Privacy Impact Assessment for the VA IT System called:

Login.gov-e (LG-e)

Office of Chief Technology Officer

VACO

Date PIA submitted for review:

03/27/2023

System Contacts:

System Contacts

	Name	E-mail	Phone Number
Privacy Officer	Tonya Facemire	Tonya.facemire@va.gov	202-632-8423
Information System Security Officer (ISSO)	Carol Phan	Carol.Phan@va.gov	415-221-4810
Information System Owner	Scottie Ross	Scottie.Ross@va.gov	478-595-1349

Abstract

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

Login.gov-e (LG-e) is an authentication platform that makes the public's online interactions with the U.S. government simpler, more efficient, and intuitive. The system is a single, secure platform owned and operated by GSA through which members of the public can sign in and access information and services from participating federal agencies ("partner agencies"). LG-e reduces the burden of operations, maintenance, and security oversight for partner agencies

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:

1 General Description

A. The IT system name and the name of the program office that owns the IT system.

LG-e is a FedRAMP authorized system hosted on Amazon Web Services (AWS), owned and operated by GSA. The VA has an interagency agreement with GSA to use LG-e.

B. The business purpose of the program, IT system, or technology and how it relates to the program office and agency mission.

The Office of CTO uses LG-e as an identity proofing system as an option for Veteran's and Dependents. The potential roll would be for every Veteran and anticipate 6,000,000 users.

C. Indicate the ownership or control of the IT system or project.

LG-e is a FedRAMP authorized system hosted on Amazon Web Services (AWS), owned and operated by GSA. The VA has an interagency agreement with GSA to use LG-e.

2. Information Collection and Sharing

D. The expected number of individuals whose information is stored in the system and a brief description of the typical client or affected individual.

Up to 6 million veteran users

E. A general description of the information in the IT system and the purpose for collecting this information.

LG-e manages user authentication by allowing users to sign in with an email address, password, and multi-factor method. LG-e manages identity proofing by verifying an individual's asserted identity through third-party identity proofing services on behalf of partner agencies. PII collected to identity proof a user includes full name, birth date, physical address, social security number, and contact phone number. When a user attempts to access a service or record offered or maintained by a partner agency, the individual will be directed off the partner agency's technical infrastructure and to LG-e. Users will be notified through the application interface what the system is used for, and how it will use their PII, if applicable. Users must authorize before proceeding. The information requested by the system and asserted back to the partner agency will be only what is necessary to establish access at the appropriate assurance level. In VA's case, the only information provided back to VA from LG-e with the user's consent is the user's email address and a unique user identification (UUID) created by GSA for VA. If the VA requires identity proofing information for a user authenticating with LG-e, then a user's self-asserted PII, including name, address, social security number, birth date and/or contact number could also be transmitted to the VA to be matched with existing information, or to create a new identity stored by the VA. It is only used to identity proof an individual. The system will be integrated with SSOe and managed by IAM. Key Aspects of Integration: (1) VA may use LG-e PII for a newly created identity (2) data entered into LG-e by a user is collected by GSA per their existing SORN (82FR37451). Data shared with VA is covered under VA SORNs 150VA19 and 138VA005Q. (3) data that is collected by GSA per their SORN is used to match existing data that is held by VA Completion of the PIA will not result in change of business practice or technology changes. Legal authority to operate - Per 1.6: 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and 40 USC § 501. GSA SORNs renew every 3 years and VA SORNs every 6 years

F. Any information sharing conducted by the IT system. A general description of the modules and subsystems, where relevant, and their functions.

If the VA requires identity proofing information for a user authenticating with LG-e, then a user's self-asserted PII, including name, address, social security number, birth date and/or contact number could also be transmitted to the VA to be matched with existing information, or to create a new identity stored by the VA. It is only used to identity proof an individual. The system will be integrated with SSOe and managed by IAM

G. 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.

LG-e is a FedRAMP authorized system hosted on Amazon Web Services (AWS), owned and operated by GSA. The VA has an interagency agreement with GSA to use LG-e.

3. Legal Authority and SORN

H. A citation of the legal authority to operate the IT system.

Key Aspects of Integration: (1) VA may use LG-e PII for a newly created identity (2) data entered into LG-e by a user is collected by GSA per their existing SORN (82FR37451). Data shared with VA is covered under VA SORNs 150VA19 and 138VA005Q. (3) data that is collected by GSA per their SORN is used to match existing data that is held by VA Completion of the PIA will not

result in change of business practice or technology changes. Legal authority to operate - Per 1.6: 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and 40 USC § 501

I. 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?

The current SORNs cover the operation of the system.

