Privacy Impact Assessment for the VA IT System called:

Status Query Response and Exchange System (SQUARES)

Veterans Health Administration Homeless Program Office (VHA HPO)

Date PIA submitted for review:

10/20/2021

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Rita Grewal	Rita.Grewal@va.gov	202-632-7861
Information System Security Officer (ISSO)	Jim Boring	*James.Boring@va.gov*	*202-842-2000 x 4613*
Information System Owner	Mike Domanski	*Michael.Domanski@va.gov*	*727-595-7291*

Abstract

The abstract provides the simplest explanation for "what does the system do?" and will be published online to accompany the PIA link.

The goal of SQUARES is to allow homeless service providers outside the VA — especially, but not exclusively, VA Homeless Program Grantees associated with Supportive Services for Veteran Families (SSVF), Grant and Per Diem (GPD), and Contract Emergency Residential Services (CERS) to quickly determine homeless individuals' eligibility for Veteran homeless programs. Identity attributes (Name, Date of Birth, Social Security Number, and Gender) are entered using the single or bulk search features of SQUARES. SQUARES invokes the VA Master Person Index (MPI) web services using the identity attributes; if the person matches to a known individual, MPI returns the DoD EDI Person Identifier (EDI PI) and the authoritative identity data for the individual. This EDI PI is then used to invoke the enterprise Military Information Service (eMIS) which queries the VA/DoD Identity Repository (VADIR) to retrieve the individual's military history and return it to SQUARES, where it is evaluated to determine potential eligibility for VA programs. The application is being hosted by the FedRAMP approved Salesforce GovCloud.

Overview

The overview is the most important section of the PIA. A thorough and clear overview gives the reader the appropriate context to understand the responses in the PIA. The overview should contain the following elements:

- *The IT system name and the name of the program office that owns the IT system.*
- *The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.*
- *Indicate the ownership or control of the IT system or project.*
- *The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.*
- *A general description of the information in the IT system and the purpose for collecting this information.*
- *Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.*
- *Whether the system is operated in more than one site, and if so, a description of how use of the system and PII is maintained consistently in all sites and if the same controls are used across sites.*
- *A citation of the legal authority to operate the IT system.*
- *Whether the completion of this PIA will result in circumstances that require changes to business processes*
- *Whether the completion of this PIA could potentially result in technology changes*
- *If the system is in the process of being modified and a SORN exists, will the SORN require amendment or revision and approval? If the system is using cloud technology, does the SORN for the system cover cloud usage or storage?*

SQUARES Advanced Veteran Search Overview

- The Status Query Response and Exchange System (SQUARES) is owned by the Homeless Program under the Veterans Health Administration.
- Status Query and Response Exchange System (SQUARES) is a VA web application that provides VA employees and external homeless service organizations with reliable, detailed information about Veteran eligibility. Users submit identity attributes for homeless individuals (name, date of birth, social security number, gender) and SQUARES returns information regarding their Veteran status and eligibility for homeless programs. The tool facilitates quick and simple access to care for homeless and at-risk Veterans. SQUARES directly supports the HPO's mission of ending Veteran homelessness because of its unique ability to empower external organizations with the use of Veteran data. This is also a top priority for the agency
- The IT system is owned by the VHA HPO, and is controlled under the Salesforce ATO
- Individuals whose information is collected in the system consists of the ~2300 users of the system's names, emails and organization's names. The typical client of the system is a person identifying themselves as a Veteran.
- Other information in the IT system includes reference guides about system usage, and about Veteran eligibility. No client (i.e. Veteran) information is collected in the system. This information is not "collected" but it is present to assist users. Veteran data is not collected in the system.
- No information sharing is conducted by the IT system (other than minor user information mentioned above). There are no modules or subsystems of SQUARES.
- SQUARES is only operated on one website but is operated at hundreds of physical sites across the country. The secure, 2 factor authenticated access to the system is present at all physical sites where SQUARES is used. PII is maintained consistently within the internal back-end data source where it was temporarily pulled from in SQUARES, but not stored. All sites utilize controls outlined in the Data Use Agreement for the allowable usage of PII.
- SQUARES is housed on the Salesforce platform, which has an ATO at VA,
- No business processes will need to change as a result of this PIA
- Completion of this PIA will result in technology changes, chiefly the introduction of the Advanced Search feature, which connects SQUARES to 3 additional VA/DOD data sources
- SORN provided is 138VA005Q, this will need to be updated. The system also uses cloud technology which is covered in the SORN.

Section 1. Characterization of the Information

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

1.1 What information is collected, used, disseminated, created, or maintained in the system?

Identify and list all Sensitive Personal Information (SPI) that is collected and stored in the system, including Individually Identifiable Information (III), Individually Identifiable Health Information (IIHI), Protected Health Information (PHI), and Privacy- Protected Information. For additional information on these information types and definitions, please see VA Directives and Handbooks in the 6500 series (https://vaww.va.gov/vapubs/). If the system creates information (for example, a score, analysis, or report), list the information the system is responsible for creating.

If a requesting system receives information from another system, such as a response to a background check, describe what information is returned to the requesting system.
This question is related to privacy control AP-1, Authority To Collect, and AP-2, Purpose Specification.

The information selected below must match the information provided in question 2.1 as well as the data elements columns in 4.1 and 5.1.

