PRIVACY IMPACT ASSESSMENT (PIA)

PRESCRIBING AUTHORITY: DoD Instruction 5400.16, "DoD Privacy Impact Assessment (PIA) Guidance". Complete this form for Department of Defense (DoD) information systems or electronic collections of information (referred to as an "electronic collection" for the purpose of this form) that collect, maintain, use, and/or disseminate personally identifiable information (PII) about members of the public, Federal employees, contractors, or foreign nationals employed at U.S. military facilities internationally. In the case where no PII is collected, the PIA will serve as a conclusive determination that privacy requirements do not apply to system.

1. DOD INFORMATION SYSTEM/ELECTRONIC COLLECTION NAME:
   Tasking, Records, and Consolidated Knowledge Enterprise (DON TRACKER)

2. DOD COMPONENT NAME:
   Department of the Navy

3. PIA APPROVAL DATE:

PEO EIS PMW 250-(SPAWAR)

SECTION 1: PII DESCRIPTION SUMMARY (FOR PUBLIC RELEASE)

a. The PII is: (Check one. Note: foreign nationals are included in general public.)
   - From members of the general public
   - From both members of the general public and Federal employees and/or
     Federal contractors
   - From Federal employees and/or Federal contractors
   - Not Collected (if checked proceed to Section 4)

b. The PII is in a: (Check one)
   - New DoD Information System
   - Existing DoD Information System
   - Existing Electronic Collection
   - Significantly Modified DoD Information System

Don Tracker will streamline DON's electronic records and task management processes under a consolidated enterprise solution. Personal information collected from system users: Name, Work Email, Work Phone, DoD ID.

c. Describe the purpose of this DoD information system or electronic collection and describe the types of personal information about individuals collected in the system.

Don Tracker will streamline DON's electronic records and task management processes under a consolidated enterprise solution. Personal information collected from system users: Name, Work Email, Work Phone, DoD ID.

Information from user CAC is collected for verification and authentication.

d. Why is the PII collected and/or what is the intended use of the PII? (e.g., verification, identification, authentication, data matching, mission-related use, administrative use)
   - Information from user CAC is collected for verification and authentication

(1) If "Yes," describe the method by which individuals can object to the collection of PII.

(2) If "No," state the reason why individuals cannot object to the collection of PII.

In order to use DON TRACKER, users must login using their CAC.

f. 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, users must login using their CAC.

g. When an individual is asked to provide PII, a Privacy Act Statement (PAS) and/or a Privacy Advisory must be provided. (Check as appropriate and provide the actual wording.)
   - Privacy Act Statement
   - Privacy Advisory
   - Not Applicable

h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component? (Check all that apply)
   - Within the DoD Component
   - SECNAV, HQUSMC, ECH I and ECH II commands

DD FORM 2930, JUN 2017
PREVIOUS EDITION IS OBSOLETE.
Other DoD Components
Specify.

Other Federal Agencies
Specify.

State and Local Agencies
Specify.

Contractor (Name of contractor and describe the language in the contract that safeguards PII. Include whether FAR privacy clauses, i.e., 52.224-1, Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 are included in the contract.)
Progeny Systems Corp. DFAR 5222.237-9603 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.

State and Local Agencies
Specify.

Other (e.g., commercial providers, colleges).
Specify.

i. Source of the PII collected is: (Check all that apply and list all information systems if applicable)

- Individuals
- Existing DoD Information Systems
- Commercial Systems
- Other Federal Information Systems

j. How will the information be collected? (Check all that apply and list all Official Form Numbers if applicable)

- E-mail
- Face-to-Face Contact
- Fax
- Information Sharing - System to System
- Other (If Other, enter the information in the box below)

k. 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 must be consistent.

