U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer

TAP EMPLOYMENT NAVIGATOR PRIVACY IMPACT ASSESSMENT

VERSION 1.8

05/04/2022

OCUMENT CHANGE HISTORY

Date	Filename / Version #	Author	Revision Description
11/19/08	Privacy Impact Assessment Template 1.5	Adrienne Ramirez	Annual Update
05/01/10	Privacy Impact Assessment	Adrienne Ramirez, Michael O'Rourke	Annual Update
01/07/11	Privacy Impact Assessment	Adrienne Ramirez	Appendix A
3/12/12	Privacy Impact Assessment	Adrienne Ramirez	To include 3rd Party Website Updates
2/25/13	Privacy Impact Assessment	Adrienne Ramirez	Annual Review
12/16/15	Privacy Impact Assessment	Adrienne Ramirez	Review and Update
12/16/16	Privacy Impact Assessment	Adrienne Ramirez	Review and Update
12/18/17	Privacy Impact Assessment	Adrienne Ramirez	Review and Update
12/17/18	Privacy Impact Assessment	Adrienne Ramirez	Annual Review and Update
11/27/20	Privacy Impact Assessment	Adrienne Ramirez	Annual Review and Updates
5/3/2022	Privacy Impact Assessment	VETS TEN	Updated Responses

DOCUMENT REVIEW HISTORY

Date	Version #	Reviewers
11/19/08	Privacy Impact Assessment Template 1.5	Tonya Manning
06/10/10	Privacy Impact Assessment Template 1.6	Tonya Manning
01/07/11	Privacy Impact Assessment Template 1.6	Tonya Manning

03/12/12	**Privacy Impact Assessment Template 1.7**	**Tonya Manning**
03/01/13	**Privacy Impact Assessment Template 1.7**	**Tonya Manning**
12/16/15	**Privacy Impact Assessment Template 1.8**	**Miranda Key**
12/16/16	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**
12/20/17	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**
12/18/18	**Privacy Impact Assessment Template 1.8**	**Adrienne Ramirez**
11/27/20	**Privacy Impact Assessment 1.8**	**Adrienne Ramirez**
5/4/2022	**Privacy Impact Assessment 1.8**	**DSAM**

TABLE OF CONTENTS

1.1 OVERVIEW

VETS TAP Employment Navigator (VETS TEN) is a system to support Transitioning Service Members (TSMs) and spouses by stationing contractor employees on select military bases (about 15) throughout the United States (CONUS & OCONUS). These "Employment Navigators" (about 55) will use TEN to assist with any needs a TSM has as he/she separates from the military into the civilian workforce. Assistance may include: career exploration, local job market information, or connection to employers or partner entities who may further assist with job placements. These "Partners" use TEN to assist veterans in getting prepared for a career, and/or placing them into appropriate jobs. VETS "Federal Staff" use TEN to monitor performance of employment navigators and partners in assisting TSMs and to evaluate Return on Investment (ROI) for continuing/expanding the program. The information about Transitioning Service Members (TSMs) collected include - First Name, Last Name, Email, Social Security Number, DOD ID and the ability to obtain all these information was submitted as part of PRA package and approved by DOD. The system does not share the collected data with any downstream systems and is self-contained.

1.2 CHARACTERIZATION OF THE INFORMATION

The following questions are intended to define the scope of the information requested and/or collected as well as reasons for its collection as part of the program, system, or technology being developed.

Specify whether the System collects personally identifiable information (PII) on DOL employees, other federal employees, contractors, members of the public (U.S. citizens), foreign citizens, or minor children.

- From whom is information to be collected?

  The system collects PII Information from members of the public, more specifically Transitioning Service Members (TSM)

- Why is the Information being collected?

  1. To effectively capture information about the Transitioning Service Members (TSM) and refer them out to Partners.
  2. The Social Security Number (SSN) and DOD ID collected will also serve in the future to match employment related information coming from NDNH - National Directory of New Hires and effectively report on the success of the TAP Program

- What is the PII being collected, used, disseminated, or maintained?

First Name, Last Name, Email, Social Security Number, DOD ID

- How is the PII collected?

  Directly by the Employment Navigators during the Transitioning Service Members (TSM) Intake into the System

- How will the information collected from individuals or derived from the system be checked for accuracy?

  There are validation rules in place to ensure the Social Security Number and email address formats are validated before allowing users to save the information

- What specific legal authorities, arrangements, and/or agreements defined allow the collection of PII?