D. System Changes

J. Whether the completion of this PIA will result in circumstances that require changes to business processes

No

K. Whether the completion of this PIA could potentially result in technology changes

No

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	☒ Personal Mailing Address	☐ Personal Fax Number
☒ Social Security Number	☒ Personal Phone Number(s)	☒ Personal Email Address
☒ Date of Birth		☐ Emergency Contact Information (Name, Phone
☐ Mother's Maiden Name		

Number, etc. of a different individual)
☐ Financial Information
☐ Health Insurance Beneficiary Numbers Account numbers
☒ Certificate/License numbers*
☐ Vehicle License Plate Number
☐ Internet Protocol (IP) Address Numbers
☐ Medications
☐ Medical Records
☐ Race/Ethnicity
☐ Tax Identification Number
☐ Medical Record Number
☐ Gender
☐ Integrated Control Number (ICN)
☐ Military History/Service Connection
☐ Next of Kin
☒ Other Data Elements (list below)

Other: UUID – Universally Unique Identifier and Agency Universally Unique Identifier. PIV/CAC subject

PII Mapping of Components (Servers/Database)

LG-e consists of 1 key components (servers/databases). Each component has been analyzed to determine if any elements of that component collect PII. The type of PII collected by LG-e and the reasons for the collection of the PII are in section 3.1.

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.

Internal Database Connections

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?
These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.2a 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?

The Veteran or dependent will sign up for an account with LG-e through the following link (https://login.gov/create-an-account/). The identity proofing process between the LG-e system and third-party identity proofing services takes place after the user provides the required account information

1.2b 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 indicate why the system is using this source of data.

The Veteran or dependent will sign up for an account with LG-e through the following link (https://login.gov/create-an-account/). The identity proofing process between the LG-e system and third-party identity proofing services is needed to verify a user's identity and takes place after the user provides the required account information

1.2c If the system creates information (for example, a score, analysis, or report), list the system as a source of information.

n/a

1.3 How is the information collected?

These questions are related to privacy controls DI-1, Data Quality, and IP-1, Consent.

1.3a 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 technologies used in the storage or transmission of information in identifiable form?

The information is collected from the Veteran or Dependent through account creation at https://login.gov/create-an-account

Each third-party identity proofing service will send information back to LG-e about its attempt to identity proof the user, including transaction ID, pass/fail indicator, date/time of transaction, and codes associated with the transaction data

1.3b 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.

n/a

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

These questions are related to privacy controls DI-1, Data Quality, and DI-2, Data Integrity and Integrity Board.

1.4a 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.

The purpose is identity proofing and authentication as part of a secure and compliant single sign-on application that allows external facing users to access VA products and services

1.4b 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.

The identity proofing process between the LG-e system and third-party identity proofing services takes place after the user provides the required account information

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

GSA developed LG-e pursuant to 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and 40 USC § 501.

https://www.federalregister.gov/documents/2017/01/19/2017-01174/privacy-act-of-1974-notice-of-anew-system-of-records (Original/New SORN)

https://www.federalregister.gov/documents/2017/08/10/2017-16852/privacy-act-of-1974-system-ofrecords (Modified SORN)

VA applicable SORNs:
150VA19 - https://www.govinfo.gov/content/pkg/FR-2008-11-26/pdf/E8-28183.pdf
138VA005Q - https://www.federalregister.gov/documents/2009/07/27/E9-17776/privacy-act-systems-of-records

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. (*Work with your System ISSO to complete this section)*

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: There is a risk when PII is held in a system

Mitigation: LG-e is taking all the requisite and security compliance measures needed for a FedRAMP moderate system. Which includes only authorized users can access data, data security rules are assigned that determine which data users can access and all data is encrypted at rest.

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.

