PRIVACY IMPACT ASSESSMENT (PIA)

For the

Knowledge Management System (KMS)
Department of the Navy - COMOPTEVFOR

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	DADMS ID: 92107
☐	**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 DPR 39

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. 136, Under Secretary of Defense for Personnel and Readiness
10 U.S.C. 3013, Secretary of the Army
10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 8013, Secretary of the Air Force
DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural or Man-madeDisasters
Air Force Instruction 10-218, Personnel Accountability in conjunction with Natural Disasters or National Emergencies
Army Regulation 500-3, U.S. Army Continuity of Operations Program Policy and Planning
E.O. 9397(SSN), as amended.

Other authorities:

COMOPTEVFORINST3120 (SORM)

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.

KMS, a web based system, contains personally identifiable information (PII) within several modules of the application however provides controlled role-based access to the PII and other sensitive unclassified information to personnel assigned to COMOPTEVFOR. Authorized users must have a Common Access Card (CAC) to access the system via the web. Once authenticated, users receive privileges for the various modules of the KMS system based upon their assigned role and level of access permissions granted by the Administrator. Upon access, users make queries and updates via the application server to the database server. Users are not granted direct access to the database server.

Personal information collected: Name, Other Names Used, DoD ID Number, Citizenship, Gender, Birth Date, Place of Birth, Personal Cell Telephone Number, Home Telephone Number, Mailing/Home Address, Security Clearance, Marital Status, Spouse Information: Name; Child Information: Number of Children; Employment Information: Employment History/Resume; Education Information: Highest degree obtained and Science, Technology engineering and/or math (STEM) category.

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

A system of controls implemented and Privacy Act Statement displayed at PII sensitive areas and access restricted by password. Access only granted by Privacy/PII officer, CSM, ISSM, CO and CoS by rotating password. General personnel cannot access this information without approval even in emergency (suicide, amcross, etc). situations.

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. COMOPTEVFOR; CNO; NCIS

☐ **Other DoD Components.**

Specify.

☒ **Other Federal Agencies.**

Specify. DOT&E; Federal Law Enforcement as applicable

☐ **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.

By not completing the information form or via face to face. When information is originally requested from the member that is their opportunity to object to their information being collected.

The information is collected for command recall, suicide awareness and potential (military) personnel action reviews. Completely voluntary for civilians and military. They are not punished for not completing/refusing to provide their information.

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

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.

When PII information is used it is because a member is requesting that a specific military form be completed, for example, the individual's Page 2 (PG2), etc. Therefore, they have the opportunity to tell us if we can or cannot use their information. However, in emergency situations (i.e., inclement weather) we don't ask the member if we can utilize their information before the event. Service members may lose BAH/BAQ housing or other specific military benefits. This information is also collected for personnel recall, suicide awareness, natural disaster preparation, etc. to provide to appropriate first responders that can provide assistance.

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.	On the bottom of the form utilized to collect information to be put into the system the 'Privacy Act Statement' is attached as well as a cover sheet.

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.