U.S. DEPARTMENT OF LABOR

Office of the Chief Information Officer

SENIOR COMMUNITY SERVICE EMPLOYMENT PROGRAM (SCSEP)
PRIVACY IMPACT ASSESSMENT

VERSION 1.8

DOCUMENT 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
11/27/21	Privacy Impact Assessment	Adrienne Ramirez	Annual Review and Updates
10/18/22	Privacy Impact Assessment	DISPP	Removal of PII Data Extract Guide question

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**

TABLE OF CONTENTS

PRIVACY IMPACT ASSESSMENT QUESTIONNAIRE

(To be completed for information systems containing PII)

1.1 OVERVIEW

The Employment and Training Administration (ETA)s Senior Community Service Employment Program (SCSEP) authorized by title V of the Older American's Act, is the only federally sponsored employment and training program targeted specifically to low-income, older individuals who want to enter or re-enter the workforce. The SCSEP system built on Department of Labor's Case Management Platform's (DOLCMP) Appian Platform as a Service (PaaS) is owned and managed by OASAM.

SCSEP participants provide their PII to their case manager (third-party) to be able to process and determine eligibility for the program. This system does not share or transact information with other systems. The system must create a PIA due to the nature of the information that it stores, collects, and reviews.

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?

  Information is being collected on elderly members of the public.

- Why is the Information being collected?

  The information is being collected to determine eligibility of grants and to track performance of the participants.

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

  Name, DOB, Address, SSN, Phone number, ethnicity

- How is the PII collected?

  The PII maintained in system is not directly collected from SCSEP participants (applicants). PII provided to the case manager (third-party) who then enters data into SCSEP as part of the process to determine eligibility of grants and to track performance of the participants.

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

  Participants applying to the SCSEP do not have direct access to the system. Third-party case workers enter data submitted and will review with a background check to confirm the PII collected is accurate.

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

  HR 1319 ARPA Subtitle D Elder Justice and Support Guarantee

- Privacy Impact Analysis

  The SCSEP systems account roles are managed centrally. Third-party users (case workers) with access to the system, who are determined through awarded proposals, reviews the cases that are submitted. External users use Login.Gov to authenticate to SCSEP through the DOLCMP portal. The data will be protected and stored within DOLGSS AWS Oracle RDS DB. Oracle encryption functions (AES256 encryption) - encrypted in transit and at rest. Tools are not being used to aggregate the data, but the data will be used to determine eligibility for the program.

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

  Name, DOB, Address, SSN, and personal phone number and ethnicity will be used to track participant performance and properly pay participants. This information allows the case workers to accurately run background checks and determine eligibility.

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

  Encryption on SSN, Date of birth. Oracle encryption functions (AES256 encryption) - encrypted in transit and at rest. There are no tools being used to aggregate the data.

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

  No, this system is not taking data and creating anything new.

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

  No – the information is not commercial or publicly available.

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

  Yes, a SORN has been published in the Federal Register.

- Privacy Impact Analysis

  SCSEP is a FedRAMP and NIST Moderate systems that implement all controls within each baseline. SCSEP does not use public data or have tools to aggregate that data and employs encryption for data at rest and in transit, therefore making the risk to the system minimal.

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?

  Data is retained as long as it is needed to determine suitability.

- Is a retention period established to minimize privacy risk?

  Yes - SCSEP follows the DOL established retention period that minimizes risk to the public.

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

  Yes

- 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?

  SCSEP will follow DOL policies regarding record retention, and NARA schedule, to ensure that PII that is no longer needed will be eliminated in accordance with proper retention polices.

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

  PII is no longer required when any assessment or applicable Federal records retention requirements have been satisfied.

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

  Anonymization or masking is not feasible as the information is used to determine participant eligibility.

- Privacy Impact Analysis

  Based on the privacy implementations listed above and security requirements, SCSEP is operating in alignment with DOL policies and procedures and follows ETAs agency-wide NARA schedule. We are mitigating risks ensuring the users acknowledge the risks of sharing information and to only provide information that is necessary.

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?

  Information is not shared externally. PII is reviewed by the SCSEP case workers and Program Analysts. Application administrators also have access to PII.

- How is the PII transmitted or disclosed?

  PII is encrypted and store internally on the DOLGSS AWS Oracle RDS DB only. This means that the data is stored and protected within the DOL network and environment. The system collects data but does not transmit the collected data.

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

  Yes. ETA only stores information for as long as it's necessary to determine the grant eligibility. Each applicant will be measured against a list of criteria and have a background check executed to determine eligibility. Once the determination is made, the SCSEP caseworkers will be allowed to properly dispose of the data.

- Privacy Impact Analysis

  The system is not sharing information, just collecting it and reviewing it for suitability for the grant. PII is not shared and the number of users who have access to it is minimal therefore the risk is low. Exposure of participant data is a risk, and mitigation strategies include database encryption, encryption of the VPN tunnel that connects Appian to the Oracle RDS database, and encryption of key data at rest (SSN, Date of Birth) for all participants.

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?

  PII held within the system cannot be shared externally.

- 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.

  There is no information sharing outside of the Department of Labor.

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

  The data within the system is only utilized internally and not shared outside the agency.

- How is the information transmitted or disclosed?

  The data within the system is only utilized internally and not shared outside the agency.

- 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.

  N/A- The data within the system is only utilized internally and not shared outside the agency.

- How is the shared information secured by the recipient?

  N/A- The data within the system is only utilized internally and not shared outside the agency.

