Privacy Impact Assessment for the VA IT System called:

Staff Sergeant Parker Gordon Fox Suicide Prevention Grant Program Data Collection Tool (SGSS)

Office of Mental Health and Suicide Prevention

Veterans Health Administration

Date PIA submitted for review:

7/22/2022

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Kamilah Jackson	kamilah.jackson@va.gov	513-288-6988
Information System Security Officer (ISSO)	Karen McQuaid	karen.mcquaid@va.gov	(708) 403-5311
Information System Owner	Jeffrey Rabinowitz	jeffrey.rabinowitz@va.gov	732-720-5711

Abstract

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

Staff Sergeant Parker Gordon Fox Suicide Prevention Grant Program (SSG Fox SPGP) Data Collection Tool is used to collect mental health assessment data from Veterans that will be enrolled in the SSG Fox SPGP. The data will provide grantees an assessment of Veterans well-being, mental health, and other de-identified at risk factors for suicide. The software is a forms-based data collection tool that only allows for the structured data capture and includes capture of general outreach activities by grantees, eligibility screening for participation in the program, general demographics (non-identifying data), and types of services that will be delivered. The data will be used by internal VA Clinical staff with the Office of Mental Health and Suicide Prevention Services and the MITRE Data Analytics Team, a third-party, independent assessor to assess the effectiveness of the program, ensuring grantees are referring Veterans into VA care for treatment when appropriate.

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?*

SSG Fox SPGP Data Collection Tool is a tool that will be used to collect data from participants in the SSG Fox SP Grant Program. That data will be used to evaluate service delivery effectiveness, monitoring of grantee compliance, and ensuring grantees are making the required referrals to VA care. Ultimately the tool will be used to develop evaluative statements of the overall effectiveness of the SSG Fox SPGP. The system is owned by Office of Mental Health and Suicide Prevention and will be managed by SSG Fox SPGP staff as well as 3rd party contractors MITRE and CSD. The number of individuals who will have information stored in the system is difficult to ascertain at this point given the grant program has not yet started. However, a rough estimate would be 80 grantees each serving on avg. 50 eligible participants for a total of 4000. In addition, the SSG Fox SPGP Data Collection Tool is used to collect mental health assessment data from Veterans, their family members, and potentially active-duty military that will be enrolled in the SSG Fox SPGP. The data will provide grantees an assessment of Veterans well-being, mental health, and other de-identified at risk factors for suicide. The software is a forms-based data collection tool that only allows for structured data capture and includes capture of general outreach activities by grantees, eligibility screening for participation in the program, general demographics (non-identifying data), and types of services that will be delivered. There will be no information sharing with the use of the data collection tool, the tool does not interface with any other systems internal or external to the VA. Access to the system will be restricted to appropriate VA OMHSP staff, grantee staff and appropriate 3rd party contractor staff. The system will be hosted in the VA Enterprise Cloud and not have more than one location of use. Legal authority to operate exists under Section 201 (1) (A) and (B) of the Hannon Act https://www.congress.gov/bill/116th-congress/senate-bill/785

Completion of this PIA will not require a change to business processes will require a change to technology. The system is cloud based and covered by SORN 173VA005OP2: https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf

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)

PII Mapping of Components

SSG Fox SPGP Data Collection Tool>consists of <0> key components (databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by **SSG Fox SPGP Data Collection Tool** > 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.
The first table of 3.9 in the PTA should be used to answer this question.

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
N/A					

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.

- Participant PII is entered by grantees. No other sources are used for PII
- The system creates scores from mental health assessment responses according to standardized scoring criteria. This is de-identified scoring with no PII or PHI associated.
- Score analysis will be done through read-only dashboards generated within data collection tool. No reports will be printed or stored outside the system.

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 through participant interview at enrollment and entered in the data collection tool by grantee staff as well as direct input from the participant throughout participation in the program.

OMB Control Number 2900-0904

Form Nos: 10-315a, 10-315b, 10-316a, 10-316b, 10-316c, 10-316d, 10-316e, 10-316e, 10-316f, 10-317a, 10-317b, 10-317c, 10-317d

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.