All users must provide an email address to create a IAL1/AAL2 account and additional PII is necessary for agency applications that require users to create a IAL2/AAL2 account. During IAL1/AAL2 account creation, the user must provide an email address and create a password. To enable multi-factor authentication as a security measure, the user can choose to receive one-time security codes via phone call or text message. If users prefer not to provide a phone number for this purpose, they can instead receive the one-time security code using an authentication application. If provided, the user's phone number is provided to a multi-factor authentication service so that it can send one-time passwords via text or phone call to that user's phone. Each user must authorize the sharing of their email address with a partner agency to access that agency's services and information and to enable that agency to recognize that user on subsequent visits.
Additional PII is collected in order to verify a user's identity and set up the IAL2/AAL2 account. Full name, date of birth and social security number are needed to match the user's identity to a single individual. The collection of state ID details, address, and phone number confirms the user has access to artifacts associated with the identified individual. Information collected for IAL2/AAL2 account creation is shared with third-party proofers.

2.2 What types of tools are used to analyze data and what type of data may be produced?
These questions are related to privacy controls DI-1, Data Quality, DI-2, Data Integrity and Integrity Board, and SE-1, Inventory of Personally Identifiable Information.

2.2a 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.

The system assigns each user a master universal unique identifier (UUID) during the account creation process and then an additional agency UUID for each partner agency a user accesses via LG-e. The agency UUID is stored during each of the user's sessions so that each partner agency can use it to locate that user's profile within their systems. For example, if an individual accesses two different agencies' information or services through LG-e, that user is assigned two different agency UUIDs. However, each agency is only provided the user's agency UUID related to the user's visit to that agency's site. The system also keeps de-identified metadata related to the user's account and transactional data for analytic and debugging purposes. For example, metadata is used to identify user interaction types, including which types of browsers access LG-e, which multi-factor methods are used, and how many LG-e users access each agency partner site.

2.2b 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.

The system assigns each user a master universal unique identifier (UUID) during the account creation process and then an additional agency UUID for each partner agency a user accesses via LG-e. The agency UUID is stored during each of the user's sessions so that each partner agency can use it to locate that user's profile within their systems. For example, if an individual accesses two different agencies' information or services through LG-e, that user is assigned two different agency UUIDs. However, each agency is only provided the user's agency UUID related to the user's visit to that agency's site. The system also keeps de-identified metadata related to the user's account and transactional data for analytic and debugging purposes. For example, metadata is used to identify user interaction types, including which types of browsers access LG-e, which multi-factor methods are used, and how many LG-e users access each agency partner site.

2.3 How is the information in the system secured?
These questions are related to security and privacy controls SC-9, Transmission Confidentiality, and SC-28, Protection of Information at Rest.

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

SSN is encrypted at transit and rest. Each PII bundle is encrypted with the user password and LG-e hardware key management infrastructure.

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

Yes, see above

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

LG-e does not handle PHI. The PII is protected by – Hosing LG in the FedRAMP High/Moderate rated AWS GovCloud. LG Cloud Service Provider maintains a FedRAMP ATO and a VA -F package within eMASS that outlines all OMB Memorandum M-06-15 safeguards and security mechanisms.

2.4 PRIVACY IMPACT ASSESSMENT: Use of the information.

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.

2.4a How is access to the PII determined?

LG-e supports two types of user roles: the public user and privileged users.

2.4b Are criteria, procedures, controls, and responsibilities regarding access documented?

Yes. Public User: The public user role allows each user to make changes to their profile information (e.g. email address, phone number) after logging into the system. Each user must authorize the sharing of their email address with a partner agency in order to access that agency's services and information and to enable that agency to recognize that user on subsequent visits. Users trying to

