**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:

Limited Duty Sailor Marine Readiness Tracker (LIMDU SMART)

### 2. DOD COMPONENT NAME:

Defense Health Agency

### 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
- [X] 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
- [X] Existing DoD Information System
- [ ] New Electronic Collection
- [ ] Existing Electronic Collection

#### 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.

LIMDU SMART provides Navy and Marine Corps with real-time visibility of all personnel on limited duty status, capability to run reports on all aspects of Limited Duty (LIMDU) Program, and electronically manage process workflows. Full visibility of all Sailors and Marines assigned to LIMDU supports overall readiness status. MTF staff with Convening Authority can compile key data elements by utilizing LIMDU SMART’s analytical reports and dashboards to depict care management.

LIMDU SMART’s data “at-a-glance” feature effectively provides visibility of all Sailors’ and Marines’ limited duty status while safeguarding service member’s Personal Identification Information (PII) through role-based access and read/write audit trails. LIMDU SMART modernizes the legacy paper-based LIMDU program, providing force strength clarity and comprehensive insight into service member’s care via a centralized, web-based application.

PII collected about active duty service members will include: Name, SSN, date of birth, gender, race/ethnicity, home address, home telephone number, personal email address, employment, medical and disability information.

LIMDU SMART is owned and operated by Department of NAVY, Bureau of Medicine and Surgery, Medical Readiness program management office under the Deputy Assistant Director Information Operations (DAD IO), (J-6), Solution Delivery Division.

#### 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)

Primary collection; User registration - verification, identification, authentication.

To determine individual and unit medical readiness - mission related.

Chapter 18 of the NAVMED P-117 (Manual of Medicine) outlines the vital components and procedures for processing of Medical Evaluation Boards (MEB) and Medical Evaluation Board Reports (MEBR) for Navy and Marine Corps service members who are removed from full duty for medical reasons; to include LIMDU. This process directly affects Individual and Unit Medical Readiness.

Fitness for duty - mission related.

The collected data is used to evaluate the fitness of service members for continued military service. Members removed from full duty for medical reasons are evaluated by medical personnel. The information entered by the medical staff and approved Convening Authority staff creates the service member's limited duty case. Patient Administration Medical Boards Department monitors the progress of limited duty case in accordance with Navy's Limited Duty Program policy.
e. 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.

Individuals may decline to provide their information, however NAVMED P-117 (Manual of Medicine) requires an evaluation for continued service for all members removed from duty for medical reasons.

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.

Individuals may provide their consent for the specific use of their information by providing the information after receiving a copy of the Privacy Act Statement.

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

A pre-printed department of Defense (DD) Form 2005, "Privacy Act Statement - Health Care Records" is provided to the patient at the point of care for review and signature and it is placed in the patient's medical record.

All members who have PII entered in LIMDU SMART are interviewed by Medical Board Office staff members prior to and during the data collection process. The process of the collection and evaluation of the data is verbally explained to each member. The privacy of the information is detailed to the member and the member's signature is required prior to the data being forwarded to the evaluation board.

Privacy Act Statement

This statement serves to inform you of the purpose for collecting personal information required by LIMDU SMART and how it will be used.

AUTHORITY:  10 U.S.C. 55 Medical and Dental Care; 10 U.S.C. 1095, Health Care Services Incurred on Behalf of Covered Beneficiaries: Collection from Third Party Payers Act; 44 U.S.C. 3101, Records management by agency heads; 5 CFR 293.502, Subpart E, Employee Medical File System Records; DoD 6025.18-R Health Information Privacy Regulation; and E.O. 9397 (SSN), as amended.

PURPOSE:  To collect information from you to be used for real-time visibility of all personnel on limited duty status, run reports on all aspects of the LIMDU Program, and electronically manage process workflows.

ROUTINE USES: Information in your records may be disclosed to private physicians and Federal agencies, including the Department of Veterans Affairs, Health and Human Services, and Homeland Security in connection with your medical care; other government agencies to determine your eligibility for benefits and entitlements; and government and nongovernment third parties to recover the cost of healthcare provided to you by the Military Health System. Use and disclosure of your records outside of DoD may also occur in accordance with the Privacy Act of 1974, as amended (5 U.S.C. 552a(b)).

Any protected health information (PHI) in your records may be used and disclosed generally as permitted by the HIPAA Privacy Rule (45 CFR Parts 160 and 164), as implemented within DoD. Permitted uses and discloses of PHI include, but are not limited to, treatment, payment, and healthcare operations.

