



## PRIVACY IMPACT ASSESSMENT (PIA)

For the

Tasking, Records and Consolidated Knowledge Enterprise (DON TRACKER)

Department of the Navy - SPAWAR - PMW 240

### **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: 16286	DITRP DON ID: 22792
-----------------	---------------------
- 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: 007-000007179
--------------------

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

DMDC 02 DOD; DMDC 12 DOD; N07220-1
------------------------------------

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:

DMDC 02 DOD

5 U.S.C. App. 3, Inspector General Act of 1978; 5 U.S.C. Chapter 90, Federal Long-Term Care Insurance; 10 U.S.C. 136, Under Secretary of Defense for Personnel and Readiness; 10 U.S.C. Chapter 53, Miscellaneous Rights and Benefits; 10 U.S.C. Chapter 54, Commissary and Exchange Benefits; 10 U.S.C. Chapter 58, Benefits and Services for Members being Separated or Recently Separated; 10 U.S.C. Chapter 75, Deceased Personnel; 10 U.S.C. 2358, Research and Development Projects; 10 U.S.C. Chapter 49, Section 987, Terms of Consumer Credit Extended to Members and Dependents; 20 U.S.C. 1070a (f)(4), Higher Education Opportunity Act; 31 U.S.C. 3512(c), Executive Agency Accounting and Other Financial Management Reports and Plans; 42 U.S.C. 18001 note, Patient Protection and Affordable Care Act (Public Law 111-148); 42 U.S.C. 1973ff, Federal Responsibilities; 50 U.S.C. Chapter 23, Internal Security; 50 U.S.C. 501, Servicemember Civil Relief Act; DoD Directive 1000.04, Federal Voting Assistance Program (FVAP); DoD Directive 1000.25, DoD Personnel Identity Protection (PIP) Program; DoD Instruction 1015.9, Professional United States Scouting Organization Operations at United States Military Installations Located Overseas; DoD Instruction 1100.13, DoD Survey; DoD Instruction 1241.03 TRICARE Retired Reserve (TRS) Program; DoD Instruction 1241.04, TRICARE Reserve Select (TRS) Program; DoD Instruction 1336.05, Automated Extract of Active Duty Military Personnel Records; DoD Instruction 1341.2, Defense Eligibility Enrollment Reporting System (DEERS)

Procedures; DoD Instruction 3001.02, Personnel Accountability in Conjunction with Natural or Manmade Disasters; Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors; DoD Instruction 7730.54, Reserve Components Common Personnel Data System (RCCPDS); 38 CFR part 9.20, Traumatic injury protection; 38 U.S.C. Chapter 19, Subchapter III, Servicemembers' Group Life Insurance; 42 U.S.C. 18001 note, Patient Protection and Affordable Care Act (Public Law 111-148); and E.O. 9397 (SSN), as amended.

DMDC 12 DOD

5 U.S.C. 9101, Access to Criminal History Information for National Security and Other Purposes; 10 U.S.C. 137, Under Secretary of Defense for Intelligence; DoD Directive 1145.02E, United States Military Entrance Processing Command (USMEPCOM); DoD 5200.2R, DoD Personnel Security Program (PSP); DoD 5105.21, Sensitive Compartment Information Administrative Security Manual; DoD Instruction (DoDI) 1304.26, Qualification Standards for Enlistment, Appointment and Induction; DoDI 5200.02, DoD Personnel Security Program (PSP); DoDD 5220.6, Defense Industrial Personnel Security Clearance Review Program; DoDI 5220.22, National Industrial Security Program (NISP); Homeland Security Presidential Directive (HSPD) 12, Policy for Common Identification Standard for Federal Employees and Contractors; and E.O. 9397 (SSN), as amended.

N07220-1

10 U.S.C. 5013, Secretary of the Navy and 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.

The Department of the Navy Tasking, Records and Consolidated Knowledge Enterprise Repository (DON TRACKER) will streamline DON's electronic records and task management processes under a consolidated enterprise solution and will enable the DON to capture unstructured and structured electronic records, seamlessly manage tasking across and within all commands, ensure uniform metadata of content, provide workflow-enabled reporting, and aid in compliance with all applicable laws, policies, and regulations. In addition, this will eliminate duplicative capabilities and result in cost-saving opportunities and efficiencies. The DON TRACKER solution will be extended to all authorized, shore-based users across the DON enterprise, including the Continental United States (CONUS) and Outside the Continental United States (OCONUS) communities. This will address the following issues: Currently, the DON lacks standard records management (RM) processes across all directorates and commands; compliance with Federal and Departmental RM mandates is inconsistent; task management (TM) across the DON is not integrated across directorates and commands; decentralized processes have reduced organizational effectiveness; implementation of DON RM and TM programs does not provide a seamless approach for managing activities, resulting in low process efficiencies resulting in duplication of effort, excess costs, non-compliance with laws, policies, regulations and standards, long and protracted process cycle times, and sub-optimal decision making due to lack of visibility of available information - all of which results in difficulties with implementing policy and guidance across the DON. The DON lacks a true lifecycle RM capability from creation through disposition. The current DON infrastructure includes multiple, non-integrated TM systems that lack the ability to edit documents in place, lack transparency, and lack integration with other TM systems and the existing RM system.