access agency applications and services that require IAL2 attributes during AAL2 authentication will be prompted to authorize the sharing of additional data with the partner agency. Privileged Users: Privileged users are LG-e employees and contractors that have access to LG-e systems, which require additional safeguards and controls around their actions. All privileged users have their access reviewed on a quarterly basis. Current LG-e categories of privileged users are: system administrators, developers, security personnel, auditors, and multi-factor authentication service administrators. System administrators are privileged users who can access LG-e from the GSA network or via cloud services. System administrators use their elevated privileges in support of account management, and to check system logs to ensure proper operation of the system and to detect potentially malicious activity. All system administrator functions require multi-factor authentication. Developers are privileged users who have some access to LG-e from the GSA network, or via cloud services. Developers use their permissions to promote new versions of the LG-e software from one environment to another (e.g. from testing to production). All developer actions taken are logged and reported and all developer functions that interact with the production environments require multi-factor authentication. All code submissions require peer review and sign-off before they can be merged into the code-base for inclusion in future versions of the software. Security personnel are privileged users who have access to the logs generated from LG-e from the GSA network or via cloud services. Security personnel can create queries on logs from the production environment and generate alerts based on those queries. Security personnel only have access to the production LG-e environment in order to perform emergency shutdown procedures. All security personnel functions that interact with production systems require multi-factor authentication. Auditors are privileged users who have access to "read" but not alter the state and data of LG-e systems. Auditors can query machines in the production environment, and report data from those queries. All auditor actions in production systems require multi-factor authentication. All auditor actions are logged and reported upon. Multi-factor authentication service administrators are privileged users with access to the third-party tools used for sending each user a one-time security code. As discussed above, LG-e only shares the user's email address and agency UUID with partner agencies after the user consents to that sharing. If provided, the user's phone number is provided to a multi-factor authentication service provider to enable multi-factor authentication as a security measure. These user actions are logged to allow auditing against any unauthorized access to the system, since it could be possible to obtain a valid one-time security code for an account via administrative access to these systems. To facilitate identity proofing, LG-e will share the user's full name, date of birth, address, social security number, state ID number and type, and phone number with third-party providers only after the user consents to that sharing. LG-e manages security from three aspects of control: auditing of access, vetting of privileged users, and enforcing principles of least-privileged access. By keeping all audit logs for any action taken as a privileged user on LG-e systems, there is a detailed history maintained to determine who made changes and when. By using background check investigations for privileged users, LG-e seeks to grant access only to those who exhibit a high level of trustworthiness. By maintaining least-privileged access, LG-e restricts access to the minimum required levels, decreasing the risk of unauthorized disclosure or abuse. Additionally, all of these managerial controls are subject to regular review.

2.4c Does access require manager approval?

Depends on the role described above.

2.4d Is access to the PII being monitored, tracked, or recorded?

LG-e manages security from three aspects of control: auditing of access, vetting of privileged users, and enforcing principles of least-privileged access. By keeping all audit logs for any action taken as a privileged user on LG-e systems, there is a detailed history maintained to determine who made changes and when. By using background check investigations for privileged users, LG-e seeks to grant access only to those who exhibit a high level of trustworthiness. By maintaining least-privileged access, LG-e restricts access to the minimum required levels, decreasing the risk of unauthorized disclosure or abuse. Additionally, all of these managerial controls are subject to regular review

2.4e Who is responsible for assuring safeguards for the PII?

LG-e manages security from three aspects of control: auditing of access, vetting of privileged users, and enforcing principles of least-privileged access. By keeping all audit logs for any action taken as a privileged user on LG-e systems, there is a detailed history maintained to determine who made changes and when. By using background check investigations for privileged users, LG-e seeks to grant access only to those who exhibit a high level of trustworthiness. By maintaining least-privileged access, LG-e restricts access to the minimum required levels, decreasing the risk of unauthorized disclosure or abuse. Additionally, all of these managerial controls are subject to regular review

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*

Email Address, Master Universally Unique Identifier (UUID), Agency UUID, Phone number for multi-factor authentication (MFA), PIV/CAC subject, Full Name, Address, Date of Birth, Social Security Number, State-issued ID Number and Type, Contact Phone number and PIV/CAC subject.

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****. The VA records officer should be consulted early in the development process to ensure that appropriate retention and destruction schedules are*

implemented. If the system is using cloud technology, will it be following the NARA approved retention length and schedule? This question is related to privacy control DM-2, Data Retention and Disposal.

For LG-e: Retention: Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use as outlined in the LG-e SORN. The VA may store this information if it's for a new identity for a 6yr retention period from time of user account termination in accordance with NARA. System logs are retained for one year unless needed for audit or investigation

3.3 Has the retention schedule been approved by the VA records office and the National Archives and Records Administration (NARA)?

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. Please work with the system Privacy Officer and VA Records Officer to answer these questions.
This question is related to privacy control DM-2, Data Retention and Disposal.

3.3a Are all records stored within the system of record indicated on an approved disposition authority?

Yes. Retention: Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use as outlined in the LG-e SORN. The VA may store this information if it's for a new identity for a 6yr retention period from time of user account termination in accordance with NARA. System logs are retained for one year unless needed for audit or investigation

3.3b Please indicate each records retention schedule, series, and disposition authority.

System Access Records. Systems Requiring Special Accountability For Access.

Description: These are user identification records associated with systems which are highly sensitive and potentially vulnerable.

