

## 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:

OMNI-CHANNEL

### 2. DOD COMPONENT NAME:

Department of the Navy

### 3. PIA APPROVAL DATE:

11/26/19

BUREAU OF NAVAL PERSONNEL (BUPERS)

### 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 Federal employees and/or Federal contractors
- ☒ From both members of the general public and 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 ☒ New Electronic Collection
- ☐ Existing DoD Information System ☐ Existing Electronic Collection
- ☐ Significantly Modified DoD Information System

#### 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.

OMNI-CHANNEL will be used to record and index telephone conversations between customers and customer service representatives (CSRs) in My Navy Career Center (MNCC) contact centers. Callers could be members of the military, family members, contractors or members of the public. Callers may ask about their own official records, family members may ask about upcoming transfers, and members of the public may call looking for individuals (for legal reasons). The inbound calls will be recorded in order to resolve misunderstandings or misperceptions made during the customer-CSR interaction. This system will also facilitate the process of monitoring and evaluating the recorded audio used by CSRs in order to provide training, collect data in support of the CSRs annual performance evaluation, and provide information used for business process improvements.

Data that will be collected: either the SSN or DoD ID.

Data collected could be: Name, personal contact information (email, phone number and home address), rank, mother's maiden name and financial 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)

PII is collected for identification and verification purposes.

#### 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.

The interactive voice response (IVR) system, which front ends the call flow process, informs the caller that the conversation is being recorded for quality evaluation purposes and explains to the customer that if they do not provide their DoD ID or SSN they cannot be assisted on a personnel specific issue. At that point, the caller can hang-up or the call will be answered by a customer service representative (CSR).

#### 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.

Once PII is provided by the individual, consent is implied.

**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

MNCC OMNI-CHANNEL Privacy Act Statement – We are required by law to provide the following Privacy Act Notice to you. The information requested is authorized for collection under Executive Order (E.O.) 9397, as amended, and System of Records Notice T5040. The information collected is used to record and index telephone conversations between customers and customer service representatives (CSRs) in My Navy Career Center (MNCC) contact centers. The inbound calls will be recorded in order to resolve misunderstandings or misperceptions made during the customer-CSR interaction. This system will also facilitate the process of monitoring and evaluating the recorded audio and computer screens used by CSRs in order to provide training, collect data in support of the CSRs annual performance evaluation, and provide information used for business process improvements. In addition to the applicable standard Routine Uses associated with SORN T5040, and DoD Instruction 1000.30 Legacy System Interface acceptable use, this information will be used by CSRs to access your Privacy Act records for customer service purposes. Disclosure of requested information is voluntary, however failure to provide the requested information may impact the CSRs ability to assist you.

More information on the PIA and SORN can be found at the following link:

<http://dpcl.d.defense.gov/Privacy/SORNsIndex/DOD-wide-SORN-Article-View/Article/>

**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

Specify.

MNCC employees and management on a need-to-know basis. Investigatory agencies (e.g., Inspector General)

☒ 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.)

Specify.

The vendor is AT&T/TTEC. All seven FAR and DFAR clauses have been added to the contract. All contract employees complete privacy training prior to having access to PII.

☐ 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

All PII is collected via telephone.

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

☐ E-mail

☐ Official Form (Enter Form Number(s) in the box below)

☐ Face-to-Face Contact

☐ Paper

☐ Fax

☒ Telephone Interview

☐ Information Sharing - System to System

☐ Website/E-Form

☐ 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 T5040 (Working with DFAS to modify the

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

**I. 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. DAA-GRS-2017-0001-00

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

(3) Retention Instructions.

Records contained in OMNI-CHANNEL are scheduled under SSIC 2000-21 and are temporary. Destroy 1 year after resolved, or when no longer needed for business use, whichever is appropriate.

**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 T5040, Call Recording Application Records (March 24, 2009, 74 FR 12320), authorities:

5 USC Section 301, Departmental Regulations; EO 12862 (Customer Service); and EO 9397 Social Security Number (SSN) as amended.

**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.

OMB package is in process at BUPERS and will be submitted by mid-December.

