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:
Total Force Retention System (TFRS)

2. DOD COMPONENT NAME:
Department of the Navy

3. PIA APPROVAL DATE:
12/06/18

United States Marine Corps - MCSC

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
   - Not Collected (if checked proceed to Section 4)
   - From Federal employees and/or Federal contractors

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

   TFRS integrates workflow and information on personnel retention requirements. The purpose of the system is to track and monitor career planning for reenlistment, extension, lateral moves, overseas extensions, and special duty assignments of personnel. TFRS assists in overall recruitment goals and assignments.

   The type of personal information about a Marine collected in TFRS includes: Name, SSN (full and truncated), citizenship, legal status, gender, race/ethnicity, birth date, place of birth, security clearance, spouse information, marital status, financial information, medical information, law enforcement information, military records, education information

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)

   Identification. HQMC has mandated that the primary purpose of TFRS is to support the Career Retention Force's mission to systematically input, review, and maintain personnel information needed to process a Reenlistment, Lateral Move, or to extend current enlistments (RELM) of both the Active Duty and Reserve components of the Marine Corps. In order to accomplish this, TFRS must have access to PII for identification purposes.

   PII is not collected directly from the individual.

f. Do individuals have the opportunity to object to the collection of their PII?
   - Yes
   - No

   (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.

PII is not collected directly from the individual.
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  ☑

PII is not collected directly from the individual.

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
☐ Other DoD Components
☐ Other Federal Agencies
☐ State and Local Agencies

<table>
<thead>
<tr>
<th>Specify.</th>
<th>Marine Corps Total Force System (MCTFS)</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Specify.</td>
</tr>
<tr>
<td></td>
<td>Specify.</td>
</tr>
<tr>
<td></td>
<td>Specify.</td>
</tr>
<tr>
<td>SAIC - Contractors sign a Non Disclosure Agreement (NDA) to assure confidentiality between the contractor and government to protect any type of confidential and proprietary information. Specific language in the contract is described as: Security measures shall be taken to satisfy the security requirements in accordance with the Marine Corps System Security Plan. TFRS data/information shall be protected from an Information Systems Security (INFOSEC) perspective. The contractor shall apply security considerations to software design and management. Only contractors who have a valid need to know and a favorably adjudicated background investigation are permitted to have access to TFRS. During the course of routine system maintenance contractors may be exposed to PII. Users are DoD employees or authorized contractors supporting the DoD. Present contract does not contain the FAR privacy contracts, but informed contracts the clauses must be included in all contracts where systems containing are concerned. Contracting office stated that the FAR privacy clauses, 52.224-1; Privacy Act Notification, 52.224-2, Privacy Act, and FAR 39.105 will be included in the new awarded contract TCSI II. The new contract starts the end of January 2019.</td>
<td></td>
</tr>
</tbody>
</table>

☐ 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
☐ Databases
☑ 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
 ☑ Information Sharing - System to System
☐ Official Form (Enter Form Number(s) in the box below)
☐ Paper
☐ Telephone Interview
☐ Website/E-Form
☐ Fax
☐ Other (If Other, enter the information in the box below)
Marine Corps total Force System (MCTFS)

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 M01040-3

SORN Identifier, not the Federal Register (FR) Citation. Consult the DoD Component Privacy Office for additional information or http://dpclid.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. N1-127-09-7

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

(3) Retention Instructions.

NARA retention and disposition instructions have been received, which states that all records are temporary and must be destroyed four years after separation or discharge. Functionality has been implemented within TFRS to fully comply with NARA instructions. An individual Marine's RELM is protected from the time the RELM is created to the time it is destroyed. The electronic records are stored on hardware that is physically protected by cipher locked doors, limited access by authorized personnel, and access controlled during normal and after hours. The processing of documents into a Marine's RELM is controlled through the Privacy Act and the rules and regulations covering PII. Documents received electronically are protected by the means in which the data is transferred, primarily through secure e-mail or through secure file transfer protocol (SFTP). Users of TFRS who review, approve, or provide input to the RELM are required to sign a Privacy Act Statement and have reviewed/completed the current PII training. In addition each authorized user is given a user identification to utilize TFRS, again this is only done after the Privacy Act and PII training has been completed.

SSIC-1040.4

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.

SORN M01040-3, Marine Corps Manpower Management Information System Records (April 29, 2010, 75 FR 22570), authorities:

10 U.S.C. 5013, Secretary of the Navy
10 U.S.C. 5041, Headquarters, Marine Corps
10 U.S.C. 1074f, Medical Tracking System for Members Deployed Overseas
32 CFR 64.4, Management and Mobilization
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  ☒ 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.