  The PRA package submitted by VETS identified the data elements that they will be collecting from public members and was approved by DOD. The details of the collection are published in Federal Register: https://www.federalregister.gov/documents/2021/05/10/2021-09669/privacy-act-of-1974-system-of-records

- Privacy Impact Analysis

  1. Privacy risks are primarily from data loss due to spillage or unauthorized system access. Unauthorized access is mitigated by using Login.gov for login and user management. Spillage is governed by DOL Policy on protecting and report PII information.
  2. Further, data masking mechanism is in place for Social Security Number (SSN) so the Employment navigators can only see masked data after entering and saving it in the system. This helps mitigate Data Spillage and unauthorized access

1.3 DESCRIBE THE USES OF THE PII

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

- Describe all the uses of the PII

  1. To effectively capture information about the Transitioning Service Members (TSM) and refer them out to Partners.
  2. The Social Security Number (SSN) and DOD ID collected will also serve in the future to match employment related information coming from NDNH - National

Directory of New Hires and effectively report on the success of the TAP Program

- What types of tools are used to analyze data and what type of data may be produced?

  The PII information collected is not used as part of any data analysis and will be used in the future phases to develop integration with NDNH - National Directory of New Hires data

- Will the system derive new data, or create previously unavailable data, about an individual through aggregation of the collected information?

  No.

- If the system uses commercial or publicly available data, please explain why and how it is used.

  No commercial or publicly available data is used in the system.

- Will the use of PII create or modify a "system of records notification" under the Privacy Act?

  This System of Records Notice (SORN) that details of the collection is published in Federal Register: https://www.federalregister.gov/documents/2021/05/10/2021-09669/privacy-act-of-1974-system-of-records

- Privacy Impact Analysis

  1. Access Controls as defined in Access Control SOP. Access Controls included AC-1, AC-2, AC-3, AC-4, AC-5, AC-6, AC-14, AC-21
  2. The Social Security Number is stored as encrypted text in the system preventing anyone with access to Transitioning Service Members (TSM) record in Salesforce from viewing it. Privileged role of VETS Admin is needed to view the unencrypted Social Security Number.
  3. Transaction Security Policies have been enforced that prevents any user from running a Salesforce report to include PII data and export it out from the System

1.4 RETENTION

The following questions are intended to outline how long information will be retained after the initial collection.

- What is the retention period for the data in the system?

  VETS is currently in the process of developing the retention schedule with NARA for VETS TEN and will update the PIA once it has been completed.

- Is a retention period established to minimize privacy risk?

  No

- Has the retention schedule been approved National Archives and Records Administration (NARA)? Provide the retention schedule number for the schedule utilized?

  No

- Per M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*; what efforts are being made to eliminate or reduce PII that is collected, stored or maintained by the system if it is no longer required?

  VETS is currently in the process of developing the retention schedule with NARA for VETS TEN and will update the PIA once it has been completed.

- Have you implemented the DOL PII Data Extract Guide for the purpose of eliminating or reducing PII?

  VETS is currently in the process of developing the retention schedule with NARA for VETS TEN and will update the PIA once it has been completed.

- How is it determined that PII is no longer required?

  VETS is currently in the process of developing the retention schedule with NARA for VETS TEN and will update the PIA once it has been completed.

- If you are unable to eliminate PII from this system, what efforts are you undertaking to mask, de-identify or anonymize PII.

  1. The Social Security Number is stored as encrypted text in the system preventing anyone with access to Transitioning Service Members (TSM) record in Salesforce from viewing it. Privileged role of VETS Admin is needed to view the unencrypted Social Security Number.

2. Transaction Security Policies have been enforced that prevents any user from running a Salesforce report to include PII data and export it out from the System

- Privacy Impact Analysis

  VETS is currently in the process of developing the retention schedule with NARA for VETS TEN and will update the PIA once it has been completed.

1.5 INTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the scope of sharing within the Department of Labor.

- With which internal organization(s) is the PII shared, what information is shared, and for what purpose?

  Currently the information collected is self-contained and not shared with any internal organization(s)

- How is the PII transmitted or disclosed?

  Not Applicable. Currently the information collected is self-contained and not shared with any internal organization(s)

- Does the agency review when the sharing of personal information is no longer required to stop the transfer of sensitive information?

  Not Applicable. Currently the information collected is self-contained and not shared with any internal organization(s)

- Privacy Impact Analysis

  Currently the information collected is self-contained and not shared with any internal organization(s)

1.6 EXTERNAL SHARING AND DISCLOSURE

The following questions are intended to define the content, scope, and authority for information sharing external to DOL which includes federal, state and local government, and the private sector.