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional SPI is collected, used, disseminated, created, or maintained, please list those in the text box below:

- ☒ Name
- ☒ Social Security Number
- ☒ Date of Birth
- ☐ Mother's Maiden Name
- ☐ Personal Mailing Address
- ☐ Personal Phone Number(s)
- ☐ Personal Fax Number
- ☐ Personal Email Address
- ☐ Emergency Contact Information (Name, Phone Number, etc. of a different individual)
- ☐ Financial Account Information
- ☐ Health Insurance Beneficiary Numbers Account numbers
- ☐ Certificate/License numbers
- ☐ Vehicle License Plate Number
- ☐ Internet Protocol (IP) Address Numbers
- ☐ Current Medications
- ☐ Previous Medical Records
- ☐ Race/Ethnicity
- ☐ Tax Identification Number
- ☐ Medical Record Number
- ☒ Gender
- ☐ Integration Control Number (ICN)
- ☐ Military History/Service Connection
- ☐ Next of Kin
- ☒ Other Unique Identifying Information (list below)

Alias
Cadency
Date of Death
Death Indicator
VA ID
Service Number
Service Component
Character of Service
Separation Code
Enter on Duty Date(s)

Release from Active Duty Date(s)
Non Pay Days
Pay Plan Paygrade

PII Mapping of Components

SQUARES consists of 4 key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by SQUARES and the reasons for the collection of the PII are in the table below.

PII Mapped to Components

Note: Due to the PIA being a public facing document, please do not include the server names in the table.

PII Mapped to Components

Database Name of the information system collecting/storing PII	Does this system collect PII? (Yes/No)	Does this system store PII? (Yes/No)	Type of PII (SSN, DOB, etc.)	Reason for Collection/ Storage of PII	Safeguards
Beneficiary Identification Records Locator Subsystem	Yes	Yes	SSN, DOB, Name, Sex, Death Date	Administration of VBA benefits across all VBA Lines of Business	Access Levels to limit privileges to view data for sensitive individuals; use of login accounts granted on a need-only basis
Veterans Health Information System and Technology Architecture/ Administrative Data Repository	Yes	Yes	SSN, DOB, Name, Sex, Death Date	Administration of VA healthcare benefits across all VA medical facilities and associated health-related applications	Use of login accounts granted on a need-only basis; most users access the data in the original source, VistA, which has its own authentication mechanisms to ensure secure access. VistA also contains PHI so access is actively managed.
United States Veterans/Social Security Administration Verification	Yes. The Social Security Administration (SSA) is the main system of records within the US	Yes	SSN, DOB, Name, Sex, Death Indicator (death date is supplied in the Social Security Death Index but here is only a Y/N indicator)	Multiple uses across government and the private sector; for VA purposes, this	The data access is managed by OEI and access is granted to systems as appropriate. This copy as used by SQUARES in the SLVSS service as a

	Government for the issuance of SSN and the tracking of all verified traits that accompany it: F/M/L Name, DOB, Sex			file contains all the Veteran and Military identities submitted by the USVETS database (part of the Office of Enterprise Integration) to the SSA for verification; it does not contain all citizens; only those for which OIE found some evidence of military service.	fallback source of potential Veterans who are unknown to BIRLS and VistA but for whom some indication of prior service exists. This is used by SQUARES to determine when military service information is to be sought from the applicant for service periods otherwise unknown to VA. It will also used in the future when adding a previously unknown identity to the Master Person Index (MPI) to ensure that the traits used to create the identity are SSA-verified as correct.
va.my.salesforce.co Salesforce GovCloud (FedRAMP) Specific IP addresses: 96.43.152.0 -- 96.43.1	Yes	Yes	• Veteran Type (Title 38 Status) • Character of Discharge (whether served honorably or otherwise, per active duty period) • Narrative Reason for Separation, per active duty per • First//Middle/Last Name/Suffix • Date of Birth • Social Security Number • Gender • Veteran Eligibility	Multiple uses across government to match veterans with services	Access Levels to limit privileges to view data for sensitive individuals; use of login accounts granted on a need-only basis

1.2 What are the sources of the information in the system?

List the individual, entity, or entities providing the specific information identified above. For example, is the information collected directly from the individual as part of an application for a benefit, or is it collected from other sources such as commercial data aggregators?

Describe why information from sources other than the individual is required. For example, if a program's system is using data from a commercial aggregator of information or data taken from public Web sites, state the fact that this is where the information is coming from and then in question 1.3 indicate why the system is using this source of data.

If the system creates information (for example, a score, analysis, or report), list the system as a source of information.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

There are two types of information used in the system, some of which overlaps.

Input information is collected from the client (i.e. the Veteran).

Output information is required to determine if the client is a verified Veteran, and to determine if their service qualifies them for homeless benefits and services.

The system does not create information or store it in any form.

VA data sources: Beneficiary Identification Records Locator Subsystem, Veterans Health Information System and Technology Architecture/ Administrative Data Repository, United States Veterans/Social Security Administration Verification

1.3 How is the information collected?

This question is directed at the means of collection from the sources listed in question 1.2. Information may be collected directly from an individual, received via electronic transmission from another system, or created by the system itself. Specifically, is information collected through technologies or other technology used in the storage or transmission of information in identifiable form?

If the information is collected on a form and is subject to the Paperwork Reduction Act, give the form's OMB control number and the agency form number.
This question is related to privacy controls DI-1, Data Quality, and IP-1, Consent.

Information is collected verbally/physically and input into form within system. Data points collected can include: First Name, Last Name, DOB, Gender, SSN

Connected back-end data sources display the following non-SPI/PII information:

- Enter on Duty (EOD) Date
- Release from Active Duty (RAD) Date
- Separation Code
- Non Pay Days
- Pay Plan / Pay Grade
- Character of Service
- Service
- Component
- Death Indicator

1.4 How will the information be checked for accuracy? How often will it be checked?

Discuss whether and how often information stored in the system is checked for accuracy. Is information in the system checked against any other source of information (within or outside your organization) before the information is used to make decisions about an individual? For example, is there a computer matching agreement in place with another government agency? For systems that receive data from internal data sources or VA IT systems, describe the system checks to ensure that data corruption has not occurred during transmission.