Information is not collected from members of the public. Information is not collected directly from the individual.
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)

- [ ] Biometrics
- [X] Citizenship
- [ ] Driver's License
- [ ] Employment Information
- [X] Home/Cell Phone
- [X] Mailing/Home Address
- [X] Military Records
- [ ] Official Duty Address
- [ ] Passport Information
- [X] Place of Birth
- [X] Race/Ethnicity
- [ ] Records
- [X] Work E-mail Address
- [ ] Birth Date
- [X] Disability Information
- [ ] Education Information
- [X] Financial Information
- [X] Law Enforcement Information
- [ ] Marital Status
- [ ] Mother's Middle/Maiden Name
- [X] Official Duty Telephone Phone
- [ ] Personal E-mail Address
- [X] Position/Title
- [X] Rank/Grade
- [ ] Security Information
- [ ] Social Security Number (SSN) (Full or in any form)

Financial Information: basic payroll information, annual bonus, etc.
Medical Information: general medical records to include initial entry physical exam, regular annual exams, etc.
Law Enforcement Information: basic background information from local law enforcement in the entrance screening, records of warrants, arrests, etc.
Education Information: college and service school data.
Military Records: Rank, Military Occupational Specialty (MOS), unit name and address, date of rank, future duty station name and address, home of record address or other additional address if taking leave en route to the new duty station, enlistment data, reserve enlistment and drill data and training data.
Spouse Information: Military spouse DOD ID

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?
- [X] Yes
- [ ] No

If "Yes," provide the signatory and date approval. If "No," explain why there is no SSN Justification Memo.

SIGNATORY: Paul Dexter Bennett (M&RA, HQMC) signed: 20180910

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

Legacy System Interface. DoD INSTR 1000.30 - Until such time as the USMC's personnel systems, namely MCTFS and ODSE, utilize a new identifier for personnel such as DoD ID Number, or the system is replaced by a follow-on system, TFRS will require the use of SSNs as the unique identifier.

(3) 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".

TFRS temporarily stores the full SSN in its database. However, as an added privacy measure, the system only displays the SSN when entered by the user. SSN has been replaced by DoD ID Number on reports and search features.

(4) 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
- [X] No

If "Yes," provide the unique identifier and when can it be eliminated?
If "No," explain.

SSN will continue to be required until all legacy systems that TFRS interface way create and or accept a new identifier for identification of individuals

b. What is the PII confidentiality impact level?
- [ ] Low
- [ ] Moderate
- [X] High
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)

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

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

- [x] Backups Secured Off-site
- [ ] Encryption of Backups
- [x] Methods to Ensure Only Authorized Personnel Access to PII
- [x] Periodic Security Audits
- [x] 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
- [x] Firewall
- [x] Role-Based Access Controls
- [x] Virtual Private Network (VPN)
- [x] Common Access Card (CAC)
- [x] Encryption of Data in Transit
- [x] Intrusion Detection System (IDS)
- [x] Used Only for Privileged (Elevated Roles)
- [ ] If Other, enter the information in the box below
- [x] DoD Public Key Infrastructure Certificates
- [ ] External Certificate Authority Certificates
- [x] Least Privilege Access
- [x] User Identification and Password
- [ ] If Other, enter the information in the box below

**d. What additional measures/safeguards have been put in place to address privacy risks for this information system or electronic collection?**

The mitigation consist of TFRS enforcing access controls to limit access and/or specific functional areas to protect sensitive data. This includes controlling access to TFRS by using identification and authentication mechanisms e.g., user IDs and passwords or Common Access Card (CAC), discretionary access control, and auditing. TFRS audits will include review and examination of records, activities, and system parameters, to assess the adequacy of maintaining, managing and controlling events that may degrade the security posture of the system. TFRS confidentiality and integrity ensures that data is not made available or disclosed to unauthorized individuals, entities, or processes as well as the data not being altered or destroyed in an unauthorized manner.

Server location: MCEITS Kansas City is 2306 East Bannister Road, Kansas City, MO 22134
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
- [x] Yes, RMF tool
- [ ] No

If "No," explain.

DITPR DON ID: 5797

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: 2/2/2016
- [ ] ATO with Conditions Date Granted: 
- [ ] Denial of Authorization to Operate (DATO) Date Granted: 
- [ ] Interim Authorization to Test (IATT) DateGranted: 

(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.