- With which external organization(s) is the PII shared, what information is shared, and for what purpose?

  The First Name, Last Name and Email address are shared with Partner Organization Users (Partner User License Holders) directly in the system to enable them to onboard the Transitioning Service Members (TSM) into the system to provide services.

- Is the sharing of PII outside the Department compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If so, provide the SORN ID in use for this system. If not, please describe under what legal mechanism the program or system is allowed to share the PII outside of DOL.

  Information shared outside of the department is in compliance with the original collection for the purpose of communications with External Contacts.

- How is the information shared outside the Department and what security measures safeguard its transmission?

  The Partner Users login directly into Salesforce to see the information. None of the data leaves the Salesforce FedRAMP boundary. The Social Security Number **is not shared** with the Partners.

- How is the information transmitted or disclosed?

  The Partner Users login directly into Salesforce to see the information. None of the data leaves the Salesforce FedRAMP boundary. The Social Security Number **is not shared** with the Partners.

- Is a Memorandum of Understanding (MOU), contract, or any agreement in place with any external organizations with whom information is shared, and does the agreement reflect the scope of the information currently shared? If the answer is yes, be prepared to provide a copy of the agreement in the event of an audit as supporting evidence.

  Yes. Each Partner entity signs an MOU with VETS before getting enrolled in the program

- How is the shared information secured by the recipient?

The Partner Users login directly into Salesforce to see the information. None of the data leaves the Salesforce FedRAMP boundary. The Social Security Number **is not shared** with the Partners.

- What type of training is required for users from agencies outside DOL prior to receiving access to the information?

  The Partners are provided with User Guide and training materials to get familiarized with the system and how to use the functionalities.

- Privacy Impact Analysis

  - Transaction Security policies to prevent report exports from Salesforce ensures Partners do not inadvertently export any PII data outside viewing it in the system.
  - No access to Social Security Number of DOD ID for Partners helps avoid any data spillages

1.7 NOTICE

The following questions are directed at notice to the individual of the scope of PII collected, the right to consent to uses of said information, and the right to decline to provide information.

- Was notice provided to the individual prior to collection of PII? If yes, please provide a copy of the notice as an appendix or be prepared to provide a copy of the notice during an audit request. A notice may include a posted privacy policy, a Privacy Act notice on forms, or a system of records notice published in the Federal Register Notice. If notice was not provided, please explain.

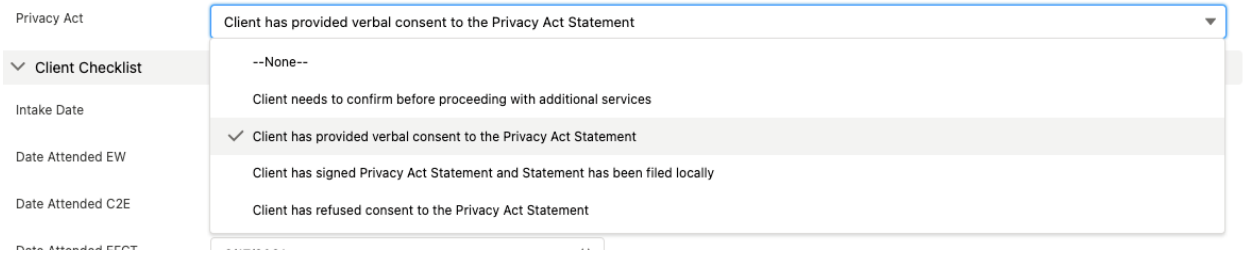
  Yes. Individuals were provided a copy of the Privacy Act and the system captures whether they have agreed to the act and signed before allowing the Employment Navigators to proceed further in administering any services to them.

- Do individuals have the opportunity and/or right to decline to provide information?

  Yes. They have the ability to decline and if they do so, the system will not allow the Employment Navigators to proceed further in administering any services to them.

- Do individuals have the right to consent to particular uses of the information? If so, how does the individual exercise the right?

  Below is the list of choices the user has and the Navigators can track the user's response accordingly in the system.



- Privacy Impact Analysis

1. Employment Navigators as part of their business process ensure to provide the details about the Privacy Act and capture the user's response in the system.
2. If the client refused to consent, the system will not allow the Employment Navigators to proceed further in administering any services to them.