For a full listing of applicable Routine Uses, refer to the applicable SORN.

APPLICABLE SORN:  N06150-2, Health Care Record System (June 16, 2003, 68 FR 35657), is the applicable SORN for this system.

DISCLOSURE: Voluntary. If you choose not to provide your information, no penalty may be imposed, but absence of the requested information may result in administrative delays.
h. With whom will the PII be shared through data exchange, both within your DoD Component and outside your Component?  (Check all that apply)

<table>
<thead>
<tr>
<th>Option</th>
<th>Specification</th>
</tr>
</thead>
<tbody>
<tr>
<td>Within the DoD Component</td>
<td>Specify. PII is shared with authorized users at Defense Health Agency (DHA) and clinicians and Patient Administration staff at DHA Medical Treatment Facilities (MTFs).</td>
</tr>
<tr>
<td>Other DoD Components</td>
<td>Specify. PII is shared with authorized users at the Bureau of Navy Medicine and Surgery (BUMED). BUMED users are only authorized to view LIMDU SMART for their specific regional commands. PII is also shared with Navy and Marine Corps personnel headquarters’ authorized users, Personnel Support Detachment (PSD), Command Deployability and LIMDU Coordinator staff. No medical information will be shared with Headquarters, PSD, Command Deployability, and LIMDU Coordinator staff.</td>
</tr>
<tr>
<td>Other Federal Agencies</td>
<td>Specify. Information may be disclosed to authorized users of Federal agencies, including the Department of Veterans Affairs, the Department of Health and Human Services, and the Department of Homeland Security.</td>
</tr>
<tr>
<td>State and Local Agencies</td>
<td>Specify. Universal Consulting Agency (UCS) provides system maintenance support to LIMDU SMART and has access to the PII therein. Contract N00189-15-P-Z464 contains the following language that safeguards PII: The Contractor shall establish required administrative, technical, and physical safeguards to protect any and all Government data, including PII/PHI. The Contractor shall also ensure the confidentiality, integrity, and availability of data in compliance with all applicable laws and regulations, including data breach reporting/responses requirements. The Contractor shall comply with federal laws relating to FOIA and records management and analyze breaches of PII/PHI for which it is responsible under both the Privacy Act and HIPAA. 9.1.11. UCS will research requests for MHS data that include PHI. These requests must be reviewed for HIPAA compliance by the DHA Privacy Board. Additionally, UCS has a Data Sharing Agreement (DSA) in place (DSA#19-2072), per DHA regulations. The DSA controls the disclosure, use, storage and/or destruction of MHS data that is managed by DHA to ensure compliance with privacy and security requirements applicable to PII and PHI.</td>
</tr>
<tr>
<td>Other (e.g., commercial providers, colleges).</td>
<td>Specify.</td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Specify.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Individuals</td>
<td></td>
</tr>
<tr>
<td>Databases</td>
<td></td>
</tr>
<tr>
<td>Existing DoD Information Systems</td>
<td></td>
</tr>
<tr>
<td>Commercial Systems</td>
<td></td>
</tr>
<tr>
<td>Other Federal Information Systems</td>
<td></td>
</tr>
</tbody>
</table>

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

<table>
<thead>
<tr>
<th>Option</th>
<th>Specify.</th>
</tr>
</thead>
<tbody>
<tr>
<td>E-mail</td>
<td></td>
</tr>
<tr>
<td>Official Form (Enter Form Number(s) in the box below)</td>
<td></td>
</tr>
<tr>
<td>Face-to-Face Contact</td>
<td></td>
</tr>
<tr>
<td>Paper</td>
<td></td>
</tr>
</tbody>
</table>
The applicant submits information in person using a web form within https://edq.med.navy.mil/.

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 [X] No

If "Yes," enter SORN System Identifier N06150-2

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

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

(3) Retention Instructions.

Unscheduled. Retain as permanent. LIMDU SMART Project Team coordinating with DHA Records Management Team to determine retention instructions.

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 Authorities:


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 8510.01, 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.