- Yes
- No

If "Yes," enter SORN System Identifier

DMDC 02 DOD; DMDC 12 DOD; N0722

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpclrd.defense.gov/Privacy/SORNs/
or

If a SORN has not yet been published in the Federal Register, enter date of submission for approval to Defense Privacy, Civil Liberties, and Transparency Division (DPCLTD). Consult the DoD Component Privacy Office for this date

If "No," explain why the SORN is not required in accordance with DoD Regulation 5400.11-R: Department of Defense Privacy Program.

l. What is the National Archives and Records Administration (NARA) approved, pending or general records schedule (GRS) disposition authority for the system or for the records maintained in the system?

(1) NARA Job Number or General Records Schedule Authority

ALL
(2) If pending, provide the date the SF-115 was submitted to NARA.

(3) Retention Instructions.

DON TRACKER is the Electronic Records Management System replacing HPE RM (formerly known as TRIM).

m. What is the authority to collect information? A Federal law or Executive Order must authorize the collection and maintenance of a system of records. For PII not collected or maintained in a system of records, the collection or maintenance of the PII must be necessary to discharge the requirements of a statute or Executive Order.

(1) If this system has a Privacy Act SORN, the authorities in this PIA and the existing Privacy Act SORN should be similar.

(2) If a SORN does not apply, 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) Cite the specific provisions of the statute and/or EO that authorizes the operation of the system and the collection of PII.

(b) If direct statutory authority or an Executive Order does not exist, indirect statutory 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) If direct or indirect authority does not exist, 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 must be identified.


n. Does this DoD information system or electronic collection have an active and approved Office of Management and Budget (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  X No  ☐ Pending

(1) If "Yes," list all applicable OMB Control Numbers, collection titles, and expiration dates.
(2) If "No," explain why OMB approval is not required in accordance with DoD Manual 8910.01, Volume 2, "DoD Information Collections Manual: Procedures for DoD Public Information Collections."
(3) If "Pending," provide the date for the 60 and/or 30 day notice and the Federal Register citation.

Per DoD Manual 8910.01 Volume 2 paragraph 2, this volume does not apply because information is not collected from members of the public.
### SECTION 2: PII RISK REVIEW

**a. What PII will be collected** *(a data element alone or in combination that can uniquely identify an individual)* *(Check all that apply)*

<table>
<thead>
<tr>
<th>PII Type</th>
<th>✔</th>
<th>☐</th>
</tr>
</thead>
<tbody>
<tr>
<td>Biometrics</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Citizenship</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Driver's License</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Employment Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Home/Cell Phone</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Mailing/Home Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Military Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Official Duty Address</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Passport Information</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Place of Birth</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Race/Ethnicity</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Records</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Work E-mail Address</td>
<td>✔</td>
<td></td>
</tr>
</tbody>
</table>

Name, DoD ID, Work Email, and Work phone are collected for authentication and verification and authentication. The system may store any or all types depending on the records placed into the system.

If the SSN is collected, complete the following questions.

*(DoD Instruction 1000.30 states that all DoD personnel shall reduce or eliminate the use of SSNs wherever possible. SSNs shall not be used in spreadsheets, hard copy lists, electronic reports, or collected in surveys unless they meet one or more of the acceptable use criteria.)*

1. Is there a current *(dated within two (2) years)* DPCLTD approved SSN Justification on Memo in place?
   - Yes ☐ No ✔
   - If “Yes,” provide the signatory and date approval. If “No,” explain why there is no SSN Justification Memo.

2. The system does not use SSN for access nor is the SSN retrievable by unique identifier.

3. Describe the approved acceptable use in accordance with DoD Instruction 1000.30 “Reduction of Social Security Number (SSN) Use within DoD”.

   **Other Cases- unstructured data is entered and collected via legacy interfaces and emails**

4. Describe the mitigation efforts to reduce the use including visibility and printing of SSN in accordance with DoD Instruction 1000.30, “Reduction of Social Security Number (SSN) Use within DoD”.

   **Only personnel with a required "Need to know" have access to the view records stored as a repository and are limited by Role based permission per UIC and Command level access.**

5. Has a plan to eliminate the use of the SSN or mitigate its use and or visibility been identified in the approved SSN Justification request?
   - Yes ☐ No ✔
   - If “Yes,” provide the unique identifier and when can it be eliminated?
   - If “No,” explain.