Structured personal information collected:

Name, Work Email, Work Phone

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

Potential threats/risks that may impact the integrity, availability, and confidentiality of the DON TRACKER

system includes individual users mishandling of data and firewall issues. Mitigations include: DoD PKI certificates are used for server and client authentication. Logins to the web page are controlled by the application. User authentication and role-based authorization are implemented to grant access to DON TRACKER. All external communications to the web server are protected by an external firewall, host address block / allow lists and HyperText Transfer Protocol (HTTP) of Secure Sockets Layer (SSL) encryption. An outer firewall interface will require HTTP of SSL opened inbound to the web servers. System logins are limited, in general, to administrators and developers. The DON TRACKER production database server resides within the Data Center's Production Private Access Zone of the EDMZ - providing another level of security.

**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.

Unstructured personal information: established access controls and permissions

**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.

N00039-14-C-0108, DFAR 5252.237-9603 Clause(s) The contractor shall ensure all guidelines for the protection of Privacy Act (PA) Data and the safeguarding of Personally Identifiable Information (PII) are followed.

The contractor shall ensure all technical data rights and source code developed under this task order ultimately becomes property of the government upon completion of the task order.

Federal Acquisition Regulation (FAR) privacy clauses are documented in the base contract

**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.

In order to use DON Tracker the user must log in using their CAC.

**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.

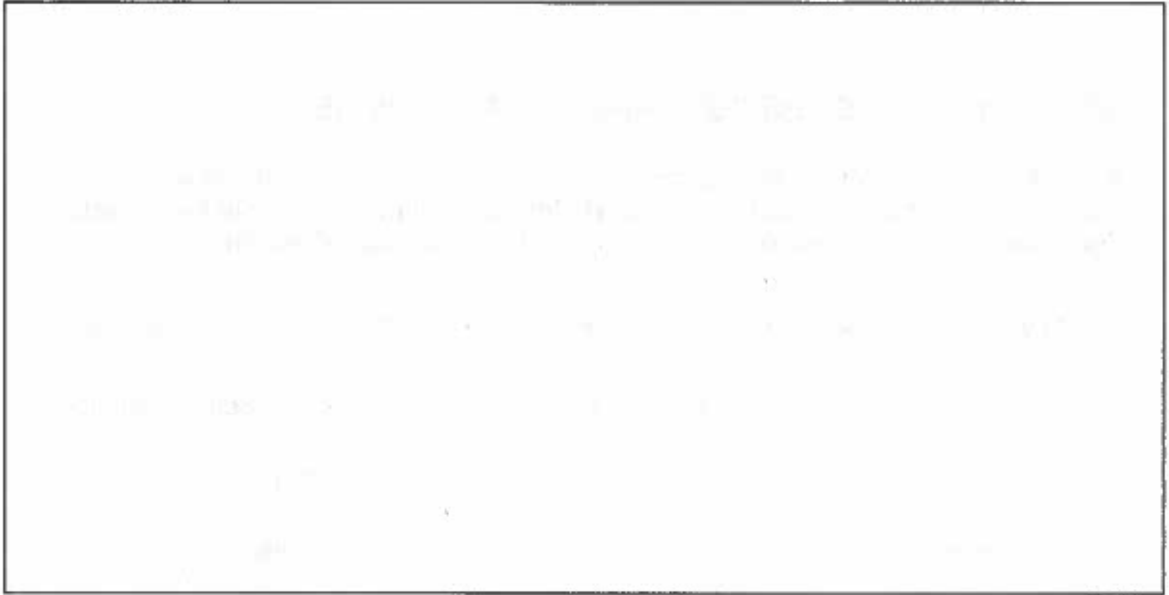
(2) If "No," state the reason why individuals cannot give or withhold their consent.

In order to use DON Tracker the user must log in using their CAC.

**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.



**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.**