1.8 INDIVIDUAL ACCESS, REDRESS, AND CORRECTION

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about them.

- What are the procedures that allow individuals to gain access to their own information?

  Only Employment Navigators (ENs) have access to an individual's data. Individuals will work directly with ENs for enter or modify their data.

- What are the procedures for correcting inaccurate or erroneous information?

  ENs work directly with individuals to review and update personal information.

- How are individuals notified of the procedures for correcting their own information?

  Individuals are notified through one-on-one working sessions with ENs for correcting their information.

- If no formal redress is provided, what alternatives are available to the individual?

  Not Applicable

- Privacy Impact Analysis

  Individuals do not have direct access to their own data. ENs enter or modify user data. ENs have been trained and have signed an agreement not to use the data from TEN for personal gains or print or share personal information.

1.9 TECHNICAL ACCESS AND SECURITY

The following questions are intended to describe technical safeguards and security measures.

- Which user group(s) will have access to the system? (For example, program managers, IT specialists, and analysts will have general access to the system and registered users from the public will have limited access.)

  Employment Navigators, Employment Navigator Managers, VETS Admin and System Administrators are the personas that have access to this information. Social Security Number is masked within the system to prevent anyone from viewing the data once saved in the system

- Will contractors to DOL have access to the system? If so, please include a copy of the contract describing their role to the OCIO Security with this PIA or be prepared to provide copies during an audit request

  Contractors from ICF that are providing O&M Administration to the application have access to the data as System Administrators. Every one of such users has also signed the Rules of Behavior to ensure they understand and comply with DOL policies.

- Does the system use "roles" to assign privileges to users of the system? If yes, describe the roles.

  The following are the functional roles in the system which are implemented in Salesforce via Permission sets and public groups:
  - Employment Navigators
  - Employment Navigator Managers
  - VETS Admin

- What procedures are in place to determine which users may access the system and are they documented?

  Any user provisioning in the System needs to be submitted to the O&M team via a service ticket and requires approval from the VETS Business Owners before they can be provisioned.

- How are the actual assignments of roles and Rules of Behavior, verified according to established security and auditing procedures? How often training is provided. Provide date of last training.

  For the application users when they login the first time, Rules of Behavior is displayed and only after accepting the same, they are allowed to access the System.
  System administrators sign the Rules of Behavior pdf document before gaining access.

- Describe what privacy training is provided to users, either generally or specifically relevant to the program or system?

  All Employment Navigators who have access to personal data within the system are DOL contractors, and they complete the annual Cybersecurity and Privacy Awareness training. Additionally, ENs have been trained and have signed the Rules of Behavior document that says they will not use the data from TEN for personal gains or print or share personal information. System has been designed in a way that prevent users from printing reports that includes PII.

- What auditing measures and technical safeguards are in place to prevent misuse of data?

  Individuals do not have direct access to their own data. Employment Navigators enter or modify user data during one-on-one sessions with the users. ENs have been trained and have signed the Rules of Behavior document that says they will not use the data from TEN for personal gains or print or share personal information. System has been designed in a way that prevent users from printing reports that includes PII.

- Is the data secured in accordance with FISMA requirements? If yes, when was Security Assessment and Authorization last completed?

  Yes, December 2021.

- Privacy Impact Analysis

  Individuals do not have direct access to their own data. Employment Navigators enter or modify user data during one-on-one sessions with the users. ENs have been trained and have signed the Rules of Behavior document that says they will not use the data from TEN for personal gains or print or share personal information. System has been designed in a way that prevent users from printing reports that includes PII.

1.10 TECHNOLOGY

The following questions are directed at critically analyzing the selection process for any technologies utilized by the system, including system hardware, biometrics, and other technology.

- Was the system built from the ground up or purchased and installed?

  The System is built on top of Salesforce SAAS

- Describe how data integrity, privacy and security were analyzed as part of the decisions made for your system.

  Data integrity, privacy and security requirements were addressed in each stage of the business process flow:
  Access to the application: Rules of Behavior clearly detailing the Dos and don'ts were displayed to users when they login first time and only after consent, they were allowed access to the application. Single Sign-on was implemented to ensure secure access to the application.
  Data collection: Privacy Act statements, Encryption and Masking of Social Security Number and clear SOP to Navigators were developed to ensure data integrity
  Access to Data: Clearly defined Role Matrix that identifies data elements and access levels to each persona in the system ensured security

- What design choices were made to enhance privacy?