LIMDU SMART does not collect information from the public; OMB Control Number is not applicable.
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
- Citizenship
- Driver's License
- Employment Information
- Home/Cell Phone
- Mailing/Home Address
- Military Records
- Official Duty Address
- Passport Information
- Place of Birth
- Race/Ethnicity
- Records
- Work E-mail Address
- Child Information
- DoD ID Number
- Emergency Contact
- Gender/Gender Identification
- Legal Status
- Medical Information
- Name(s)
- Other ID Number
- Photo
- Protected Health Information (PHI)¹
- Religious Preference
- Social Security Number (SSN) (Full or in any form)

Employment Information: Occupational specialty, assignment information.
Medical Information: Diagnosis

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.

Pending approval. Submitted to PCLO on 3/20/2020.

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

2.c(8) Computer Matching: “Systems, processes, or forms that interact with other Government agencies may require the continued use of the SSN as a primary identifier until such time as the applications to which they are linked move to some other identifier as a primary means for transferring, matching, or checking information.”

A function of LIMDU SMART is the ability to share information in a Service member’s records to private physicians and Federal agencies, including the Department of Veteran’s Affairs (VA), Health and Human Services (HHS), and Department of Homeland Security (DHS) in connection with medical care; other government agencies to determine eligibility for benefits and entitlements; and government and non-government third parties to recover the cost of healthcare provided by the Military Health System. This transfer of information between multiple entities necessitates the need for continued use of SSN to ensure all Service member’s records are able to be connected back to them.

An example of this requirement is the Department of the Navy Electronic Military Personnel System, EMPRS. According to NSC-1300, the member's personnel record is stored in the EMPRS and consists of permanent documents that reflect a member’s fitness for service, performance of duties, and entitlements, which satisfy both statutory and corporate requirements, and affect or influence a member’s career and benefits. EMPRS’ requires an interface with LIMDU SMART in order to compile a Service member’s comprehensive Official Military Personnel File (OMPF).

All OMPFs created after 1995 are digital image records. When a new accession file is received, a digital image OMPF is created using the member’s SSN. Documents are scanned into the digital record system EMPRS. Individual documents received afterwards will be scanned to EMPRS using the SSN on the document. After the system runs its record input cycle, documents are indexed to the record that matches the SSN. The paper document is then destroyed. A document that has been digitized is considered an original official document.

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”.

LIMDU SMART uses role-based accounts to ensure that users have access to only the specific cases they need in order to accomplish their mission. Additionally, it has read/write audit trails to track the activities of users utilizing the system. Access to the data center where PII is stored is restricted to authorized personnel only; and will only be stored and accessible from one site: NOLA. Personnel with an authorized swipe card are considered visitors and must follow the visitor policy. This includes military and employees of the Naval Information Warfare
Center (NIWC), and their badges must be displayed at all times. PII captured within LIMDU SMART is securely transmitted over Hypertext Transfer Protocol Secure (HTTPS) with Secure Socket Layer. Furthermore, LIMDU SMART uses Public Key Infrastructure (PKI), authenticated by the Common Access Card (CAC), and is used to authenticate validated users. PII is encrypted at rest and the system is only accessible over NIPR Net.

(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?

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

- Yes
- No

LIMDU SMART shares data with the Bureau of Medicine and Surgery (BUMED); this system remains as the Contracting Officer’s Representative (COR) for TIER II/III operations. BUMED has made a thorough effort to evaluate the risk associated with the system and every reasonable step has been taken to remove the use of the SSN and protect it where the use is still required.

b. What is the PII confidentiality impact level?  

<table>
<thead>
<tr>
<th>Low</th>
<th>Moderate</th>
<th>High</th>
</tr>
</thead>
</table>

1The definition of PHI involves evaluating conditions listed in the HIPAA. Consult with General Counsel to make this determination.

2Guidance 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 Officer 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

Naval Information Warfare Center (NIWC) Atlantic, New Orleans (NOLA) and Navy Enterprise Disaster Recovery (NEDRC), Kansas City (COOP site) provide physical security which prevents unauthorized personnel from gaining access to equipment, facilities, materials and documents by use of door badge readers. Assets are safeguarded against espionage, sabotage, damage, fire and theft by electronic means with the use of a security system, fire alarms and sprinkler equipment.

Access to the data center is restricted to authorized personnel only and will only be stored at and accessible from one site: NOLA. Personnel with an authorized swipe card are considered visitors and must follow the visitor policy. This includes military and employees of NIWC. A NIWC ID badge must be displayed at all times. Visitors must sign in the visitor log located at the data center entrance and sign out upon exiting. Visitors must display either a NIWC ID or NIWC Visitor badge. Visitors shall be escorted and remain escorted by authorized personnel while in the data center.