   The system does not require the use of SSN or structured fields for SSN full or truncated. The 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.

**b. What is the PII confidentiality impact level?**

<table>
<thead>
<tr>
<th>Level</th>
<th>✔</th>
<th>☐</th>
<th>☐</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Moderate</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>✔</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

Guidance on determining the PII confidentiality impact level, see Section 2.5 “Categorization of PII Using NIST SP 800-122.” Use the identified PII confidentiality impact level to apply the appropriate Privacy Overlay low, moderate, or high. This activity may be conducted as part of the categorization exercise that occurs under the Risk Management Framework (RMF). Note that categorization under the RMF is typically conducted using the information types described in NIST Special Publication (SP) 800-60, which are not as granular as the PII data elements listed in the PIA table. Determining the PII confidentiality impact level is most effective when done in collaboration with the Information Owner, Information System Owner, Information System Security Manager, and representatives from the security and privacy organizations, such as the Information System Security Officer (ISSO) and Senior Component Official for Privacy (SCOP) or designees.

c. How will the PII be secured?

(1) Physical Controls. (Check all that apply)

- Cipher Locks
- Combination Locks
- Key Cards
- Security Guards
- Closed Circuit TV (CCTV)
- Identification Badges
- Safes
- If Other, enter the information in the box below

(2) Administrative Controls. (Check all that apply)

- Backups Secured Off-site
- Encryption of Backups
- Methods to Ensure Only Authorized Personnel Access to PII
- Periodic Security Audits
- Regular Monitoring of Users’ Security Practices
- If Other, enter the information in the box below

(3) Technical Controls. (Check all that apply)

- Biometrics
- Encryption of Data at Rest
- Firewall
- Role-Based Access Controls
- Virtual Private Network (VPN)
- Command Access Card (CAC)
- Encryption of Data in Transit
- Intrusion Detection System (IDS)
- Used Only for Privileged (Elevated Roles)
- If Other, enter the information in the box below

Access is controlled and PII/Privacy Act Data is only available to those specifically authorized in writing by an authorized officer and have a valid "need to know”

d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?
SECTION 3: RELATED COMPLIANCE INFORMATION

a. Is this DoD Information System registered in the DoD IT Portfolio Repository (DITPR) or the DoD Secret Internet Protocol Router Network (SIPRNET) Information Technology (IT) Registry or Risk Management Framework (RMF) tool?

- [x] Yes, DITPR
- [ ] Yes, SIPRNET
- [ ] Yes, RMF tool
- [ ] No

If "No," explain.

DITPR DON ID: 22792

DITPR ID: 16286

b. DoD information systems require assessment and authorization under the DoD Instruction 8510.01, “Risk Management Framework for DoD Information Technology”.

Indicate the assessment and authorization status:

- [x] Authorization to Operate (ATO) Date Granted: 8/15/2018
- [ ] ATO with Conditions Date Granted: 
- [ ] Denial of Authorization to Operate (DATO) Date Granted: 
- [ ] Interim Authorization to Test (IATT) Date Granted: 

(1) If an assessment and authorization is pending, indicate the type and projected date of completion.

(2) If an assessment and authorization is not using RMF, indicate the projected transition date.

c. Does this DoD information system have an IT investment Unique Investment Identifier (UII), required by Office of Management and Budget (OMB) Circular A-11?

- [x] Yes
- [ ] No

If "Yes," Enter UII 007-000007179

If unsure, consult the component IT Budget Point of Contact to obtain the UII.

3Guidance on Risk Management Framework (RMF) tools (i.e., eMASS, Xacta, and RSA Archer) are found on the Knowledge Service (KS) at https://rmfks.osd.mil.
Completion of the PIA requires coordination by the program manager or designee through the information system security manager and privacy representative at the local level. Mandatory coordinators are: Component CIO, Senior Component Official for Privacy, Component Senior Information Security Officer, and Component Records Officer.