If the system checks for accuracy by accessing a commercial aggregator of information, describe this process and the levels of accuracy required by the contract.
This question is related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

SQUARES is not a system that checks for accuracy of input data, that is accomplished via Internal systems connected to SQUARES.

1.5 What specific legal authorities, arrangements, and agreements defined the collection of information?

List the full legal authority for operating the system, specifically the authority to collect the information listed in question 1.1. Provide the authorities in a manner understandable to any potential reader, i.e., do not simply provide a legal citation; use statute names or regulations in addition to citations. Legal authorities include Federal laws, regulations, statutes, and Executive Orders.
This question is related to privacy control AP-1, Authority to Collect

VA SORN 23VA10NB3 "Non-VA Care (Fee) Records-VA" provides legal authority for operation.

1.6 <u>PRIVACY IMPACT ASSESSMENT: Characterization of the information</u>

Consider the specific data elements collected and discuss the potential privacy risks and what steps, if any are currently being taken to mitigate those identified risks.

Consider the following Fair Information Practice Principles (FIPPs) when assessing the risk to individual privacy:

Principle of Purpose Specification: Explain how the collection ties with the purpose of the underlying mission of the organization and its enabling authority.

Principle of Minimization: Is the information directly relevant and necessary to accomplish the specific purposes of the program?

Principle of Individual Participation: Does the program, to the extent possible and practical, collect information directly from the individual?

Principle of Data Quality and Integrity: Are there policies and procedures for VA to ensure that personally identifiable information is accurate, complete, and current?
This question is related to privacy control AR-1, Governance and Privacy Program, and AR-2, Privacy Impact and Risk Assessment.

Follow the format below when entering your risk assessment:
Privacy Risk:

The information displayed on the screen to the end user is relevant for them determining an eligibility status for the Veteran in question.

The end user of the system does collect information directly from the individual for purposes of running a search to verify their identity and service information, not for any medical purposes.

The PII that is temporarily displayed belongs to official VA data sources, therefore it is checked for accuracy there.

Mitigation: Access Controls – 2 factor authentications, signed agreement with VA on data usage (DUA), permission-based access on need-to-know basis, Encryption in transit.

Section 2. Uses of the Information

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

2.1 Describe how the information in the system will be used in support of the program's business purpose.

Identify and list each use (both internal and external to VA) of the information collected or maintained.
This question is related to privacy control AP-2, Purpose Specification.
SQUARES operates under Veteran Experience Office Eligibility & Enrollment and VHA Homeless Program Office to support the mission of ending Veteran Homelessness. Users utilize search data from return to search to determine a person's Veteran status, and their eligibility for homeless programs.

Data elements are split up into two categories, inputs and outputs. They and are used in the following ways, by both internal VA users and external Community users, within the SQUARES Community:

- Input data: First/Last Name, DOB, SSN, Gender
    - Use: any combination of the above data elements are entered to execute an Advanced Search to find a Veteran
- Output data: the final 14 data elements in the SPI list in section 1.1
    - Those 14 fields are: **Alias, Cadency, Date of Death, Death Indicator, VA ID, Service Number, Service, Component, Character of Service, Separation Code, Enter on Duty Date(s), Release from Active Duty Date(s), Non Pay Days, Pay Plan Paygrade**
    - Use: To enable the user to ascertain whether or not the person searched for is a Veteran, and if they are, to determine if they had qualifying military service for VA homeless services
    - Note: There are different combinations of the above 14 fields that can help the end user make the Veteran status and homeless services eligibility determinations

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

Many systems sift through large amounts of information in response to a user inquiry or programmed functions. Systems may help identify areas that were previously not obvious and need additional research by agents, analysts, or other employees. Some systems perform complex analytical tasks resulting in, among other types of data, matching, relational analysis, scoring, reporting, or pattern analysis. Describe any type of analysis the system conducts and the data that is created from the analysis.

If the system creates or makes available new or previously unutilized information about an individual, explain what will be done with the newly derived information. Will it be placed in the individual's existing record? Will a new record be created? Will any action be taken against or for the individual identified because of the newly derived data? If a new record is created, will the newly created information be accessible to Government employees who make determinations about the individual? If so, explain fully under which circumstances and by whom that information will be used.
This question is related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information

Data in transit is protected via a secure connection to the API/middleware that passes data from the source to the application, and encryption in transit.
Data at rest is protected via Access Controls and an auto-clear process.

The system does not retain data, however Social Security Numbers that are displayed on screen are partially hidden to only display the last 4 digits. The SSN search field also auto-hides characters as they're typed in.

2.3 How is the information in the system secured?

2.3a What measures are in place to protect data in transit and at rest?

2.3 b If the system is collecting, processing, or retaining Social Security Numbers, are there additional protections in place to protect SSNs?

This question is related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest

Data in transit is protected via a secure connection to the API/middleware that passes data from the source to the application, and encryption in transit.
Data at rest is protected via Access Controls and an auto-clear process.

The system does not retain data, however Social Security Numbers that are displayed on screen are partially hidden to only display the last 4 digits. The SSN search field also auto-hides characters as they're typed in.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information. How is access to the PII determined? Are criteria, procedures, controls, and responsibilities regarding access documented? Does access require manager approval? Is access to the PII being monitored, tracked, or recorded? Who is responsible for assuring safeguards for the PII?

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above. Example: Describe if training for users of the project covers how to appropriately use information. Describe the disciplinary programs or system controls (i.e. denial of access) that are in place if an individual is inappropriately using the information.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Is the PIA and SORN, if applicable, clear about the uses of the information?

Principle of Use Limitation: Is the use of information contained in the system relevant to the mission of the project?
This question is related to privacy control AR-4, Privacy Monitoring and Auditing, AR-5, Privacy Awareness and Training, and SE-2, Privacy Incident response.