(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

All PII collected will be provided protection corresponding with the nature and type of information involved. Back-ups are run every night. Back-ups are encrypted to FIPS 140-2 compliance. System has user manuals which are maintained for users. The system uses audit logs, configuration management, as well as document versions to ensure access is monitored and the data integrity, accuracy, and availability are not compromised by a user. Users receive training to use LIMDU SMART appropriately.

Data stored or processed temporarily in automated data processing systems, and will be protected due to the inherent security risks posed by storing PII in an ADP environment. Examples of safeguards used by LIMDU SMART include:

1. Labeling or designating output and storage media products containing PII that do not contain classified material to alert those using or handling the information of the need for special protection.
2. Marking and protecting all computer products containing classified data in accordance with DoD 5200.1-R and DoD 5200.28-M.
3. Restoring all PII being processed in the event of a computer failure, using proper recovery procedures to ensure data integrity.
4. Training all ADP personnel processing information in proper safeguarding procedures.
5. System has a user's manual and help section for Frequently Asked Questions.

All PII and Protected health Information collected in LIMDU SMART is protected by the privacy and security provisions outlined in the Health Insurance Portability and Accountability Act (HIPAA).

<table>
<thead>
<tr>
<th>(3) Technical Controls. (Check all that apply)</th>
</tr>
</thead>
<tbody>
<tr>
<td>✔ Biometrics</td>
</tr>
<tr>
<td>✔ Encryption of Data at Rest</td>
</tr>
<tr>
<td>✔ Firewall</td>
</tr>
<tr>
<td>✔ Role-Based Access Controls</td>
</tr>
<tr>
<td>✔ Virtual Private Network (VPN)</td>
</tr>
<tr>
<td>✔ Encryption of Data in Transit</td>
</tr>
<tr>
<td>✔ Intrusion Detection System (IDS)</td>
</tr>
<tr>
<td>✔ Used Only for Privileged (Elevated Roles)</td>
</tr>
<tr>
<td>✔ Least Privilege Access</td>
</tr>
<tr>
<td>✔ External Certificate Authority Certificates</td>
</tr>
<tr>
<td>✔ DoD Public Key Infrastructure Certificates</td>
</tr>
<tr>
<td>✔ Least Privilege Access</td>
</tr>
<tr>
<td>✔ User Identification and Password</td>
</tr>
<tr>
<td>✔ If Other, enter the information in the box below</td>
</tr>
</tbody>
</table>

PII captured within LIMDU SMART is securely transmitted over HTTPS with Secure Socket Layer.

Public Key Infrastructure (PKI), authenticated by the Common Access Card (CAC), is used to authenticate validated users. PII is encrypted at rest. System is only accessible over NIPR NET.

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

All systems are vulnerable to "insider threats." LIMDU SMART managers are vigilant to this threat by limiting system access to those individuals who have a defined need to access the information. Service member’s Personal Identification Information (PII) is protected through role-based access. It has read/write audit trails to track the activities of any user utilizing the system.

Data in LIMDU SMART is maintained in accordance with HIPAA requirements. Only users with appropriate access and need-to-know are authorized to manage data in this system. All application support users have background investigation and are approved Automated Data Processing (ADP) II clearances prior to being granted access to LIMDU SMART. These procedures mitigate any risk of compromise of PII.
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) tool3?

- [x] Yes, DITPR
  - DITPR System Identification Number: 18334

- [ ] Yes, SIPRNET
  - SIPRNET Identification Number:

- [x] Yes, RMF tool
  - RMF tool Identification Number: 1341

- [ ] No

If "No," explain.

