PRIVACY IMPACT ASSESSMENT (PIA)

For the

Navy Enterprise Resource Planning (Navy ERP)
Department of the Navy - SPAWAR

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 802

☐ **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 007-17-01-03-01-0186-00

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 N07220-1, N01080-1, N01080-2, DPR 34, T7335

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.

5 U.S.C. 301, Departmental Regulations; 5 U.S.C. 7201, Antidiscrimination Policy; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. 5013, Secretary of the Navy; Executive Order 9830, Amending the Civil Service Rules and Providing for Federal Personnel Administration, as amended; Executive Order 9397 (SSN), as amended; DoD Initiatives: Sea Power 21, Business Management Modernization Program (BMMP), and Enterprise Software Initiative (ESI); Naval Network Warfare Command (NETWARCOM) granted approval to operate (ATO) on 1 August 2007.

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 Navy Enterprise Resource Planning (ERP) system provides a standard set of tools to Navy organizations that will facilitate business process re-engineering and provide interoperable data elements for acquisition, financial, and supply chain operations. The Navy ERP system provides an integrated means for planning, acquiring, and managing personnel, financial and material resources. In addition to providing tools for managing the acquisition and financial record keeping of purchasing necessary equipment and supplies, Navy ERP facilitates Navy personnel's ability to manage their training and enables Navy personnel to ensure appropriate accommodations are made in determining work assignments. For example, ensuring proper berthing accommodations on Navy vessels requires knowledge of our personnel's gender, just as knowledge of any physical disability is necessary to ensure appropriate accommodations in an office setting. Navy ERP is a major component of the Navy's Global Combat Support System (GCSS) and will provide a critical link between operating forces and the support echelons.

The Navy ERP system does not collect any information directly from the general public, though we continue to make miscellaneous disbursements to individuals with whom the Navy has a legal relationship, such as owing royalty payments. If such payments are due, DFAS requires that these payments are certified within Navy ERP by authorized individuals at the respective Command. Once the certification is complete the identifying information, such as name and SSN or Tax Identification Number are sent to DFAS for disbursement. However, Section 1, question a., of the Privacy Impact Assessment template, requires us to choose answer 3 because we do collect information from foreign national personnel working at Navy facilities, such as time and attendance information.

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

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

b) All systems are vulnerable to "insider threats". The Navy ERP Information Assurance Manager (IAM) and Navy ERP Information Assurance Officers (IAO) along with the responsible Commands Information Assurance/Security personnel are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. Navy ERP has defined criteria to identify who should have access to the information resident in the Navy ERP system. These individuals are required have gone through extensive background and employment investigations.

c) The residual privacy risks regarding the collection, use, and sharing of PII is LOW. Navy ERP consolidates, improves and accelerates existing processes. Extraneous PII is not collected and, by reducing the number of redundant systems and copies of PII, over-all privacy risks are reduced.

d) Navy ERP reduces over-all risk through the adoption of state-of-the-practice security measures, which have been designed to meet the most current Information Assurance issuances. By modernizing processes, consolidating data stores, and replacing aging security controls (many of which were deployed in accordance with Information Assurance requirements that are now superseded), the Navy ERP system will lower over-all risk to existing and future PII records.

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 personnel with an official need to know.

☒ **Other DoD Components.**

Specify. Defense Finance and Accounting Service personnel and non-Navy military personnel with an official need to know.

☐ **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.

a. In cases where Navy ERP collects information from other systems, those systems already have offered individuals the option to object to the collection of information about themselves, or to consent to such collection.

b. All Navy ERP users are required to complete a SAAR-N (System Access Authorization Request Navy). The SAAR-N includes a Privacy Act notification which provides the account requestor with the opportunity to concur or not with the terms of the Privacy Act notification. Requestor signature indicates consent with the terms. No signature indicates objection to collection of their PII.

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

N/A

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.

Navy ERP does not collect PII directly from the individual other than time and attendance records. Navy ERP collects large data files from existing DoD and DON systems for business purposes, 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.

a. In cases where Navy ERP collects information from other systems, it is assumed that those systems already have offered individuals the option to object to the collection of information about themselves, or to consent to such collection.

b. All Navy ERP users are required to complete a SAAR-N. The SAAR-N includes a Privacy Act Statement which provides the account requestor with the opportunity to concur or not with the terms of the Privacy Act notification. Account requestor determines if they want to supply PII in the appropriate blocks. However, lack of certain identifying information may impede, delay or prevent the establishment of an account. Requestor signature indicates consent with the terms. Without signature, the requester would not be able to establish an account.

c. The Navy ERP system displays the following Privacy Act Statement: Information on these pages are subject to the Privacy Act of 1974, as amended.

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.