Access controls are in place to ensure that only approved users can access the SQUARES search features. There is system training that users are required to complete before applying for access with manager approval. There are reminders throughout the system reminding users not to transmit PII without encryption.

Section 3. Retention of Information

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

3.1 What information is retained?

Identify and list all information collected from question 1.1 that is retained by the system. This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal

The SQUARES Advanced Search does not retain data.

3.2 How long is information retained?

In some cases VA may choose to retain files in active status and archive them after a certain period of time. State active file retention periods, as well as archived records, in number of years, for the information and record types. For example, financial data held within your system may have a different retention period than medical records or education records held within your system, please be sure to list each of these retention periods. If the system is using cloud technology, will it be following the NARA approved retention length and schedule?

The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are implemented.
This question is related to privacy control DM-2, Data Retention and Disposal.

The SQUARES Advanced Search does not retain data.

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)? If so please indicate the name of the records retention schedule.

An approved records schedule must be obtained for any IT system that allows the retrieval of a record via a personal identifier. The VA records officer will assist in providing a proposed schedule. The schedule must be formally offered to NARA for official approval. Once NARA approves the proposed schedule, the VA records officer will notify the system owner.
This question is related to privacy control DM-2, Data Retention and Disposal.

The SQUARES Advanced Search does not retain data.

3.4 What are the procedures for the elimination of SPI?

Explain how records are destroyed or eliminated at the end of the retention period. Please give the details of the process. For example, are paper records shredded on site, or by a shredding company and accompanied by a certificate of destruction, etc?
This question is related to privacy control DM-2, Data Retention and Disposal

Search results are auto-cleared when navigating to other pages within system. Session management auto-clears results and logs users out after 15 minutes of inactivity.

3.5 Does the system, where feasible, use techniques to minimize the risk to privacy by using PII for research, testing, or training?

Organizations often use PII for testing new applications or information systems prior to deployment. Organizations also use PII for research purposes and for training. These uses of PII increase the risks associated with the unauthorized disclosure or misuse of the information. Please explain what controls have been implemented to protect PII used for testing, training and research. Have policies and procedures been developed to minimize the use of PII for testing, training, and research?
This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research

PII is only used for testing in a pre-PROD environment by administrative use only, with Single Sign On (SSO) access controls.

3.6 <u>PRIVACY IMPACT ASSESSMENT: Retention of information</u>

Discuss the risks associated with the length of time data is retained and what steps, if any, are currently being taken to mitigate those identified risks.

While we understand that establishing retention periods for records is a formal process, there are policy considerations behind how long a project keeps information. The longer a project retains information, the longer it needs to secure the information and assure its accuracy and integrity. The proposed schedule should match the requirements of the Privacy Act to keep the minimum amount of PII for the minimum amount of time, while meeting the Federal Records Act. The schedule should align with the stated purpose and mission of the system.

Consider the following FIPPs below to assist in providing a response:

<u>Principle of Minimization:</u> Does the project retain only the information necessary for its purpose? Is the PII retained only for as long as necessary and relevant to fulfill the specified purposes?

<u>Principle of Data Quality and Integrity:</u> Has the PIA described policies and procedures for how PII that is no longer relevant and necessary is purged?

This question is related to privacy controls DM-1, Minimization of Personally Identifiable Information, and DM-2, Data Retention and Disposal.

Follow the format below:
Privacy Risk:

Data is not retained, and search results are auto-cleared when logging out, or when navigating to a new page within the system, so there is no privacy risk.

Mitigation: Access to search data is restricted to only those users with a need to know. Search data is auto-cleared by the system.

Section 4. Internal Sharing/Receiving/Transmitting and Disclosure

The following questions are intended to define the scope of information sharing/receiving/transmitting within VA.

4.1 With which internal organizations is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?
NOTE: Question 3.10 (second table) on Privacy Threshold Analysis should be used to answer this question.

Identify and list the names of any program offices, contractor-supported IT systems, and any other organization or IT system within VA with which information is shared.

State the purpose for the internal sharing. If you have specific authority to share the information, provide a citation to the authority.

For each interface with a system outside your program office, state what specific data elements (PII/PHI) are shared with the specific program office, contractor-supported IT system, and any other organization or IT system within VA.

Describe how the information is transmitted. For example, is the information transmitted electronically, by paper, or by some other means? Is the information shared in bulk, on a case-by-case basis, or does the sharing partner have direct access to the information?
This question is related to privacy controls AP-2, Purpose Specification, AR-3, Privacy Requirements for Contractors and Service Providers, AR-8, Accounting of Disclosures, TR-1, Privacy Notice, and UL-1, Internal Use.

Data Shared with Internal Organizations

List the Program Office or IT System information is shared/received with	***List the purpose of the information being shared /received with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program Office or IT system***	***Describe the method of transmittal***
Office of Veterans Health Administration (VHA) Enrollment and Eligibility Records	Critical web service connection to	SSN, DOB, Name, Sex, Death Date, Death Indicator	Electronically pulled from VHA via the E&E web service. System of record number (SORN#): 147VA10NF1. Data is returned for specifically queried individuals
Office of Veterans Health Administration (VHA) VA Identity and Service Services Master Person Index (MPI)	Critical data source connection to transform SSN into an EDIPI for a data return in the advanced search	SSN, DOB, Name, Sex, Death Date, Death Indicator	Electronically pulled from VHA. System of record number (SORN#): 121VA10P2. MPI records are returned for specifically queried individuals via MPI's search services
Office of the Secretary of Veterans Affairs / Office of Veterans Experience Veterans Affairs / Department of Defense Identity Repository (VADIR)	Critical data source connection to return data in the advanced search (See above)	SSN, DOB, Name, Sex, Death Date, Death Indicator SSN, DOB, Name, Sex, Death Date, Death Indicator	Electronically pulled from VHA via eMIS, a web service maintained by VIERS. System of record number (SORN#): 138VA005Q. Data is returned for specifically queried individuals.