March 1, 2019

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 UII: 007-000002243

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

Guidance 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.
SECTION 4: REVIEW AND APPROVAL SIGNATURES

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>Gary Johnson</th>
<th>(1) Title</th>
<th>Project manager</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>PM Applications, Supporting Establishment Systems</td>
<td>(3) Work Telephone</td>
<td>703-432-7494</td>
</tr>
<tr>
<td>(4) DSN</td>
<td></td>
<td>(5) E-mail address</td>
<td><a href="mailto:gary.johnson2@usmc.mil">gary.johnson2@usmc.mil</a></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td>09/24/18</td>
<td>(7) Signature</td>
<td>JOHNSON.GARY.W.1110451284</td>
</tr>
<tr>
<td>b. Other Official (to be used at Component discretion)</td>
<td>Cheryl Randall</td>
<td>(1) Title</td>
<td>ISSM</td>
</tr>
<tr>
<td>(2) Organization</td>
<td>PM Applications, Supporting Establishment Systems</td>
<td>(3) Work Telephone</td>
<td>703-432-7875</td>
</tr>
<tr>
<td>(4) DSN</td>
<td></td>
<td>(5) E-mail address</td>
<td><a href="mailto:cheryl.randall@usmc.mil">cheryl.randall@usmc.mil</a></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td>09/24/18</td>
<td>(7) Signature</td>
<td>RANDALL.CHERYL.NMN.1024521539</td>
</tr>
<tr>
<td>c. Other Official (to be used at Component discretion)</td>
<td>(1) Title</td>
<td></td>
<td></td>
</tr>
<tr>
<td>(2) Organization</td>
<td></td>
<td>(3) Work Telephone</td>
<td></td>
</tr>
<tr>
<td>(4) DSN</td>
<td></td>
<td>(5) E-mail address</td>
<td></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td></td>
<td>(7) Signature</td>
<td></td>
</tr>
<tr>
<td>d. Component Privacy Officer (CPO)</td>
<td>Deborah Contaoi</td>
<td>(1) Title</td>
<td>USMC Privacy Program Coordinator</td>
</tr>
<tr>
<td>(2) Organization</td>
<td>HQMC FOIA/PA Programs</td>
<td>(3) Work Telephone</td>
<td>703-692-2445</td>
</tr>
<tr>
<td>(4) DSN</td>
<td></td>
<td>(5) E-mail address</td>
<td><a href="mailto:deborah.contaoi@usmc.mil">deborah.contaoi@usmc.mil</a></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td>11/19/18</td>
<td>(7) Signature</td>
<td>CONTAO.TERI.DEBORAH.VANNEWKIRK.1176225200</td>
</tr>
</tbody>
</table>

Digitally signed by:
- JOHNSON.GARY.W.1110451284
  Date: 2018.09.24 13:01:09 -04'00'
- RANDALL.CHERYL.NMN.1024521539
  Date: 2018.09.24 13:29:37 -04'00'
- CONTAO.TERI.DEBORAH.VANNEWKIRK.1176225200
  Date: 2018.11.19 10:11:00 -05'00'
### Component Records Officer

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Elena Drayer</td>
<td>Marine Corps Records Manager</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(2) Organization</th>
<th>(3) Work Telephone</th>
<th>(5) E-mail address</th>
</tr>
</thead>
<tbody>
<tr>
<td>HQMC (ARDB)</td>
<td></td>
<td><a href="mailto:elena.drayer@usmc.mil">elena.drayer@usmc.mil</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(6) Date of Review</th>
<th>(7) Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/03/18</td>
<td></td>
</tr>
</tbody>
</table>

### Component Senior Information Security Officer or Designee

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>Dr. Ray A. Letteer</td>
<td>Chief, Cybersecurity Division; Marine Corps Authorizing Official (AO)</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(2) Organization</th>
<th>(3) Work Telephone</th>
<th>(5) E-mail address</th>
</tr>
</thead>
<tbody>
<tr>
<td>HQMC DC I C4/CY</td>
<td>703-693-3490</td>
<td><a href="mailto:ray.letteer@usmc.mil">ray.letteer@usmc.mil</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(6) Date of Review</th>
<th>(7) Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>09/26/18</td>
<td></td>
</tr>
</tbody>
</table>

### Senior Component Official for Privacy (SCOP) or Designee Name

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>for CAPT Damen Hofheinz</td>
<td>Director, OCIO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(2) Organization</th>
<th>(3) Work Telephone</th>
<th>(5) E-mail address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the Chief Information Officer (OCIO)</td>
<td>703-695-1297</td>
<td><a href="mailto:steven.muck@navy.mil">steven.muck@navy.mil</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(6) Date of Review</th>
<th>(7) Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MUCK.STEVEN.R</td>
</tr>
</tbody>
</table>

### Component CIO Reviewing Official Name

<table>
<thead>
<tr>
<th>Name</th>
<th>Title</th>
</tr>
</thead>
<tbody>
<tr>
<td>for CAPT Damen Hofheinz</td>
<td>Director, OCIO</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(2) Organization</th>
<th>(3) Work Telephone</th>
<th>(5) E-mail address</th>
</tr>
</thead>
<tbody>
<tr>
<td>Office of the Chief Information Officer (OCIO)</td>
<td>703-695-1297</td>
<td><a href="mailto:steven.muck@navy.mil">steven.muck@navy.mil</a></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>(6) Date of Review</th>
<th>(7) Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>MUCK.STEVEN.R</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.