These records are created as part of the user identification and authorization process to gain access to systems. Records are used to monitor inappropriate systems access by users. Includes records such as:
• user profiles
• log-in files
• password files
• audit trail files and extracts
• system usage files
• cost-back files used to assess charges for system use

Exclusion 1. Excludes records relating to electronic signatures.

Exclusion 2. Does not include monitoring for agency mission activities such as law enforcement.

Retention: Temporary. Destroy 6 years after password is altered or user account is terminated, but longer retention is authorized if required for business use.

Legal Authority: DAA-GRS-2013-0006-0004 (GRS 03.2/031)

For the VA, any information retained has been approved by the retention schedule approved by the National Archives and Records Administration (NARA), NARA GRS 3.2, Information System Security Records to provide historical reports and to be available as needed for investigations or other legal reasons. GRS 3.2, item 031. Covers User Identification, Profiles, Authorizations, and Password Files and at time of publication requires a 6yr retention period from time of user account termination. System logs are retained for one year unless needed for audit or investigation.

https://www.archives.gov/files/records-mgmt/grs/grs03-2.pdf

3.4 What are the procedures for the elimination or transfer of SPI?

Explain how records are destroyed, eliminated or transferred to NARA at the end of their mandatory 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.

LG-e information is sent to VA SSOe, which then interacts with VA MPI. If there is a new identity, records are entered into the system and they remain as part of the protected system information. System logs are maintained for one year and then flagged for deletion by their automated processes. System logs are not retained after one year and any SPI containing them will be overwritten as part of the process for audit management. When virtual machines are no longer required to support the system they are wiped clean and the data overwritten. Paper documents are destroyed to an unreadable state in accordance with the Department of Veterans' Affairs VA Directive 6371, (April 8, 2014), http://www1.va.gov/vapubs/viewPublication.asp?Pub_ID=742&FType=2 In addition, any equipment that is decommissioned and is leaving the controlled data center will be sanitized (e.g., degaussing) or destroyed in accordance with VA Handbook 6500 and the Veterans Affairs Dedicated Cloud Media Sanitization Procedure. VA Dedicated Cloud Media Sanitization policy outlines the VA Dedicated Cloud policy and procedure for tracking, documentation and disposal of storage media within the environment and their return to the VA, in accordance with VA Handbook 6500. LG-e follows IT Security Procedural Guide: Media Protection (MP) CIO-IT Security-06-32.

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. This question is related to privacy control DM-3, Minimization of PII Used in Testing, Training and Research.

LG-e limits the collection of PII to what is needed to accomplish the stated purpose for its collection. LG-e keeps PII only as long as needed to fulfill that purpose. No LG-e data is used for research, testing, or training.

3.6 PRIVACY IMPACT ASSESSMENT: Retention of information

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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: Data collected and retained is not needed for the purpose of the system

Mitigation: LG-e does not ask for or store any information not needed for authentication and identity proofing. Privileged personnel also conduct audits of LG-e to assure this is the case and records are managed according to NARA guidance as outlined in section 3.3. Records are eliminated according to guidance as outlined in section 3.4.

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 3.9 (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***
SSOe IAM	Identity Proof	Universally Unique Identifier (UUID) Email First Name Last Name Physical Address Phone Date of Birth SSN Verification Time Stamp	Encrypted SAML response/token over TLS/SSL

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. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

This question is related to privacy control UL-1, Internal Use.

Follow the format below:

Privacy Risk: Unauthorized sharing of information within the VA

Mitigation: The system integration is managed by IAM, and IAM SSOe interacts with the VA Master Person Index (MPI). Access to all IAM infrastructure is allowed only by authorized personnel and controlled following VA processes. IAM has a full ATO that covers SSOe and VA MPI. The VA may store information if it's for a new identity for a 6yr retention period from time of user account termination. System logs are retained for one year unless needed for audit or investigation

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				

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: LG-e does not collect VA information and share it

Mitigation: LG-e does not collect VA information and share it

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 6.1 on the last page of the document. Also provide notice given to individuals by the source system (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?

These questions are 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.

6.1a 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, Notice of Privacy Practice provided to individuals for VHA systems. If notice was provided in the Federal Register, provide the citation.