4.2 PRIVACY IMPACT ASSESSMENT: Internal sharing and disclosure

Discuss the privacy risks associated with the sharing of information within the Department and what steps, if any, are currently being taken to mitigate those identified risks.
This question is related to privacy control UL-1, Internal Use.

Follow the format below:
Privacy Risk:

There are minor inherent risks with the sharing of information from colleague to colleague both within the Department and within the external organizations that use SQUARES.

Mitigation:

Access to search data is restricted to only those users with a need to know. Search data is auto-cleared by the system. Users understand that the data they have access to is only to be used to materially advance the goal of ending Veteran homelessness. If a user is aware of theft, loss, or compromise of any device used to access Veteran sensitive information, or if there is a leak of sensitive information, they are to immediately report the incident to the VA POC outlined in their agreement.

Section 5. External Sharing/Receiving and Disclosure

The following questions are intended to define the content, scope, and authority for information sharing external to VA, which includes Federal, State, and local governments, and the private sector.

5.1 With which external organizations (outside VA) is information shared/received? What information is shared/received, and for what purpose? How is the information transmitted and what measures are taken to ensure it is secure?

Is the sharing of information outside the agency compatible with the original collection? If so, is it covered by an appropriate routine use in a SORN? If not, please describe under what legal mechanism the IT system is allowed to share the information in identifiable form or personally identifiable information outside of VA.

NOTE: Question 3.11 on Privacy Threshold Analysis should be used to answer this question.
Identify and list the names of any Federal, State, or local government agency or private sector organization with which information is shared.

For each interface with a system outside VA, state what specific data elements (PII/PHI) are shared with each specific partner.

What legal mechanisms, authoritative agreements, documentation, or policies are in place detailing the extent of the sharing and the duties of each party? For example, is the sharing of data compatible with your SORN? Then list the SORN and the applicable routine use from the SORN. Is there a Memorandum of Understanding (MOU), Computer Matching Agreement (CMA), or law that mandates the sharing of this information?

Describe how the information is transmitted to entities external to VA and what security measures have been taken to protect it during transmission.
This question is related to privacy control UL-2, Information Sharing with Third Parties

Data Shared with External Organizations

List External Program Office or IT System information is shared/received with	***List the purpose of information being shared / received / transmitted with the specified program office or IT system***	***List the specific PII/PHI data elements that are shared/received with the Program or IT system***	***List the legal authority, binding agreement, SORN routine use, etc. that permit external sharing (can be more than one)***	***List the method of transmission and the measures in place to secure data***
N/A				

5.2 PRIVACY IMPACT ASSESSMENT: External sharing and disclosure

Discuss the privacy risks associated with the sharing of information outside the Department and what steps, if any, are currently being taken to mitigate those identified risks.

Discuss whether access controls have been implemented and whether audit logs are regularly reviewed to ensure appropriate sharing outside of the Department. For example, is there a Memorandum Of Understanding (MOU), contract, or agreement in place with outside agencies or foreign governments.
Discuss how the sharing of information outside of the Department is compatible with the stated purpose and use of the original collection.
This question is related to privacy control AR-2, Privacy Impact and Risk Assessment, AR-3, Privacy Requirements for Contractors and Service Providers, and AR-4, Privacy Monitoring and Auditing

Follow the format below:
Privacy Risk: There are inherent minor risks with sharing information between colleagues within an external organization.

Mitigation: Access Controls – 2 factor authentication, signed agreement with VA on data usage (DUA), permission-based access on need-to-know basis, Encryption in transit.

Section 6. Notice

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

6.1 Was notice provided to the individual before collection of the information? If yes, please provide a copy of the notice as an appendix. (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.) If notice was not provided, why not?

This question is directed at the notice provided before collection of the information. This refers to whether the person is aware that his or her information is going to be collected. A notice may include a posted privacy policy, a Privacy Act statement on forms, or a SORN published in the Federal Register. If notice was provided in the Federal Register, provide the citation.

If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Describe how the notice provided for the collection of information is adequate to inform those affected by the system that their information has been collected and is being used appropriately. Provide information on any notice provided on forms or on Web sites associated with the collection. This question is related to privacy control TR-1, Privacy Notice, and TR-2, System of Records Notices and Privacy Act Statements, and TR-3, Dissemination of Privacy Program Information.

There is no VA-dictated notice provided to Veterans prior to the collection of their information. Individual shelters/organizations may or may not have their own privacy act statement.

6.2 Do individuals have the opportunity and right to decline to provide information? If so, is a penalty or denial of service attached?

This question is directed at whether the person from or about whom information is collected can decline to provide the information and if so, whether a penalty or denial of service is attached. This question is related to privacy control IP-1, Consent, IP-2, Individual Access, and IP-3, Redress

Individuals (Veterans) have the right to decline to provide personal information. If so, they cannot be serviced. There is no "denial of service attached."

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

This question is directed at whether an individual may provide consent for specific uses or the consent is given to cover all uses (current or potential) of his or her information. If specific consent is required, how would the individual consent to each use?
This question is related to privacy control IP-1, Consent

Individuals (Veterans) do have the right to consent to only specific uses of their personal information. Namely for search/verification purposes. They exercise this right verbally.

6.4 <u>PRIVACY IMPACT ASSESSMENT: Notice</u>

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks.

Consider the following FIPPs below to assist in providing a response:

Principle of Transparency: Has sufficient notice been provided to the individual?

