PRIVACY IMPACT ASSESSMENT (PIA)

For the

OCONUS Navy Consolidated Emergency Response System (ON-CERS)
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 DITPR DON ID: 23313

☐ **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 UII: 007-000009990

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 N05200-08 (pending the processing of the OMB Control Nbr)

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

The SORN is currently submitted for processing. An OMB agency 60-day Federal Register Notice and OMB Form 83-I is submitted for processing. This PIA will be updated to reflect the OMB control number upon issuance by OMB.

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 N05200-08 authorities:

10 U.S.C 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
OPNAVINST 5530.14E, Navy Physical Security
DODD 5200.8, Security of DOD Installations and Resources.

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.

OCONUS Navy Consolidated Emergency Response System (ON-CERS) is a computer aided dispatch (CAD) system that offers an integrated and expandable Navy Enterprise system to support emergency responders OCONUS to Navy shore installations. Integrated technologies enable the Navy to consolidate emergency calls, collect data if applicable to the incident, and dispatch functions for police, fire, and emergency medical agencies. ON-CERS is a scaled down version (physically) than Enterprise Navy Emergency Response Management Systems (ENERMS) however serves the same function for OCONUS.

Personal information collected: Name, other names used, driver's license and other government identification numbers, citizenship, legal status, gender, race/ethnicity, birth date, place of birth, home and personal cell telephone numbers, personal email address, mailing and home address,marital status, Spouse information: collected only if relevant to emergency. 1) Be On the Lookout For (BOLO) is issued for spouse - dispatch collects and stores Name/AKA/Physical Description/Last known Sighting, etc. Think Amber Alert type information. 2) If the spouse is involved in a Police call (ex: Domestic Violence) only name/address/statement if given. Other information like injuries is collected at the ER, NOT Dispatch.

Child information: collected only if relevant to emergency involving a child, such as the child is the victim of a medical emergency, or the child is the subject of an alert, like an Amber Alert.

Medical information: collected only if relevant to medical emergency/event up to the point when EMS arrives on scene. Good examples would include symptoms that required the 911 call, such as chest pains or shortness of breath. All other medical info is collected/stored by the responders and receiving healthcare facility, not within ON-CERS.

Disability information: Not typically collected, seldom relevant to call. Could be if a person with a disability requires assistance, such as "is in a wheelchair" or "is hearing impaired."

Law enforcement information: collected only if relevant to call up until police arrive on scene. Further LE info is not collected. For example, if we dispatched police to your home and you left under arrest - that is not collected or stored by ON-CERS. We only record that "Police Unit 4) is off scene and back in service.

Emergency contact information: relevant to almost every call and stored by ON-CERS as necessary. Such as, if you call 911 for yourself, and they ask who your emergency contact is, and you provide the name of your roommate, or spouse, etc.

Additional information provided by the program to add clarity:
Some general statements regarding PII collected and stored by Dispatch/ON-CERS:
1) The "automatic/mandatory" data stored include: the phone number and location of that call, what response unit was dispatched, and that unit's disposition (On Scene, En Route, Out of Service, etc).
2) Virtually all PII is collected by the Dispatcher and recorded per SOP, County and State Laws, etc. For example, dispatchers can enter whether or not there are firearms in that residence, something LEO would like to know before knocking. Whether or not they actually do that, is a matter of SOP.

There is no specific PII information required by CAD for entry but any of the categories above and any other desired information may be collected and recorded depending upon the operational procedures for each region. For example, a traffic stop would typically include the vehicle license plate number and driver's license information along with any returned criminal history information from an NCIC check. A fire response to a heart attack would typically involve collecting and recording patient information such as name, age, sex and current health condition. However, what ultimately is entered is determined by the operation procedures of each region."

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

The perceived threats are primarily computer hackers, disgruntled employees, state sponsored information warfare, and acts of nature (e.g., fire, flood, etc.)

Access is provided on a need-to-know only. Collection for the ON-CERS system is provided via field officers and emergency personnel which will be relayed via radio to to dispatchers or by direct phone contact from the reporting party. The computer terminals are located in supervised areas. Access is controlled by password or other user code systems. Computerized records maintained in a controlled area are accessible only to authorized personnel. Records are maintained in a controlled facility. Physical entry is restricted by the use of locks, guards and is accessible only to authorized personnel. Physical and electronic access is restricted only to authorized personnel. Physical and electronic access is restricted to designated individuals having a need in the performance of official duties and who are properly screened and cleared for need-to-know. Access is restricted by authorized persons who are properly screened. The systems are also password protected and/or use Primary Key Infrastructure (PKI)/Common Access Card (CAC) protected.

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 law enforcement and legal offices as required

☐ **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. Serco. The NAVFAC AT/FP Program Office administers and sustains the ON-CERS IS through a global sustainment contracts. In these contracts, DoDI 8500.01 is referenced. Within 8500.01 is DoD 5400.11 and 14 (also referenced) which contractors are required to follow to safeguard PII. The FAR Privacy clauses are included in the current contract.

☐ **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.

Dispatchers consolidate emergency calls, collect data as applicable to the incident, and dispatch functions for police, fire, and emergency medical agencies. The information is of use for emergency situations and Navy Legal/Law Enforcement as required.

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.

Dispatchers consolidate emergency calls, collect data if applicable to the incident, and dispatch functions for police, fire, and emergency medical agencies. The information is of use for emergency situations and Navy Legal/Law Enforcement as required.

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.

Emergency calls for service require information to be collected and services dispatched for appropriate response as quickly as possible. Due to life-safety concerns and time being a critical element in response, no privacy act statements or advisories are provided to a caller that is requesting emergency services.

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.