Applicable VA SORNs

E8-28183.pdf (govinfo.gov)
150VA19
https://www.govinfo.gov/content/pkg/FR-2008-11-26/pdf/E8-28183.pdf
138VA005Q
https://www.govinfo.gov/content/pkg/FR-2009-07-27/pdf/E9-17776.pdf

Yes. LG-e presents the following Privacy Act Notice to the user when creating an account or signing in using LG-e:

Privacy Act Notice for IAL1/AAL2:

GSA is asking for your email address in order to create your account. You are not required to provide it; however, if you do not, you won't be able to create a LG-e account.

This collection of information is authorized by 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and 40 USC § 501. GSA uses your email address to create your account and may disclose this information pursuant to its published Privacy Act system of records notices (SORNs), GSA/TTS-1:

https://www.federalregister.gov/documents/2017/01/19/2017-01174/privacy-act-of-1974-notice-of-anew-system-of-records (Original/New SORN)

https://www.federalregister.gov/documents/2017/08/10/2017-16852/privacy-act-of-1974-system-ofrecords (Modified SORN)

Privacy Act Notice for IAL2/AAL2:

GSA is asking for your personal information in order to verify your identity. You are not required to provide any personal information. However, if you do not, you won't be able to access services that require a verified LG-e account.

This collection of information is authorized by 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and 40 USC § 501. GSA will use this information to attempt to verify you and may disclose this information pursuant to its published Privacy Act system of records notices (SORNs), GSA/TTS-1:

https://www.federalregister.gov/documents/2017/01/19/2017-01174/privacy-act-of-1974-notice-of-anew-system-of-records (Original/New system of records notice/SORN)

https://www.federalregister.gov/documents/2017/08/10/2017-16852/privacy-act-of-1974-system-ofrecords (Modified SORN)

Users may access the LG-e Privacy Practices on any web page of the site.

6.1b If notice was not provided, explain why. If it was provided, attach a copy of the current notice.

Please provide response here

6.1c 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.

n/a

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.

The information gathered is the minimum required for the outlined purposes. There are no other uses. The Privacy Act Notice provided to users informs them of their option to decline to provide information and the fact that they may not be able to access services require a verified account. Privacy Act Notice for IAL2/AAL2: GSA is asking for your personal information in order to verify your identity. You are not required to provide any personal information. However, if you do not, you won't be able to access services that require a verified LG-e account. This collection of information is authorized by 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and

40 USC § 501. GSA will use this information to attempt to verify you and may disclose this information pursuant to its published Privacy Act system of records notices (SORNs), GSA/TTS-1: https://www.federalregister.gov/documents/2017/01/19/2017-01174/privacy-act-of-1974-notice-of-anew-system-of-records (Original/New system of records notice/SORN)https://www.federalregister.gov/documents/2017/08/10/2017-16852/privacy-act-of-1974-system-ofrecords (Modified SORN) Users may access the LG-e Privacy Practices on any web page of the site.

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.

https://www.federalregister.gov/documents/2017/01/19/2017-01174/privacy-act-of-1974-notice-of-anew-system-of-records indicates
The information in *LG-e* is contributed voluntarily by the user and cannot be accessed, used, or disclosed by GSA without consent of the user, except as provided in this notice. A partner agency may add its own unique identifier to the user's *LG-e* account information for the purpose of identifying the user on subsequent attempts to access that agency's services.

The additional uses in the SORN:

In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act, all or a portion of the records or information contained in this system may be disclosed to authorized entities, as is determined to be relevant and necessary, outside GSA as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows:

a. To the Department of Justice or other Federal agency conducting litigation or in proceedings before any court, adjudicative or administrative body, when: (a) GSA or any component thereof, or (b) any employee of GSA in his/her official capacity, or (c) any employee of GSA in his/her individual capacity where DOJ or GSA has agreed to represent the employee, or (d) the United States or any agency thereof, is a party to the litigation or has an interest in such litigation, and GSA determines that the records are both relevant and necessary to the litigation.

b. To NIST-compliant third party identity proofing services, as necessary to identity proof an individual for access to a service at the required level of assurance.

c. To an appropriate Federal, State, tribal, local, international, or foreign law enforcement agency or other appropriate authority charged with investigating or prosecuting a violation or enforcing or implementing a law, rule, regulation, or order, where a record, either on its face or in conjunction with

other information, indicates a violation or potential violation of law, which includes criminal, civil, or regulatory violations and such disclosure is proper and consistent with the official duties of the person making the disclosure.

d. To a Member of Congress or his or her staff in response to a request made on behalf of and at the request of the individual who is the subject of the record.