  - Login flows were implemented to display Rules of Behavior detailing the Dos and don'ts were displayed to users when they login first time and only after consent, they were allowed access to the application
  - Transaction Security policy (as part of Salesforce Shield offering) was implemented to prevent any user from exporting PII data outside the System
  - Data Masking and encryption of Social Security Number was implemented to prevent data spillage

- For systems in development, what stage of development is the system in, and what project development life cycle was used?

  Agile was the development lifecycle used in delivering the application. Minimum Viable Product (MVP) has been released in production and there are 2 more key phases planned for future releases.

- For systems in development, does the project employ technology that may raise privacy concerns? If so, please discuss their implementation?

  All the configurations and development of the system are performed within the confines of the platform toolsets and there are no privacy concerns.

1.11 DETERMINATION

As a result of performing the PIA, what choices has the agency made regarding the information technology system and collection of information?

VETS has completed the PIA for TEN which is currently in operation. VETS has determined that the safeguards and controls for this Moderate system adequately protect the information.

VETS has determined that it is collecting the minimum necessary information for the proper performance of a documented agency function.

1.12 PIA SIGNATURE PAGE

Responsible Officials

Edward Meyman
System Owner

EDWARD MEYMAN Digitally signed by EDWARD MEYMAN Date: 2022.05.26 15:27:20 -04'00'

Signature of System Owner *Date*

APPENDIX A: DEFINITIONS FOR PII AND PII ELEMENTS THIS SYSTEM COLLECTS

Non-Sensitive PII. PII whose disclosure cannot reasonably be expected to result in personal harm. Examples include first/last name; e-mail address; business address; business telephone; and general education credentials that are not linked to or associated with any protected PII.

Protected PII. PII whose disclosure could result in harm to the individual whose name or identity is linked to that information. Examples include, but are not limited to, social security number; credit card number; bank account number; residential address; residential or personal telephone; biometric identifier (image, fingerprint, iris, etc.); date of birth; place of birth; mother's maiden name; criminal records; medical records; and financial records. The conjunction of one data element with one or more additional elements increases the level of sensitivity and/or propensity to cause harm in the event of compromise.

What information about individuals will be collected, generated, shared, and/or retained? Also, note whether the collection is for ☐ Federal employees, ☐ Contractor staff, ☐ Members of the Public {Check all that apply}

- ☒ Prefix or title, such as Mr., Mrs., Ms., Jr. Sr. ☐
- ☒ First name ☒ Middle initial and/or ☒ Last name
- ☒ Name suffix such as Jr. Sr., etc.
- ☐ Date of birth
- ☐ Place of birth
- ☐ Mother's maiden name
- ☒ SSN
- ☐ SSN [truncated]
- ☐ SSN [elongated]
- ☐ Language spoken
- ☒ Military, immigration, or other government-issued identifier
- ☐ Photographic identifiers (i.e., photograph image, x-rays, video)
- ☐ Biometric identifier (i.e., fingerprint, voiceprint, iris)
- ☐ Other physical identifying information (e.g., tattoo, birthmark)
- ☐ Vehicle identifier (e.g., license place, VIN)
- ☐ Driver's license number
- ☐ Residential address
- ☐ Personal phone numbers (e.g., phone, fax, cell)

- ☐ Mailing address (e.g., P.O. Box)
- ☐ Personal e-mail address
- ☐ Business address
- ☐ Business phone number (e.g., phone, fax, cell)
- ☒ Business e-mail address
- ☐ Medical information including physician's notes
- ☐ Medical record number
- ☐ Device identifiers (e.g., pacemaker, hearing aid)
- ☐ Employer Identification Number (EIN)/Taxpayer Identification Number (TIN)
- ☐ Financial account information and/or number (e.g., checking account number, PIN, retirement, investment account)
- ☐ Certificates (e.g., birth, death, marriage)
- ☐ Legal documents or notes (e.g., divorce decree, criminal records)
- ☒ Educational records
- ☐ Network logon credentials (e.g., username and password, public key certificate)
- ☐ Digital signing or encryption certificate
- ☐ Other: _____
- ☐ None

- Is any part of the PII collection voluntary?

  First Name, Last Name and Email Address are the only required fields

- Is any part of this PII collection voluntary?

  First Name, Last Name and Email Address are the only required fields

- If any part of the PII collection is voluntary, what efforts are being made to redact, mask, anonymize or eliminate PII from this system?

  Data Masking and encryption of Social Security Number was implemented to prevent data spillage