<table>
<thead>
<tr>
<th>a. Program Manager or Designee Name</th>
<th>(1) Title</th>
<th>Michael Perozziello</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>(3) Work Telephone</td>
<td>PEO EIS PMW 250</td>
</tr>
<tr>
<td>(4) DSN</td>
<td>(5) E-mail address</td>
<td>202-433-8939</td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td>(7) Signature</td>
<td><a href="mailto:michael.perozziello@navy.mil">michael.perozziello@navy.mil</a></td>
</tr>
</tbody>
</table>

b. Other Official (to be used at Component discretion)

<table>
<thead>
<tr>
<th>(1) Title</th>
<th>Assistant Program Manager - Engineering</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>PEO EIS PMW 250</td>
</tr>
<tr>
<td>(4) DSN</td>
<td>202-433-8942</td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td>THOMAS.ROBER</td>
</tr>
<tr>
<td>(7) Signature</td>
<td>T.W.1282744917</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(1) Title</th>
<th>Assistant Program Manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>Office of the Chief of Naval Operations (CNO)</td>
</tr>
<tr>
<td>(4) DSN</td>
<td>202-685-6545</td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td>PATTERSON.ROBIN.W.1229323403</td>
</tr>
<tr>
<td>(7) Signature</td>
<td>Date: 2019.01.25 09:28:55 -05'00'</td>
</tr>
<tr>
<td>e. Component Records Officer</td>
<td>Jennifer M. Acevedo</td>
</tr>
<tr>
<td>------------------------------</td>
<td>--------------------</td>
</tr>
<tr>
<td>(2) Organization</td>
<td>SPAWARSYSCOM</td>
</tr>
<tr>
<td>(4) DSN</td>
<td>537-0333</td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td>09/18/18</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>f. Component Senior Information Security Officer or Designee Name</th>
<th>Danny K Cain</th>
<th>(1) Title</th>
<th>CSPM/ISSM</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>PEO EIS PMW 250</td>
<td>(3) Work Telephone</td>
<td></td>
</tr>
<tr>
<td>(4) DSN</td>
<td>647-1521</td>
<td>(5) E-mail address</td>
<td><a href="mailto:danny.cain@navy.mil">danny.cain@navy.mil</a></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td>10/15/18</td>
<td>(7) Signature</td>
<td>CAIN.DANNY.K.1085340626 Digitally signed by CAIN.DANNY.K.1085340626 Date: 2018.10.15 14:23:45 -04'00'</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>g. Senior Component Official for Privacy (SCOP) or Designee Name for CAPT Damen Hofheinz</th>
<th>Director, OCIO</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>Office of the Chief Information Officer (OCIO)</td>
</tr>
<tr>
<td>(4) DSN</td>
<td></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td></td>
</tr>
<tr>
<td>(7) Signature</td>
<td>MUCK.STEVEN.ROBERT.11794888597 Digitally signed by MUCK.STEVEN.ROBERT.11794888597 Date: 2019.01.28 10:37:44 -05'00'</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>h. Component CIO Reviewing Official Name for CAPT Damen Hofheinz</th>
<th>Director, OCIO</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>Office of the Chief Information Officer (OCIO)</td>
</tr>
<tr>
<td>(4) DSN</td>
<td></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td></td>
</tr>
<tr>
<td>(7) Signature</td>
<td>MUCK.STEVEN.ROBERT.11794888597 Digitally signed by MUCK.STEVEN.ROBERT.11794888597 Date: 2019.01.28 10:38:08 -05'00'</td>
</tr>
</tbody>
</table>

**Publishing:** Only Section 1 of this PIA will be published. Each DoD Component will maintain a central repository of PIAs on the Component's public Web site. DoD Components will submit an electronic copy of each approved PIA to the DoD CIO at: osd.mc-alex.dod-cio.mbx.pia@mail.mill.

If the PIA document contains information that would reveal sensitive information or raise security concerns, the DoD Component may restrict the publication of the assessment to include Section 1.