Data collected by grantee staff is via face-to-face or telephonic interview and entered in the data collection tool. The data is verified with the participant in the face-to-face interview or over the telephone and will also be compared to other source documentation to help determine eligibility (i.e. a DD-214) and/or SQUARES. System checks will be completed to validate completeness on a daily basis and will not be compared to other sources of information (i.e. commercial aggregator). Accuracy of participant contact information is then checked via use: the grantee will use this information to send mental health assessment links so participants can provide self-reported data.

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

Legal authority to operate exists under Section 201 (1) (A) and (B) of the Hannon Act https://www.congress.gov/bill/116th-congress/senate-bill/785

The system is cloud based and covered by SORN 173VA005OP2:
https://www.govinfo.gov/content/pkg/FR-2021-11-08/pdf/2021-24368.pdf

1.6 PRIVACY IMPACT ASSESSMENT: Characterization of the information

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 SSG Fox SPGP Data Collection tool holds only the most limited PII necessary in order to support contact with participants for program operations: email addresses and telephone numbers of participants. These data elements are collected by grantee staff from participants. Participant contact is necessary to send mental health assessment links so participants can provide self-reported data.

PII data are held in separate zones from assessment and services data. The system itself is subject to the same threats as all VA Enterprise Cloud hosted systems.

Mitigation: VA Enterprise Cloud controls including Access Control, Audit and Accountability; VA system controls including Awareness and Training, Security Assessment and Authorization, Configuration Management, Contingency Planning, Identification and Authentication, Incident Response, Media Protection, Personnel Security, Physical and Environmental Protection, Risk Assessment, System and Services Acquisition, System and Communications Protection, System and Information Integrity, and Planning.

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.

- SSN: Used to create unique identifier (not stored)
- DOB: Used to create unique identifier (not stored)
- Email address: Used to contact participant
- Phone number: Used to contact participant

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

No PII data is involved with any reporting or analysis. Data is aggregated to evaluate individual grantee and overall program effectiveness. Reports will be generated with the tool to show enrollment, service provision, aggregated standard mental health assessment scoring and overall program implementation and execution measures. No individual data or linkable data are used or reported.

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?

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

2.3c How is PII/PHI safeguarded in accordance with OMB Memorandum M-06-15?

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

PII is strictly limited to those elements required for program operations and are encrypted at rest and transmitted only over secure VA network using HTTPS.

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.

Add answer here:

Access to PII that is stored (email and phone number) is determined by VA through grantee award determination and system controls (training, role determination, user access controls). If it is determined that information is being inappropriately used, access to the system can/will be denied via user account management processes currently in development.

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 information listed in Section 1.1 is retained in the SSG Fox SPGP data collection tool database and not deleted. However, SSN and DOB are only collected for the purposes of creating a unique identifier using a hash. Once created, the SSN and DOB are not stored.

- Social Security Number
- Date of Birth
- Phone number
- Email address

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 'data' in this case refers to all SSG Fox SPGP Data Collection tool data. The participant's record is to be maintained indefinitely. National Archives and Records Administration (NARA) guidelines as stated in Records Control Schedule (RCS) 10-1 record policy, 1009.2 (pg 33) & 1009.3 (pg 34). The p*articipant and grantor records captured during grant program will be destroyed 3 years after final action is taken on the file, but longer retention is authorized if required for OMHSP business per 1009.2.*
https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

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 data retention period has been approved by NARA and is processed according to the following:

- Records Control Schedule 10-1 link for VHA: www.va.gov/vhapublications/rcs10/rcs10-1.pdf
- Records Control Schedule VB-1, Part II Revised for VBA: www.benefits.va.gov/WARMS/docs/admin20/rcs/part2/part2.pdf
- National Archives and Records Administration: www.nara.go

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

Data is not removed from SSG Fox SPGP Data Collection Tool. The status of the participant can be changed, but policy is to never remove a record. Data is retained until the system is decommissioned or migrated to a new replacement system.