Principle of Use Limitation: Is the information used only for the purpose for which notice was provided either directly to the individual or through a public notice? What procedures are in place to ensure that information is used only for the purpose articulated in the notice?
This question is related to privacy control TR-1, Privacy Notice, AR-2, Privacy Impact and Risk Assessment, and UL-1, Internal Use

Follow the format below:
Privacy Risk: There is no official, recommended VA-mandated policy for users to read to individuals (Veterans).

Mitigation: Individual shelters/organizations may or may not have their own privacy act statement.

Section 7. Access, Redress, and Correction

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

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

Cite any procedures or regulations your program has in place that allow access to information. These procedures, at a minimum, should include the agency's FOIA/Privacy Act practices, but may also include additional access provisions. For example, if your program has a customer satisfaction unit, that information, along with phone and email contact information, should be listed in this section in addition to the agency's procedures. See 5 CFR 294 and the VA FOIA Web page at http://www.foia.va.gov/ to obtain information about FOIA points of contact and information about agency FOIA processes.

If the system is exempt from the access provisions of the Privacy Act, please explain the basis for the exemption or cite the source where this explanation may be found, for example, a Final Rule published in the Code of Federal Regulations (CFR).

If the system is not a Privacy Act system, please explain what procedures and regulations are in place that covers an individual gaining access to his or her information.
This question is related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

Veterans do not have access to SQUARES, so there is no procedure in place.

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

Describe the procedures and provide contact information for the appropriate person to whom such issues should be addressed. If the correction procedures are the same as those given in question 7.1, state as much.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

SQUARES does not have a system-supported, automated process for this. There is not a two-way connection to any external data source.
An end user can reach out to their assigned VA Medical Center (VAMC) for the correct process to address data inaccuracies.

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

How are individuals made aware of the procedures for correcting his or her information? This may be through notice at collection or other similar means. This question is meant to address the risk that even if procedures exist to correct information, if an individual is not made fully aware of the existence of those procedures, then the benefits of the procedures are significantly weakened.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

An end user can reach out to their assigned VA Medical Center (VAMC) for the correct process to address data inaccuracies.

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

Redress is the process by which an individual gains access to his or her records and seeks corrections or amendments to those records. Redress may be provided through the Privacy Act and Freedom of Information Act (FOIA), and also by other processes specific to a program, system, or group of systems.
This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Example: Some projects allow users to directly access and correct/update their information online. This helps ensures data accuracy.

An end user can reach out to their assigned VA Medical Center (VAMC) for the correct process to address data inaccuracies. (Note: Veterans are never end uses of SQUARES)

7.5 PRIVACY IMPACT ASSESSMENT: Access, redress, and correction

Discuss what risks there currently are related to the Department's access, redress, and correction policies and procedures for this system and what, if any, steps have been taken to mitigate those

risks. For example, if a project does not allow individual access, the risk of inaccurate data needs to be discussed in light of the purpose of the project. For example, providing access to ongoing law enforcement activities could negatively impact the program's effectiveness because the individuals involved might change their behavior.

Consider the following FIPPs below to assist in providing a response:
Principle of Individual Participation: Is the individual provided with the ability to find out whether a project maintains a record relating to him?

Principle of Individual Participation: If access and/or correction is denied, then is the individual provided notice as to why the denial was made and how to challenge such a denial?

Principle of Individual Participation: Is there a mechanism by which an individual is able to prevent information about him obtained for one purpose from being used for other purposes without his knowledge?
This question is related to privacy control IP-3, Redress.

Follow the format below:
Privacy Risk: Because SQUARES is not the system of record for Veteran information, nor does it have the ability to correct erroneous information, there is the propensity for incorrect information remain that way and keep the Veteran from accessing services.

Mitigation: An end user can reach out to their assigned VA Medical Center (VAMC) for the correct process to address data inaccuracies.

Section 8. Technical Access and Security

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

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

Describe the process by which an individual receives access to the system.

Identify users from other agencies who may have access to the system and under what roles these individuals have access to the system. Who establishes the criteria for what PII can be shared?

Describe the different roles in general terms that have been created to provide access to the system. For example, certain users may have "read-only" access while others may be permitted to make certain amendments or changes to the information.

This question is related to privacy control AR-7, Privacy-Enhanced System Design and Development.

External users go through the application process, which includes gaining a VA endorsement, signing a Data Use Agreement, completing a training module, applying for access via AccessVA/ID.me portals, and being approved by their organization's manager.

Internal users (i.e. VA employees who already have Salesforce access) submit a web-to-case form via the Salesforce platform, for approval by the SQUARES Admin team.

8.2 Will VA contractors have access to the system and the PII? If yes, what involvement will contractors have with the design and maintenance of the system? Has a contractor confidentiality agreement, Business Associate Agreement (BAA), or a Non-Disclosure Agreement (NDA) been developed for contractors who work on the system?

If so, how frequently are contracts reviewed and by whom? Describe the necessity of the access provided to contractors to the system and whether clearance is required. If Privacy Roles and Responsibilities have been established to restrict certain users to different access levels, please describe the roles and associated access levels. Explain the need for VA contractors to have access to the PII.

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, VA contractors have access to the system. Their only access to PII is in the Staging (pre-PROD) for testing purposes.

All VA contractors complete a security and awareness training during the onboarding process, prior to receiving system access.

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

VA offers privacy and security training. Each program or system may offer training specific to the program or system that touches on information handling procedures and sensitivity of information. Please describe how individuals who have access to PII are trained to handle it appropriately.
This question is related to privacy control AR-5, Privacy Awareness and Training.

There is specified SQUARES training for end users, required before they can apply for access.

