PRIVACY IMPACT ASSESSMENT (PIA)

For the

Scientific Computing Operations (SCO)
CNO - OPNAV N81 - Center for Naval Analysis

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**		

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 N01070-3, Navy Military Personnel Records System

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 authorities:

10 U.S.C. 5013, Secretary of the Navy
42 U.S.C. 10606 as implemented by DoD Instruction 1030.1, Victim and Witness Assistance Procedures
E.O. 9397 (SSN), as amended.

As a Federally Funded Research and Development Center (FFRDC), the Center for Naval Analyses (CNA) enjoys a special relationship with the DoN, having access beyond that which is common to the normal contractual relationship, to Government and supplier data, including sensitive data and proprietary data, and to employees and facilities. In keeping with this mandate, all DoN Activities shall provide CNA with all the information necessary to plan and conduct studies.

As the Navy's FFRDC CNA is expected to have current, up to date data in order to properly support DoN Study requirements. In particular, CNA has a requirement to provide Scientific Analyst support to N1/ CNP, which includes the requirement to provide quick-turnaround analyses making use of our historical and current holdings of Navy personnel and billet data.

CNA has legal and ethical obligations to ensure that private (and legally protected) information is secured in a manner that minimizes risk of unauthorized or inappropriate use or disclosure. In order to meet those obligations CNA maintains a Scientific Computing Operation (SCO). The mission of SCO is

to provide a secure, multi-user computing environment for project oriented analysis requiring the use of sensitive (PHI/PII) DoD, Navy, federal, non-DoD, and non-federal data. The data stored in the system includes sensitive and non-sensitive unclassified research data used for analysis only. SCO allows CNA staff members secure access to statistical analysis, mathematical, and mapping applications for studies requiring the use of sensitive data. Access to all SCO computing resources is permitted on an as needed, need-to-know basis only.

CNA maintains a data feed with SPAWAR to receive MPT&E data on a regular basis. CNA also maintains an MOU with BUPERS to receive PRIDE and a data feed with NETC to receive CETARS data on a regular basis. In addition to data received on a recurring basis CNA receives other types of data on a per project basis. All data requests are processed through BUPERS. All data is stored in a data archive on the SCO system.

SCO obtained a Navy DIACAP accreditation in Sept. 2012. It expires on August 27, 2015. The SCO IATS/eMASS number is: 18733. The ATO letter can be provided upon request.

Please contact Anne Brambora, Manager Scientific Computing Operations (703.824.2752, Brambora@cna.org) for further information regarding the SCO system. Due to CNA's working relationship with BUPERS, SCO falls under the BUPERS SORN: N01070-3.

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 purpose of Scientific Computing Operations (SCO) is to provide a secure environment for studies requiring the use of sensitive data, support for multiuser access to non-standarad scientific applications for project oriented analysis, and secure FTP services for the transfer of large datasets containing PHI/PII from CNA clients. The CNA SCO LAN supports Department of Defense (DoD), Navy, federal, non-DoD, and non-federal customers. The CNA SCO LAN components include a Windows Domain (application servers, SQL server, and administrative servers), thin clients, and a Virtual Private Network (VPN) that allows access to the information from outside the CNA facility. CNA SCO LAN provides multiple software applications which allow researchers to create deliverable content in accordance with contractual obligations. CNA SCO LAN contains both federal and DOD information.

PII collected: name, other name used, social security number (SSN), truncated SSN, driver license, DoD id number, citizenship, legal status, gender, race/ethnicity, birth date, place of birth, home/personal telephone number, personal email address, mailing/home address, religious preference, biometrics, security clearance, mother maiden name, mother middle name, military records, Spouse Information: military spouse, employment status and educational level; Child Information: number of children, age, and if there is an exceptional family member; Financial Information: Unemployment status of those who separate as related to financial situation; Medical Information: Active duty patient status, limited duty status, or medical discharge status; Disability Information: type of discharge; Law Enforcement Information: who enters with waivers for felonies, misdemeanors, incidents to include DUI, assault, sexual harassment; Employment Information: Unemployment status of veterans. Jobs veterans get and how much they are being paid compared to their military compensation – which may help to explain why they separated; and Education Information: educational level of the individual, such as attrition, retention, advancement, job performance.

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

The information is logically protected via Windows Active Directory, Group Policies, and Access Control Lists (ACL) which allow individuals to access information based on a need-to-know basis. Data includes Personally Identifiable Information (PII) and Private Health Information (PHI). SCO servers reside behind a second firewall permitting access from thin clients only. Access to SCO computing resources is on an as

needed, need to know basis. Users access the system with a domain username and password.

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. BUMED, BUPERS, as necessary to conduct statistical analysis.

☐ **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.

PII is not collected directly from the individual.

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.

PII is not collected directly from the individual.

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.

PII is not collected directly from the individual.

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.