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

All IT system and application development and deployment is handled by VA OI&T. VHA does test new or modified IT systems for VHA operations prior to deployment, and PII/PHI may be used for that Alpha or Beta testing at the facility-level per VHA policy. In addition, VHA may need to train staff on functionality in the new or modified IT system. Training, including on IT systems, is part of health care operations and per VHA policy PII and PHI may be used for that training purpose. However, VHA must minimize the use of PII and PHI in training presentations or materials per VA policy. In case human subject research was intended to be covered by this control: VA Research investigators may use PII for VA Institutional Review Board (IRB)-approved research, and there is no effort to minimize the use of PII for research. Controls for protecting PII used for testing, training and research are often security controls if the PII is electronic. When paper PII, reasonable safeguards for protecting the PII are to be employed.

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:

Principle of Minimization: *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?*

Principle of Data Quality and Integrity: *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: There is a risk that the information contained in the system will be retained for longer than is necessary to fulfill the VA mission.

Mitigation: All personnel with access to Veteran's information are required to complete the VA Privacy and Information Security Awareness & Rules of Behavior training annually.
SSG Fox SPGP adheres to all information security requirements instituted by the VA Office of Information and Technology (OI&T).

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? NONE.

NOTE: Question 3.9 (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 processed (shared/received/transmitted) with the Program Office or IT system***	***Describe the method of transmittal***
N/A			

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 is very little risk in collection data via the SSG Fox SPGP Data Collection Tool. Information may be compromised through shoulder surfing what may result in a breach of confidentiality.

Mitigation: The VA Rules of Behavior are required to be signed by all personnel prior to accessing any VA related equipment according to VA Directive and Handbook 6500. Only authorized users have access. Role based accessed for VA activity is restricted by least privilege account management. Penalties are executed to the full extension of the law if a breach in confidentiality is determined.

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 3.10 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 processed (shared/received/transmitted) 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				

**PII Is not shared from this system.

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: As SSG Fox SPGP Data Collection tool does not share data with any outside organizations, there are minimal to no privacy risks to the data collected, stored, and maintained in the system.

Mitigation: The key mitigation to any privacy risk related to external sharing of VA data from the SSG Fox SPGP Data Collection tool hosted on the VAEC is that the system does not connect to or share with any external organizations or systems. Privacy is further secured by storing all data on encrypted cloud servers behind firewalls.

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.

Notice is provided to potential participants on the Eligibility Screening Form with the following statement:

Paperwork Reduction Act and **Privacy Statement:** This information is being collected in accordance with section 3507 of the Paperwork Reduction Act of 1995. Accordingly, we may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB number. We anticipate that the time expended to complete this eligibility screening will average 30 minutes. This includes the time needed to follow instructions, gather the necessary facts, and respond to the questions. This information is being collected to help inform eligibility for services under the SSG Fox SPGP by providing additional background information about the participants to better serve them. Any information provided will be kept private to the extent provided by law. Participation in this program is voluntary, and failure to respond will not have any impact on a participant's entitlement to benefits.

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

Any potential participant may decline to have their information collected and not participate in the program. However, if the individual agrees to participate the data collection is mandatory.

If an individual declines the collection of information, they cannot participate in the respective grantee's program but referrals by the grantee organization will be made for service and any emergency clinical care needed will still be provided.

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

The Privacy Act and VA policy require that personally identifiable information only be used for the purpose(s) for which it is collected, unless consent (opt-in) is granted. Individuals must be provided an opportunity to provide consent for any secondary use of information, such as use of collected information for surveys or marketing purposes.
If the individual wants to consent to a particular use of the information, they can contact the grantee program they are enrolled in for updating of their record within the data collection tool.

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:

<u>Principle of Transparency:</u> Has sufficient notice been provided to the individual?

<u>Principle of Use Limitation:</u> 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 a risk that individuals who provide information to the SSG Fox SPGP Data Collection tool application will not know how their information is being used internally to the Department of Veterans Affairs.

Mitigation: The VA mitigates this risk by providing veterans and other beneficiaries with multiple forms of notice of information collection, retention, and processing. The main forms of notice are discussed in the Privacy Act statement, a System of Record Notice, and the publishing of this Privacy Impact Assessment.

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.

Individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420. Inquiries should, at a minimum, include the person's full name, social security number, type of information requested or contested, their return address, and phone number. See VA SORN: VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2).

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.

Individuals seeking information regarding access to and contesting of records in this system may write the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420. Inquiries should, at a minimum, include the person's full name, social security number, type of information requested or contested, their return address, and phone number. See VA SORN: VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2).

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.

