport Layer Security (TLS) technology, which is the electronic commerce standard for securing information over the internet. TLS technology encrypts your information, preventing an unauthorized party from viewing and downloading your information.

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.