## 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)

- |  |   |  |
|--|---|--|
| <input type="checkbox"/> Biometrics                      | <input type="checkbox"/> Birth Date                                       | <input type="checkbox"/> Child Information   |
| <input type="checkbox"/> Citizenship                     | <input type="checkbox"/> Disability Information                           | <input checked="" type="checkbox"/> DoD ID Number                                      |
| <input type="checkbox"/> Driver's License                | <input type="checkbox"/> Education Information                            | <input type="checkbox"/> Emergency Contact   |
| <input type="checkbox"/> Employment Information          | <input checked="" type="checkbox"/> Financial Information                 | <input type="checkbox"/> Gender/Gender Identification                                  |
| <input checked="" type="checkbox"/> Home/Cell Phone      | <input type="checkbox"/> Law Enforcement Information                      | <input type="checkbox"/> Legal Status  |
| <input checked="" type="checkbox"/> Mailing/Home Address | <input checked="" type="checkbox"/> Marital Status                        | <input type="checkbox"/> Medical Information   |
| <input checked="" type="checkbox"/> Military Records     | <input checked="" type="checkbox"/> Mother's Middle/Maiden Name           | <input checked="" type="checkbox"/> Name(s)  |
| <input type="checkbox"/> Official Duty Address           | <input type="checkbox"/> Official Duty Telephone Phone                    | <input type="checkbox"/> Other ID Number   |
| <input type="checkbox"/> Passport Information            | <input checked="" type="checkbox"/> Personal E-mail Address               | <input type="checkbox"/> Photo   |
| <input type="checkbox"/> Place of Birth                  | <input type="checkbox"/> Position/Title                                   | <input type="checkbox"/> Protected Health Information (PHI) <sup>1</sup>               |
| <input type="checkbox"/> Race/Ethnicity                  | <input checked="" type="checkbox"/> Rank/Grade                            | <input type="checkbox"/> Religious Preference  |
| <input type="checkbox"/> Records                         | <input type="checkbox"/> Security Information                             | <input checked="" type="checkbox"/> Social Security Number (SSN) (Full or in any form) |
| <input type="checkbox"/> Work E-mail Address             | <input type="checkbox"/> If Other, enter the information in the box below |  |

Military Records: Pay, Service Years, Time in Grade

Financial Information: Basic Allowance for Housing, Basic Allowance for Subsistence, advance travel pay, per diem

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.

BUPERS CIO; approved 07 NOV 2019

(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

(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".

The MNCC system is required to have the full SSN provided because of the need to interface with systems that do not contain the DoD ID.

(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

We adhere to the SSN reduction policy as stated in the mitigation efforts above; Section 2 a (3). Until such time corporate systems are modernized to utilize the DoD ID, the SSN must continue to be used to ensure the correct official record is matched to the individual requesting assistance. It would be unrealistic to identify a date this modification to our corporate systems will occur.

**b. What is the PII confidentiality impact level<sup>2</sup>?**

☐ Low ☒ Moderate ☐ High

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

<sup>2</sup>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)*

- |   |   |
|---|---|
| <input checked="" type="checkbox"/> Cipher Locks    | <input type="checkbox"/> Closed Circuit TV (CCTV)                         |
| <input type="checkbox"/> Combination Locks          | <input checked="" type="checkbox"/> Identification Badges                 |
| <input type="checkbox"/> Key Cards                  | <input type="checkbox"/> Safes  |
| <input checked="" type="checkbox"/> Security Guards | <input type="checkbox"/> 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)*

- |   |   |  |
|---|---|--|
| <input type="checkbox"/> Biometrics                               | <input checked="" type="checkbox"/> Command Access Card (CAC)                 | <input checked="" type="checkbox"/> DoD Public Key Infrastructure Certificates |
| <input checked="" type="checkbox"/> Encryption of Data at Rest    | <input checked="" type="checkbox"/> Encryption of Data in Transit             | <input type="checkbox"/> External Certificate Authority Certificates           |
| <input checked="" type="checkbox"/> Firewall                      | <input checked="" type="checkbox"/> Intrusion Detection System (IDS)          | <input checked="" type="checkbox"/> Least Privilege Access                     |
| <input checked="" type="checkbox"/> Role-Based Access Controls    | <input checked="" type="checkbox"/> Used Only for Privileged (Elevated Roles) | <input checked="" type="checkbox"/> User Identification and Password           |
| <input checked="" type="checkbox"/> Virtual Private Network (VPN) | <input type="checkbox"/> 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?**

COLLECTION: OMNI-CHANNEL automatically and systemically collects PII by recording telephone conversations. The information is retained on servers in secure facilities.

USE and PROCESSING: A limited number of personnel on a need-to-know basis have been approved through the National Agency Check with Law and Credit (NACLC) and System Authorization Access Request (SAAR) processes to access the OMNI-CHANNEL system.

RETENTION and DESTRUCTION: The records are destroyed in accordance with SECNAV M-5210 Change 1, Department of the Navy Records Management Program Manual and SECNAVINST 5210.8F Department of the Navy Records Management Program.