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

N/A- The data within the system is only utilized internally and not shared outside the agency.

- Privacy Impact Analysis

  The data within the system is only utilized internally and not shared outside the agency. The system is not sharing information, just ingesting it and reviewing it for suitability. By not sharing data outside of the network DOL has minimized the level of risk for information sharing. Exposure of participant data is a risk, and mitigation strategies include database encryption, encryption of the VPN tunnel that connects Appian to the Oracle RDS database, and encryption of key data at rest (SSN, Date of Birth) for all participants.

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, participants sign releases acknowledging the use of PII for grant purposes only. However, system does not collect participant information directly from user. Information is collected by the case manager (third-party)

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

  It's voluntary, they sign up to see if they qualify and the PII collected is necessary to properly track and pay participants. If they do not want to share PII then they do not have to sign up for the program.

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

  It's voluntary, they sign up to see if they qualify and the PII collected is necessary to properly track and pay participants. If they do not want to share PII then they do not have to sign up for the program. The only information needed is required to be used, and it can only be used for purposes stated in the grant agreement.

- Privacy Impact Analysis

  DOL minimizes the risk by having the user sign a release to provide the PII. This means that the user willing shares the PII and has been adequately notified of the purpose of its collection.

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?

  Participants do not have direct access to the system. They can contact their case manager to access their information.

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

  Participants do not have direct access to the system. Once a request has been formally submitted, the participant would need to notify their case manager that an error exists in their information. The Program Analyst would update the information in the system.

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

  Participants do not have direct access to the system. Once a request has been formally submitted, if participants see an error or need to change data (name change for example), they may contact their case manager for the change. The Program Analyst makes the change after the case manager approves it.

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

  There is no formal notification, but the process is in the above explanation

- Privacy Impact Analysis

  Participants do not have direct access to the system. Once a request has been submitted, updates are made by case manager and their employees. No outside individual has access to make changes therefore decreasing the level of risk.

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.)

  Program Analysts and application administrators will have general access to the system and external registered users will have limited access to only the case data that pertains to their organization(s). These users include grantee and sub-grantee administrators, case managers, and supervisors.

- 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

  Yes – contractors will have access to the system. PWS's can be found in the Miscellaneous artifacts tab in CSAM.

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

  SCSEP users are comprised of program analysts (DOL users), system administrators, and external users. There is a user/roles matrix. The User Roles Matrix was uploaded as an artifact and can be found in CSAM.

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

  The DOLCMP user guide determines the roles and access for all applications built on DOLCMP.

- 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.

  Assignments of roles for external users are done by contacting the program office when a new user registers for access to the system via login.gov. The program office or the organization's administrators will assign roles using a utility built into the application to provide access to the correct roles within the organization. Internal user assignment will be done through the platform-wide User Access Management (UAM) application managed by the Common Operating Environment (CoE). All new users will need to access the rules of behavior upon logging into the system for the first time and this is

tracked in the database. Cybersecurity and Privacy Awareness (CSPA) Training is required for all DOL employees and contractors annually through the DOL Learning Link system. Training assigned to users must be completed by the deadline as established in LearningLink.

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

  DOL provides initial awareness and training to all DOL employees and contractors before granting access to DOL network and system resources. Additionally, basic privacy awareness training is provided to all DOL users as part of the annual CSPA training. Users with significant security responsibilities are required to complete annual Role-Based Training.

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

  Users must be logged in via login.gov or via the DOL VPN on GFE. DOLCMP utilizes a central auditing capability that is built into Appians platform. All auditing executed by DOLCMPs would be at the platform level.

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

  Appian as a platform is FISMA certified

- Privacy Impact Analysis

  Exposure of participant data is a risk, and mitigation strategies include database encryption, encryption of the VPN tunnel that connects Appian to the Oracle RDS database, and encryption of key data at rest (SSN, Date of Birth) for all participants.

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 an upgrade/migration from a Legacy system and was built from the ground up by duplicating and enhancing existing functionality.

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

  Data integrity was analyzed by utilizing the legacy application to model the database and making improvements to the data structure to improve data quality. Data mapping from the legacy system to the modernized application has been done as part of data migration activities and will ensure greater data integrity in the future. Utilizing a more normalized data structure, implementing foreign key for referential integrity, and developing real-time data validations before data is saved to the database ensures that data quality will improve over the legacy application. Privacy and security concerns are addressed by limiting access to the data based on role membership and organization association. Additionally, security controls are in place to encrypt data at rest and in transit to protect sensitive data from the public.

- What design choices were made to enhance privacy?

  Authentication for all external users is done via Login.gov which is Fedramp certified and requires multi-factor authentication. Appian as a platform is also Fedramp and FISMA certified and utilizes role-based access to ensure that users only see data pertinent to them. The connection from Appian to the Oracle RDS database occurs over an encrypted VPN tunnel and sensitive data like SSN and Date of Birth are encrypted at rest.

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

  SCSEP is in the operations phase and was developed following the DOL Software Development Life Cycle Management (SDLCM) Manual.

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

  SCSEP is in the operation phase

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?

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

ETA 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

Ravi Kotti
SCSEP System Owner

RAVI KOTTI Digitally signed by RAVI KOTTI Date: 2023.02.03 08:19:52 -05'00'

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: ____Ethnicity___
- ☐ None

- Is any part of the PII collection voluntary?

  Yes – populating the document to understand eligibility is completely optional.

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

  N/A - There is currently no effort to execute this for SCSEP.