PRIVACY IMPACT ASSESSMENT (PIA)

For the

Commander Navy Installations Command Gateway 2.0 (GATEWAY 2.0)
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 ID: 14112 DITPR DON ID: 22289
- ☐ **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: 007-000004004

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 K890.21 DoD; N12293-1; N05041-1; T1300

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.

SORN K890.21 DoD authorities:

5 U.S.C. 301, Departmental Regulations
Pub. L. 106-229, Electronic Signatures in Global and National Commerce
OASD (C3I) Policy Memorandum, subject: Department of Defense (DoD) Public Key Infrastructure (PKI)
OASD (C3I) Memorandum, subject: Common Access Card (CAC).

SORN N12293-1 authorities:

5 U.S.C. 301, Department Regulations
5 U.S.C. Chapters 11, Office of Personnel Management; 13, Special Authority; 29, Commissions, Oaths and Records; 31, Authority for Employment; 33, Examination Selection, and Placement; 41, Training; 43, Performance Appraisal; 51, Classification; 53, Pay Rates and Systems; 55, Pay Administration; 61, Hours of Work; 63, Leave; 72, Antidiscrimination, Right to Petition Congress; 75, Adverse Actions; 83, Retirement; 99, Department of Defense National Security Personnel System;
5 U.S.C. 7201, Antidiscrimination Policy
10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness
E.O. 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended
29 CFR 1614.601, EEO Group Statistics

SECNAV Instruction 12250.6, Civilian Human Resources Management in the Department of the Navy
E.O. 9397 (SSN), as amended.

SORN N05041-1 authorities:

10 U.S.C. 5014, Office of the Secretary of the Navy
10 U.S.C. 5020, Naval Inspector General: details; duties
SECNAVINST 5430.57 series, Mission and Functions of the Naval Inspector General
SECNAVINST 5370.5 series, DON Hotline Program
E.O. 9397 (SSN), as amended.

SORN T1300 authorities:

5 U.S.C. 301, Departmental Regulations
DoD 7000.14-R, DoD Financial Management Regulation
DFAS 005, Delegation of Statutory Authority
E.O. 9397 (SSN), as amended.

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.

Gateway 2.0 (G2) utilizes a Microsoft SharePoint platform to provide CNIC HQ, Region, and Installation personnel with an integrated suite of capabilities that improve organizational effectiveness and collaboration by providing comprehensive content management and enterprise search, accelerating shared business processes, and facilitating information sharing for better business insight. In some instances, programs have created business management applications that capture/store/analyze/report on structured data related to service delivery. In limited cases, this involves the capture of PII. The collection of PII within G2 is only allowed with proper authority to support the program mission and must be contained within a designated controlled access area. Programs are only allowed to collect PII from Federal personnel and Federal contractors. Unstructured PII collected within G2 is described in Section 3 of this PIA. Each program's collection of the identified types of PII may vary depending on the purpose of the program.

Structured personal information collected: PII is used by the system to create the user account profile, i.e., user's name, DoD ID number, and department (N-code/Program/etc.)/office contact information.

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

The primary privacy risks associated with G2 is that with the large amounts of unstructured data, users may have put data in an unauthorized location or without proper authority. Data files stored by the programs are limited by logical controls to data types and storage methodologies and this is enforced by periodic monitoring of content stores. In addition, all data on G2 is protected by controlling access to G2 through CAC-based authentication. User default access is limited based on their profile. User profile data is limited to identity information related to the individual's office persona(s) and environment. No other data of a personal nature is included. The data will not be copied or shared with other systems for other purposes. Data access will be restricted to authorized and authenticated system administrators and other implementation and maintenance personnel. All access by these personnel will be logged and periodically audited. Users of this data will be CAC authenticated and restricted to viewing only the appropriate data.

Authorized collection of PII is safeguarded by:
1. Restricting capture/storage of PII to Controlled Access (CA) sites within the Gateway 2.0 environment, which further restricts access to such data;
2. Restricting membership for CA sites to persons identified by the affected N-Code as requiring access to the PII;
3. Configuring that restricted membership using Active Directory and SharePoint group memberships to automate access control and prevent unauthorized persons from accessing CA sites and the PII contained

therein; access controls are maintained 24/7/365;
4. Conducting random reviews of access to CA sites to ensure that CA sites are properly configured and used;
5. Reviewing PII collection on a periodic basis to determine whether its collection continues to be required;
6. If not required, removing PII entirely from the Gateway 2.0 platform.

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. CNIC, registered users of G2, including NAVFAC, DONCIO, NAVSEA. Programmatic exchange of PII to external systems is not performed. Any exchange of PII information is internal to CNIC and registered users of G2.

☐ **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.

(2) If "No," state the reason why individuals cannot object.

The PII collected, captured, and stored is required for the execution of command business (N1 management functions, OGC investigations, IG investigations and the like). Activities which involve collection, capture, and storage of PII are mission-essential activities and not subject to the individual approval of subjects of such activities. In fact, in many cases, it is essential to the performance of such activities that individuals not know that those activities are ongoing.

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.

As stated above, activities which collect, capture, and store PII are mission-essential CNIC activities not subject to consent or approval from individuals. Therefore, the command does not seek consent before gathering such data or storing it within the business management technology platform.

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.

Privacy Act Statements (PAS) are provided to individuals on a form when PII is collected as well as on the site where PII is collected.

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.