PRIVACY IMPACT ASSESSMENT (PIA)

For the

Consolidated Emergency Response System (CERS)
Department of the Navy - United States Marine Corps (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	☐	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	13992 (DITPR DON ID 22322)
☐	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

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.

Other Authorities:

Sec Def Memo dated August 18, 2010 "Final recommendations of the Fort Hood Follow-On Review"
Sec Nav Memo dated 13 Sept 2010, "Department of the Navy Policy on Emergency Calls Originating from DoN operated installations."
Marine Corps Order MCO 5580.2B 27 Aug 2008 "Law Enforcement Manual"
Marine Corps Order MCO 11000.11 23 Jun 2010 "Marine Corps Fire Protection and Emergency Services Program"

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.

CERS will be a Commercial Off the Shelf (COTS) product used by emergency dispatchers answering E911 calls. The purpose of the system is NOT to collect PII, but might as part of the handling of any given emergency response. This system is used to support, manage and document emergency responses from Fire, Police, Emergency Medical Services (EMS) or other entity via a emergency call dispatch center (911 services). The personal information about individuals collected during any given response is highly situational. In some cases, a name and address may be obtained, e.g. a caller gives their name and address for the dispatching of fire, police or EMS. Since not all emergencies are the same, different personal information could collected for each call or emergency response. The caller may also refuse to give their name.

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

There are a few privacy risks associated with this system. Unauthorized Disclosure is the biggest and most likely risk. The Dispatchers, Fire, Police or EMS personnel may inappropriately discuss an incident and use the names of the involved personnel. Depending upon the scale of the incident, local news or national news personnel may broadcast information about the incident or personnel involved. Dispatch, Fire, Law Enforcement, Emergency Medical Services (EMS) personnel are trained to not discuss PII with unauthorized personnel. Large newsworthy incidents are handled by authoritative command personnel. Dispatch personnel are trained and treat all matters of incidents, including PII, professionally and within the bounds of job requirements.
Another risk to privacy is unauthorized access to PII. CERS itself contains different fields for information input, which are searchable for data elements. The system is designed to support emergency responses from a dispatch center. Dispatch centers are typically operated 24 x 7 x 365 by trained personnel. These centers are access controlled, may have cameras, or intrusion detection systems and are often co-located with law enforcement personnel. CERS resides within a limited access guarded facility. CERS is only accessible to a very limited number of trained personnel from a small number of Dispatcher workstations. CERS operates on a restricted access LAN that is not connected to the internet or the USMC network but rather on a Public Safety Network (PSNet) provided by Commander Navy Installations Command (CNIC). PSNet is a very restricted access network design to support emergency responses for military bases, posts and installations.
PII may also reside on media such as back-up data disks, tapes, or output to other media to share with other entities. All information from CERS will be encrypted to the greatest extent possible to meet mission requirements and information sharing agreements. All information shared will be subject to an information sharing agreement that will require the recipients to protect PII in accordance with all applicable laws and directives.

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. PII may be shared with fire, EMS, hospital, a Commander, or Law Enforcement.

☒ **Other DoD Components.**

Specify. PII may be shared with mutual aid partners that could include fire, EMS, hospital, a Commander, or Law Enforcement.

☒ **Other Federal Agencies.**

Specify. Depending upon a given incident, PII could be shared with other Federal

Agencies, e.g. another Fort Hood type shooting incident could drive the need to share PII with other Federal Agencies such as the FBI.

☒ **State and Local Agencies.**

Specify. Depending upon a given incident, PII could be shared with State and Local Agencies, e.g. a local citizen non-affiliated with the USMC is involved in an incident on a USMC installation may have PII shared with State and Local Agencies.

☐ **Contractor** (Enter name and describe the language in the contract that safeguards PII.)

Specify.

☒ **Other** (e.g., commercial providers, colleges).

Specify. It is possible that an incident may occur that requires the sharing of PII with Mutual Aid Partners.

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.

The purpose of the system is NOT to collect PII, but might as part of the handling of any given emergency. The individual(s) involved in any given emergency response may object but are not specifically given notice or offered the opportunity to object. Criminal law enforcement information is usually exempted from the Privacy Act individual notice provisions, and the Privacy Act (j)(2) exemption has also been claimed to exempt that same information. An unconscious victim being treated under an emergency dispatch has implied consent. Because of the nature of an emergency response, an unconscious victim is unable to object. A law enforcement emergency response has a need to collect information as part of an emergency response. For example, due to the law enforcement need to request and obtain a drivers license (within the boundary of a given incident e.g. traffic accident), the individual may object but are still required to produce a valid license. This information may be entered into CERS and/or shared with other DoD, State, Local or other entity (i.e. a Want or Warrant may trigger the sharing of information).

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 Privacy Act of 1974
(b) Conditions of Disclosure
(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

In addition, an unconscious victim being treated under an emergency dispatch has implied consent. Because of the uncertain nature of any emergency, it would not be practical to give notice to object or consent at the time of the emergency. A law enforcement emergency response has a need to collect information as part of an emergency response. Criminal law enforcement information is usually exempted from the Privacy Act's individual notice provisions, and the Privacy Act's (j)(2) exemption has also been claimed to exempt that same information.

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.

A PAS would not be provided to the individual since this would be in relationship to an emergency situation.

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.