8.4 Has Authorization and Accreditation (A&A) been completed for the system?

If Yes, provide:

1. *The Security Plan Status,*

2. *The Security Plan Status Date,*
3. *The Authorization Status,*
4. *The Authorization Date,*
5. *The Authorization Termination Date, .*
6. *The Risk Review Completion Date*
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH).*

Please note that all systems containing SPI are categorized at a minimum level of "moderate" under Federal Information Processing Standards Publication 199.

If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

Salesforce has an approved security plan as 24 Feb 2021 and a full ATO, through October 2024. SQUARES current has a moderate Data Security Categorization.

Section 9 – Technology Usage

The following questions are used to identify the technologies being used by the IT system or project.

9.1 Does the system use cloud technology? If so, what cloud model is being utilized?

If so, Does the system have a FedRAMP provisional or agency authorization? If the system does use cloud technology, but does not have FedRAMP authorization, explain how the Cloud Service Provider (CSP) solution was assessed and what FedRAMP documents and processes were used for the assessment in order to comply with VA Handbook 6517. Types of cloud models include: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

Note: For systems utilizing the VA Enterprise Cloud (VAEC), no further responses are required after 9.1.

Yes, Salesforce GovCloud has FedRAMP authorization

9.2 Identify the cloud model being utilized.

Example: Software as a Service (SaaS), Infrastructure as a Service (IaaS), Platform as a Service (PaaS), Commercial off the Shelf (COTS).

This question is related to privacy control UL-1, Information Sharing with Third Parties.

PaaS

9.3 Does the contract with the Cloud Service Provider, Contractors and VA customers establish who has ownership rights over data including PII? (Provide contract number and supporting information about PII/PHI from the contract)

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

The Salesforce application (SQUARES) does not have ownership over any PII data.

Contract number: T4NG-0534 | VA-20-00037251

9.4 Will the CSP collect any ancillary data and if so, who has ownership over the ancillary data?

Per NIST 800-144, cloud providers hold significant details about the accounts of cloud consumers that could be compromised and used in subsequent attacks. Ancillary data also involves information the cloud provider collects or produces about customer-related activity in the cloud. It includes data collected to meter and charge for consumption of resources, logs and audit trails, and other such metadata that is generated and accumulated within the cloud environment.

This question is related to privacy control DI-1, Data Quality.

Meta data and audit trails are only captured if specifically set to do so on the system's backend

9.5 NIST 800-144 states, "Organizations are ultimately accountable for the security and privacy of data held by a cloud provider on their behalf." Is this principle described in contracts with customers? Why or why not?

What are the roles and responsibilities involved between the organization and cloud provider, particularly with respect to managing risks and ensuring organizational requirements are met?

This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.

Yes, reference the Data Use Agreement

9.6 If the system is utilizing Robotics Process Automation (RPA), please describe the role of the bots.

Robotic Process Automation is the use of software scripts to perform tasks as an automated process that executes in parallel with or in place of human input. For example, will the automation move or touch PII/PHI information. RPA may also be referred to as "Bots" or Artificial Intelligence (AI).

No

Section 9. References

Summary of Privacy Controls by Family

Summary of Privacy Controls by Family

ID	Privacy Controls
AP	**Authority and Purpose**
AP-1	Authority to Collect
AP-2	Purpose Specification
AR	**Accountability, Audit, and Risk Management**
AR-1	Governance and Privacy Program
AR-2	Privacy Impact and Risk Assessment
AR-3	Privacy Requirements for Contractors and Service Providers
AR-4	Privacy Monitoring and Auditing
AR-5	Privacy Awareness and Training
AR-7	Privacy-Enhanced System Design and Development
AR-8	Accounting of Disclosures
DI	**Data Quality and Integrity**
DI-1	Data Quality
DI-2	Data Integrity and Data Integrity Board
DM	**Data Minimization and Retention**
DM-1	Minimization of Personally Identifiable Information
DM-2	Data Retention and Disposal
DM-3	Minimization of PII Used in Testing, Training, and Research
IP	**Individual Participation and Redress**
IP-1	Consent
IP-2	Individual Access
IP-3	Redress
IP-4	Complaint Management
SE	**Security**
SE-1	Inventory of Personally Identifiable Information
SE-2	Privacy Incident Response
TR	**Transparency**
TR-1	Privacy Notice
TR-2	System of Records Notices and Privacy Act Statements
TR-3	Dissemination of Privacy Program Information
UL	**Use Limitation**

ID	Privacy Controls
UL-1	Internal Use
UL-2	Information Sharing with Third Parties

Signature of Responsible Officials

The individuals below attest that the information provided in this Privacy Impact Assessment is true and accurate.

RITA K GREWAL 114938

Digitally signed by RITA K GREWAL 114938
Date: 2021.11.12 15:38:30 -05'00'

Privacy Officer, Rita Grewal

James C. Boring 149438

Digitally signed by James C. Boring 149438
Date: 2021.11.18 13:48:48 -05'00'

Information Security Systems Officer, Jim Boring

Michael S. Domanski 326889

Digitally signed by Michael S. Domanski 326889
Date: 2021.11.22 10:15:01 -05'00'

System Owner, Mike Domanski

APPENDIX A-6.1

Please provide a link to the notice or verbiage referred to in Section 6 (a notice may include a posted privacy policy, a Privacy Act notice on forms).