e. To the Office of Management and Budget (OMB) and the Government Accountability Office (GAO) in accordance with their responsibilities for evaluation or oversight of Federal programs.

f. To an expert, consultant, or contractor of GSA in the performance of a Federal duty to which the information is relevant.

g. To the National Archives and Records Administration (NARA) for records management purposes.

h. To appropriate agencies, entities, and persons when (1) GSA suspects or has confirmed that there has been a breach of the system of records; (2) GSA has determined that as a result of the suspected or confirmed breach there is a risk of harm to individuals, GSA (including its information systems, programs and operations), the Federal Government, or national security; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed breach or to prevent, minimize, or remedy such harm.

i. To another Federal agency or Federal entity, when GSA determines that information from this system of records is reasonably necessary to assist the recipient agency or entity in (1) responding to a suspected or confirmed breach or (2) preventing, minimizing, or remedying the risk of harm to individuals, the recipient agency or entity (including its information systems, programs, and operations), the Federal Government, or national security, resulting from a suspected or confirmed breach.

6.4 PRIVACY IMPACT ASSESSMENT: Notice

Describe the potential risks associated with potentially insufficient notice and what steps, if any, are currently being taken to mitigate those identified risks. (Work with your System ISSO to complete all Privacy Risk questions inside the document this section).

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: An individual is unaware of why they are being asked for information or what it is used for even though they are informed during the process

Mitigation: Each user is provided a Privacy Act Notice with links to the LG-e Privacy Practices and Terms of Use before creating an account and submitting information. The LG-e Privacy Practices describes, among other things, what information is collected and stored automatically; how to share submitted information; security practices; and the purpose of the information collection. Users may access the LG-e Privacy Practices on any web page of the site

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?

These questions are related to privacy control IP-2, Individual Access, and AR-8, Accounting of Disclosures.

7.1a 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.***

Individuals with a LG-e account can sign into their account at any time to access their information when they present their email address, password, and multi-factor method. If an IAL2/AAL2 user loses their password, they can reset it through access to their email and presentation of their multi-factor method. If an IAL1/AAL2 user loses access to their multi-factor authentication method, the user can access their account using their personal key. If the user does not have access to their personal key, they can request to delete their account without signing in. When a user requests to delete their account, LG-e sends a notification to the email and the phone number associated with the account, if provided for MFA purposes. As a security measure, the user must wait 24 hours after submitting the request before deleting the account. After 24 hours, the user will receive a second email with a link to confirm the account deletion. Completing this process will allow the user to reset their LG-e account using the same email address. However, deleting the account removes any agency applications previously linked to the account. If an IAL2/AAL2 user loses access to their password, they can reset it through access to their email and presentation of their multi-factor method. If an IAL2/AAL2 user loses access to their multi-factor authentication method, the user can access their account using their personal key. If an IAL2/AAL2 user does not have access to their personal key, they will not be able to regain access to their LG-e account.

7.1b 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).

n/a

7.1c 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.

n/a

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.

The LG-e account page allows a user to update or amend any PII in the system used for account authentication (email address or optional multi-factor phone number). The user is also able to view their account history as well as delete their account. To amend the additional PII that is used for IAL2/AAL2 verification, the user must delete their account, and then create a new account and reproof. System administrators and other privileged users have no access to modify PII on a user's behalf. The user retains full control of their data and the means to update it.

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.

A user is made aware when they create an account and on the account page

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

This question is related to privacy control IP-3, Redress, and IP-4, Complaint Management.

Individuals with a LG-e account can sign into their account at any time to access their information when they present their email address, password, and multi-factor method.

If an IAL2/AAL2 user loses their password, they can reset it through access to their email and presentation of their multi-factor method. If an IAL1/AAL2 user loses access to their multi-factor authentication method, the user can access their account using their personal key. If the user does not have access to their personal key, they can request to delete their account without signing in. When a user requests to delete their account, LG-e sends a notification to the email and the phone number associated with the account, if provided for MFA purposes. As a security measure, the user must wait 24 hours after submitting the request before deleting the account. After 24 hours, the user will receive a second email with a link to confirm the account deletion. Completing this process will allow the user to reset their LG-e account using the same email address. However, deleting the account removes any agency applications previously linked to the account.