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: 8/29/2018

- [ ] 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
  - UII: 000100873

- [ ] No

If "Yes," Enter UII

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>Title</th>
<th>Organization</th>
<th>Work Telephone</th>
<th>E-mail address</th>
<th>Date of Review</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCDR Saad Alaziz</td>
<td>Project Manager</td>
<td>DHA</td>
<td>(210) 536-7043</td>
<td><a href="mailto:saad.m.alaziz.mil@mail.mil">saad.m.alaziz.mil@mail.mil</a></td>
<td>11/07/18</td>
<td>ALAZIZ.SAAD.MUHAMMAD.1088839842</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>b. Other Official (to be used at Component discretion)</th>
<th>Title</th>
<th>Organization</th>
<th>Work Telephone</th>
<th>E-mail address</th>
<th>Date of Review</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>LCDR William Haywood</td>
<td>Program Manager</td>
<td>BUMED/M3</td>
<td>(703) 681-9080</td>
<td><a href="mailto:william.p.haywood.mil@mail.mil">william.p.haywood.mil@mail.mil</a></td>
<td>02/20/19</td>
<td>HAYWOOD.WILLIAM.PETER.1267645252</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>c. Other Official (to be used at Component discretion)</th>
<th>Title</th>
<th>Organization</th>
<th>Work Telephone</th>
<th>E-mail address</th>
<th>Date of Review</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Eric Jackson</td>
<td>ISSM/ BUMED CIO</td>
<td>BUMED/M6</td>
<td>(703) 681-2490</td>
<td><a href="mailto:eric.c.jackson1.civ@mail.mil">eric.c.jackson1.civ@mail.mil</a></td>
<td>02/22/19</td>
<td>JACKSON.ERIC.C.1131607870</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>d. Component Privacy Officer (CPO)</th>
<th>Title</th>
<th>Organization</th>
<th>Work Telephone</th>
<th>E-mail address</th>
<th>Date of Review</th>
<th>Signature</th>
</tr>
</thead>
<tbody>
<tr>
<td>Rahwa Keleta</td>
<td>Chief, Privacy and Civil Liberties Office</td>
<td>DHA</td>
<td>703-275-6363</td>
<td><a href="mailto:rahwa.a.keleta.civ@mail.mil">rahwa.a.keleta.civ@mail.mil</a></td>
<td></td>
<td>KELETA.RAHWA.AMD6A.M1298456431</td>
</tr>
</tbody>
</table>

Digitally signed by:

- ALAZIZ.SAAD.MUHAMMAD.1088839842
- HAYWOOD.WILLIAM.PETER.1267645252
- JACKSON.ERIC.C.1131607870
- KELETA.RAHWA.AMD6A.M1298456431
<table>
<thead>
<tr>
<th><strong>e. Component Records Officer</strong></th>
<th>Glinda Hodgkin</th>
<th>(1) Title</th>
<th>DHA Records Management Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>DHA J1 Records Management Office</td>
<td>(3) Work Telephone</td>
<td>303-676-3418</td>
</tr>
<tr>
<td>(4) DSN</td>
<td></td>
<td>(5) E-mail address</td>
<td><a href="mailto:glinda.l.hodgkin.civ@mail.mil">glinda.l.hodgkin.civ@mail.mil</a></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td>03/04/19</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>f. Component Senior Information Security Officer or Designee Name</strong></th>
<th>Franklin D. Rowland Jr.</th>
<th>(1) Title</th>
<th>Chief, Cyber Security Division</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>DHA J-6 Cyber Security Division</td>
<td>(3) Work Telephone</td>
<td>703-681-6389</td>
</tr>
<tr>
<td>(4) DSN</td>
<td></td>
<td>(5) E-mail address</td>
<td><a href="mailto:franklin.d.rowland.civ@mail.mil">franklin.d.rowland.civ@mail.mil</a></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td>04/04/20</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>g. Senior Component Official for Privacy (SCOP) or Designee Name</strong></th>
<th>Rahwa Keleta</th>
<th>(1) Title</th>
<th>Chief, Privacy and Civil Liberties Office</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>DHA</td>
<td>(3) Work Telephone</td>
<td>703-275-6363</td>
</tr>
<tr>
<td>(4) DSN</td>
<td></td>
<td>(5) E-mail address</td>
<td><a href="mailto:rahwa.a.keleta.civ@mail.mil">rahwa.a.keleta.civ@mail.mil</a></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>h. Component CIO Reviewing Official Name</strong></th>
<th>T. Patrick Flanders, SES</th>
<th>(1) Title</th>
<th>Chief Information Officer, (DADIO &amp; J-6)</th>
</tr>
</thead>
<tbody>
<tr>
<td>(2) Organization</td>
<td>DHA</td>
<td>(3) Work Telephone</td>
<td>703-681-9530</td>
</tr>
<tr>
<td>(4) DSN</td>
<td></td>
<td>(5) E-mail address</td>
<td><a href="mailto:thomas.p.flanders2.civ@mail.mil">thomas.p.flanders2.civ@mail.mil</a></td>
</tr>
<tr>
<td>(6) Date of Review</td>
<td></td>
<td></td>
<td></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.mil.

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.