Data Use Agreement (DUA)…..see below

SQUARES USE AGREEMENT BETWEEN

UNITED STATES DEPARTMENT OF VETERANS' AFFAIRS

1. PREAMBLE. This Agreement is between the United States Department of Veterans Affairs (VA), a department in the executive branch of the Government, and Veterans Housing Program for (also called the "Partner Organization"). Collectively, the two organizations are also called the "Parties".
2. AUTHORITY. The activities performed under this Agreement by VA are authorized pursuant to 38 U.S.C. § 7301(b) and 38 U.S.C. Chapter 20.
3. PURPOSE. VA is engaged in a campaign to functionally end Veteran homelessness nationwide. As the key housing programs under this campaign are administered by VA and coordinated by outside non-profit organizations, collaboration between these entities is essential to reliably identify all Veterans experiencing homelessness and target the highest-intensity resources to the highest-need

   Veterans. SQUARES facilitates this coordination by synthesizing Veteran eligibility information from VA providing it to front-line case managers who provide services to homeless Veterans. SQUARES improves coordination between providers, limits time spent on manual eligibility determinations, and increases the coverage and efficiency of homeless services for Veterans.

4. SCOPE. Each Party will provide its own resources in order to accomplish the responsibilities and goals outlined in this agreement.
5. DISCLOSURE AUTHORITY. The authority for VA to disclose to the Partner Organization per this agreement is found in the HIPAA Privacy Rule, 45 C.F.R. Parts 160 and 164, and the Privacy Act, 5 U.S.C. § 552a; 38 U.S.C. § 570; and their implementing regulations.
6. PRIVACY AND SECURITY. Both Parties agree to safeguard any personally identifying information (PII) in accordance with their respective privacy and security standards. The Partner Organization may not utilize the name or address of any veteran obtained from VA other than for the conduct of programs and utilization of benefits under USC Title 38, except for such data already in possession of the Partner Organization. 38 U.S.C. § 5701(f).
7. RESPONSIBILITIES OF VA. VA will provide the Partner Organization access to SQUARES.
8. RESPONSIBILITIES OF THE PARTNER ORGANIZATION. The Partner Organization must use the data disclosed through SQUARES to materially advance the goal of functionally ending homelessness among Veterans. This may include any or all of the following:
   1. Participating in community-wide provider meetings to coordinate and plan services for Veterans experiencing homelessness, based on data provided by SQUARES,

2. Providing outreach services to homeless Veterans not yet engaged in permanent housing programs, based on data provided by SQUARES,
3. Providing permanent housing to homeless Veterans, based on data provided by SQUARES,
4. Making homeless Veterans aware of other services available to them, based on data provided by
   SQUARES,
5. Providing oversight and coordination of the various organizations serving homeless Veterans, based on data provided by SQUARES.

The Partner Organization must appoint a SQUARES Manager who will control SQUARES access for other Partner Organization staff. The SQUARES Manager is responsible for ensuring that he/she approves access only for qualified Partner Organization staff members, with a business need to access SQUARES. The Manager is also responsible for deactivating SQUARES accounts within two (2) business days when a specific staff member no longer requires access to the data due to transfer, resignation, termination, or for some other reason.

9. FINANCIAL COST OR REIMBURSEMENT. Each Party will pay its own costs to participate in this program, and there will be no cost exchange, payment, or reimbursement between the Parties.
10. POINTS OF CONTACT. For VA: Leisa Davis. , for the Partner Organization: .
11. SECURITY INCIDENTS. VA Handbook 6500.2, Management of Data Breaches Involving Sensitive Personal Information (SPI), governs the reporting of incidents involving VA systems and information. If the Partner Organization's employee, contractor, or agent becomes aware of the theft, loss, or compromise of SQUARES or of any device used to transport, access, or store VA sensitive information or data, such employee, agent, or contractor must immediately report the incident to the VA Point of Contact (POC) listed in Paragraph 10 so that the incident can be reported to the VA Network Security Operations Center (VA-NSOC) for action.
12. MISCELLANEOUS
    1. Representation and Warranty; Liability. VA makes no representation or warranty as to the accuracy of the information received from SQUARES, or as to its fitness for a particular purpose. Each Party acknowledges and agrees that any claim or cause of action arising from this Agreement shall be governed by the Federal Tort Claims Act or other appropriate federal authority. Federal Statute of Limitations provisions shall apply to any breach or claim.
    2. Third Parties. This Agreement creates no rights, obligations, or claims between third parties and VA or the Partner Organization.
    3. Applicable Law: This Agreement shall be governed by and interpreted and enforced in accordance with the laws of the United States of America without reference to conflict of laws. To the extent permitted by federal law, the laws of the State of the Partner Organization (excluding choice of law rules) will apply in the absence of applicable federal law.
    4. Modification of Agreement: This Agreement may be modified at any time by VA. VA will provide written notice to the Partner Organization's POC in Paragraph 10 not less than thirty (30) days before the proposed modification will take effect.
    5. Dispute Resolution: Disputes arising from the application of the terms of the Agreement shall be handled beginning with the POCs listed in Paragraph 10. Should disputes not be resolved at the initial level, the areas of disagreement will be reduced to writing by each Party, and presented to the authorized officials at both Parties for resolution. If settlement

cannot be reached at this level, the disagreement will be raised to the next level in accordance with each Party's procedures for final resolution.

6. No endorsement:The Partner Organization agrees that VA's name, seals, trademarks, logos, service marks, or trade names shall not be used by the Partner Organization in such a manner as to state or imply that the Partner Organization is endorsed, sponsored, or recommended by VA or by any other element of the Federal Government. The Partner Organization agrees not to use VA's name or display any VA or government seals, trademarks, logos, service marks, and trade names unless permission to do has been granted in advance and in writing by VA or by other relevant federal government authority.

13. DURATION AND TERMINATION. This agreement shall be effective until termination by either Party. Either Party may terminate this agreement upon written notice to the non-terminating Party's POC in Paragraph 10 not less than thirty (30) days before the proposed termination date. The requirement for thirty (30) days' notice may be waived by mutual written consent of both Parties.
14. IMPLEMENTATION: This Agreement shall be implemented upon signing by authorized VA and Community Partner officials.