Individuals who wish to determine whether this system of records contains information about them should contact the Director of VA Connected Health, VHA Office of Informatics and Analytics, Department of Veterans Affairs, 810 Vermont Avenue NW, Washington, DC 20420 or via the Web at http://mobilehealth.va.gov. Inquiries should include the person's full name, social security number, and their return address. See VA SORN: VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2).

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.

The individual has the right to request amendment of erroneous information in accordance with the Privacy Act and HIPAA Privacy Rule. Any discrepancies are to be reported to the SSG Fox SPGP staff.

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: There is a risk that members of the public (i.e. participants enrolled in respective grantee programs) will not know the relevant procedures for gaining access to, correcting or contesting their information.

Mitigation: The privacy risk is mitigated by information provided by VA SORN: VA Enterprise Cloud—Mobile Application Platform (Cloud) Assessing (VAEC–MAP) (173VA005OP2). This states that individuals should contact their local VA Regional Office for additional information about accessing and contesting their records at the VA. Furthermore, this document and the SORN provide the point of contact for members of the public who have questions or concerns about the application.

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.

Participant PII (email addresses and telephone numbers) is accessible (read/write) by the grantees via login and passwords, administered by contractors and VA staff developing and managing the system, who will have permissions to view and alter PII if needed.

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.

VA ensures that all personnel take annual security training and pass VA Privacy and Information Security Awareness training.
All users of the SSG Fox SPGP Data Collection tool project team are required to sign a Rules of Behavior agreement prior to being given access to the system. Additionally, the Rules of Behavior is required to be reviewed and signed annually by each user. Annual training for the National Rules of Behavior is performed through the Talent Management System (TMS).
There are two versions of the National Rules of Behavior: one for VA employees and one for contractors.

Definitions of VA employee and VA Contractor:
• VA Employees - VA employees are all individuals who are employed under title 5 or title 38, United States Code, as well as individuals whom the Department considers employees such as volunteers, without compensation employees, and students and other trainees.
• VA Contractors - VA contractors are all non-VA users having access to VA information resources through a contract, agreement, or other legal arrangement. Contractors must meet the security levels defined by the contract, agreement, or arrangement. Contractors must read and sign the Rules of Behavior and complete security awareness and privacy training prior to receiving access to the information systems.

Users agree to comply with all terms and conditions of the National Rules of Behavior, by signing a certificate of training at the end of the training session.

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.

VA requires Privacy and Information Security Awareness & Rules of Behavior training to be completed on an annual basis. The Talent Management System offers the following applicable privacy courses:
VA 10176: Privacy and Information Security Awareness and Rules of Behavior
VA 10203: Privacy and HIPPA Training
VA 3812493: Annual Government Ethics

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.***

In process, IOC date September 28, 2022

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, VA Enterprise Cloud (VAEC) AWS

9.2 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.

N/A

9.3 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.

N/A

9.4 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.

N/A

9.5 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).

N/A

Section 10. 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.

KAMILAH M. JACKSON 105810

Digitally signed by KAMILAH M. JACKSON 105810
Date: 2022.08.24 16:16:10 -04'00'

Privacy Officer, Kamilah Jackson

Karen A. McQuaid 321576

Digitally signed by Karen A. McQuaid 321576
Date: 2022.08.25 07:37:45 -05'00'

Information System Security Officer, Karen McQuaid

JEFFREY RABINOWITZ

Digitally signed by JEFFREY RABINOWITZ
Date: 2022.08.24 14:50:32 -04'00'

Information System Owner, Jeffrey Rabinowitz

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).

Paperwork Reduction Act and **Privacy Statement:** This information is being collected in accordance with section 3507 of the Paperwork Reduction Act of 1995. Accordingly, we may not conduct or sponsor, and you are not required to respond to, a collection of information unless it displays a valid OMB number. We anticipate that the time expended to complete this eligibility screening will average 30 minutes. This includes the time needed to follow instructions, gather the necessary facts, and respond to the questions. This information is being collected to help inform eligibility for services under the SSG Fox SPGP by providing additional background information about the participants to better serve them. Any information provided will be kept private to the extent provided by law. Participation in this program is voluntary, and failure to respond will not have any impact on a participant's entitlement to benefits.