PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:

Consolidated Information Center- Portal for Readiness and Emergency Preparedness Dashboard

2. DOD COMPONENT NAME:	3. PIA APPROVAL DATE:
Defense Health Agency	04/22/24

Navy Bureau of Medicine and Surgery (BUMED) Consolidated Information Center (CIC)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: *(Check one. Note: Federal contractors, military family members, and foreign nationals are included in general public.)*

☐ From members of the general public   ☒ From Federal employees

☐ from both members of the general public and Federal employees   ☐ Not Collected *(if checked proceed to Section 4)*

b. The PII is in a: *(Check one.)*

☒ New DoD Information System   ☐ New Electronic Collection

☐ Existing DoD Information System   ☐ Existing Electronic Collection

☐ Significantly Modified DoD Information System

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

The Consolidated Information Center Portal for Readiness and Emergency Preparedness (CIC PREP) Dashboard is a web application for data entry and reporting designed for various Navy Medicine Facilities. The application is divided into two main sections: Emergency Preparedness and Anti-Terrorism. It enables the management of live data in real-time and provides analytical reports, empowering Navy Medicine to visualize metrics related to preparedness and readiness and gauge its progress toward meeting preparedness and readiness goals. The application is constructed using a high-performance modern front-end web framework (React), a backend (Python Flask), and a database (PostgreSQL 15). Infrastructure and continuous Integration Continuous delivery/deployment (CI/CD) pipelines have been set up within the Amazon Web Solution (AWS) cloud environment and will serve as the deployment platform for the application. Both the application's database and codebase will be housed in the AWS. A front-end web user interface (UI) allows the user to input data into specific form fields as well uploading supporting documents. Other UI services provide users with a forum for comments and feedback for the development team. Report data will be recorded weekly and saved in historical reports, allowing users to access records and important reports for defined periods. Access to the application via a web interface requiring DoD PKI authentication. Further access is restricted to a predefined list of users. This list resides within its codebase and maintained by its administrators. The application utilizes a role-based model granting access to either side of the application or both, depending on user's need-to-know and position. A record of access activity is maintained by application for auditing and security purposes. CIC PREP is a Tier 3 SOR inheriting policies from the DHA.
The following categories of individuals from which PII is collected includes Active Duty Service Members, Reserve personnel, and Federal employees. CIC PREP collects official point of contact information such as names, work e-mail address, official duty telephone, PII.

CIC PREP is owned and managed by the Navy Bureau of Medicine and Surgery (BUMED) Consolidated Information Center (CIC) Program Management Office (PMO).

d. Why is the PII collected and/or what is the intended use of the PII? *(e.g., verification, identification, authentication, data matching, mission-related use, administrative use)*

The intended use of the PII collected is to provide point of contact information for mission-related and administrative purposes.

e. Do individuals have the opportunity to object to the collection of their PII?   ☒ Yes   ☐ No

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

An individual can refuse participation by not inputing the requested information. Results of not providing the requested information will severely hinder CIC PREP users from gaining point of contact information for MTF emergency management and/or anti-terrorist personnel.

f. 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.

It is assumed that consent is given by the individual inputing their PII in order to utilize and participate in the mission function of CIC PREP.

g. **When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided.** *(Check as appropriate and provide the actual wording.)*

☐ Privacy Act Statement ☐ Privacy Advisory ☒ Not Applicable

The PII collected is considered Business Rolodex Information, therefore does not require a PAS or advisory.

h. **With whom will the PII be shared through data/system exchange, both within your DoD Component and outside your Component?** *(Check all that apply)*

☒ Within the DoD Component — Specify. Navy Bureau of Medicine and Surgery (BUMED)

☐ Other DoD Components *(i.e. Army, Navy, Air Force)* — Specify.

☐ Other Federal Agencies *(i.e. Veteran's Affairs, Energy, State)* — Specify.

☐ State and Local Agencies — Specify.

☐ Contractor *(Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)* — Specify.

☐ Other *(e.g., commercial providers, colleges).* — Specify.

i. **Source of the PII collected is**: *(Check all that apply and list all information systems if applicable)*

☒ Individuals ☐ Databases
☐ Existing DoD Information Systems ☐ Commercial Systems
☐ Other Federal Information Systems

j. **How will the information be collected?** *(Check all that apply and list all Official Form Numbers if applicable)*

☐ E-mail ☐ Official Form *(Enter Form Number(s) in the box below)*
☐ In-Person Contact ☐ Paper
☐ Fax ☐ Telephone Interview
☐ Information Sharing - System to System ☒ Website/E-Form
☐ Other *(If Other, enter the information in the box below)*

k. **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 <u>retrieved</u> by name or other unique identifier. PIA and Privacy Act SORN information must be consistent.

☐ Yes ☒ No

If "Yes," enter SORN System Identifier

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpcld.defense.gov/Privacy/SORNs/
    o*r*

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

A system of record notice (SORN) is not necessary because Consolidated Information Center- Portal for Readiness and Emergency Preparedness Dashboard (CIC PREP) is a AWS cloud hosted application utilizing a web form for collecting and reporting Emergency and Anti-terrorism readiness information. The CIC PREP system collects PII which is considered Business Rolodex Information, therefore does not require a SORN.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority.

GRS 5.3, item 010 (DAA-GRS-2016-0004-0001)

(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

FILE NUMBER: 201-22
DISPOSITION: Temporary. Cut off when superseded or obsolete. Destroy 3 years after cutoff.

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statue or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.
(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

  (b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.

Authorities include: 5 U.S.C §301 "Departmental Regulations"; 10 U.S.C §142 "Chief Information Officer"; 40 U.S.C §11315 "Agency Chief Information Officer"; 44 U.S.C §3506 "Federal Agency Responsibilities"; and 44 U.S.C §3554 "Federal Agency Responsibilities." Additional authorities to collect information are specific to the information systems or electronic collections of CIC PREP users and addressed in the privacy impact assessment for those respective information systems and electronic collections.

n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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   ☒ No   ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, " DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

CIC PREP does not collect data from other than DoD military, DoD civilians, or other Federal employees, therefore OMB approval is not required.