If an IAL2/AAL2 user loses access to their password, they can reset it through access to their email and presentation of their multi-factor method. If an IAL2/AAL2 user loses access to their multi-factor authentication method, the user can access their account using their personal key. If an IAL2/AAL2 user does not have access to their personal key, they will not be able to regain access to their LG-e account.

The LG-e account page allows a user to update or amend any PII in the system used for account authentication (email address or optional multi-factor phone number). The user is also able to view their account history as well as delete their account. To amend the additional PII that is used for IAL2/AAL2 verification, the user must delete their account, and then create a new account and reproof.

System administrators and other privileged users have no access to modify PII on a user's behalf. The user retains full control of their data and the means to update it.

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.*** *(Work with your System ISSO to complete all Privacy Risk questions inside the document this section).*

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 risk that an individual is unaware how to access or update their information.

Mitigation: An individual can access their account at any time and there is a help center through LG-e where a user can manage their account. https://LG-e/help/manage-your-account/overview/

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?
These questions are related to privacy control AR-7, Privacy-Enhanced System Design and Development.

8.1a Describe the process by which an individual receives access to the system.

There are defined user groups that allow for certain access based on assigned user group. The user groups have been documented and defined. See here for details. Public User: The public user role allows each user to make changes to their profile information (e.g. email address, phone number) after logging into the system. Each user must authorize the sharing of their email address with a partner agency in order to access that agency's services and information and to enable that agency to recognize that user on subsequent visits. Users trying to access agency applications and services that require IAL2 attributes during AAL2 authentication will be prompted to authorize the sharing of additional data with the partner agency. Privileged Users: Privileged users are LG-e employees and contractors that have access to LG-e systems, which require additional safeguards and controls around their actions. All privileged users have their access reviewed on a quarterly basis. Current LG-e categories of privileged users are: system administrators, developers, security personnel, auditors, and multi-factor authentication service administrators. System administrators are privileged users who can access LG-e from the GSA network or via cloud services. System administrators use their elevated privileges in support of account management, and to check system logs to ensure proper operation of the system and to detect potentially malicious activity. All system administrator functions require multi-factor authentication. Developers are privileged users who have some access to LG-e from the GSA network, or via cloud services. Developers use their permissions to promote new versions of the LG-e software from one environment to another (e.g. from testing to production). All developer actions taken are logged and reported and all developer functions that interact with the

production environments require multi-factor authentication. All code submissions require peer review and sign-off before they can be merged into the code-base for inclusion in future versions of the software. Security personnel are privileged users who have access to the logs generated from LG-e from the GSA network or via cloud services. Security personnel can create queries on logs from the production environment and generate alerts based on those queries. Security personnel only have access to the production LG-e environment in order to perform emergency shutdown procedures. All security personnel functions that interact with production systems require multi-factor authentication. Auditors are privileged users who have access to "read" but not alter the state and data of LG-e systems. Auditors can query machines in the production environment, and report data from those queries. All auditor actions in production systems require multi-factor authentication. All auditor actions are logged and reported upon.

8.1b 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?

n/a

8.1c 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.

There are defined user groups that allow for certain access based on assigned user group. The user groups have been documented and defined. See here for details. Public User: The public user role allows each user to make changes to their profile information (e.g. email address, phone number) after logging into the system. Each user must authorize the sharing of their email address with a partner agency in order to access that agency's services and information and to enable that agency to recognize that user on subsequent visits. Users trying to access agency applications and services that require IAL2 attributes during AAL2 authentication will be prompted to authorize the sharing of additional data with the partner agency. Privileged Users: Privileged users are LG-e employees and contractors that have access to LG-e systems, which require additional safeguards and controls around their actions. All privileged users have their access reviewed on a quarterly basis. Current LG-e categories of privileged users are: system administrators, developers, security personnel, auditors, and multi-factor authentication service administrators. System administrators are privileged users who can access LG-e from the GSA network or via cloud services. System administrators use their elevated privileges in support of account management, and to check system logs to ensure proper operation of the system and to detect potentially malicious activity. All system administrator functions require multi-factor authentication. Developers are privileged users who have some access to LG-e from the GSA network, or via cloud services. Developers use their permissions to promote new versions of the LG-e software from one environment to another (e.g. from testing to production). All developer actions taken are logged and reported and all developer functions that interact with the production environments require multi-factor authentication. All code submissions require peer review and sign-off before they can be merged into the code-base for inclusion in future versions of the software. Security personnel are privileged users who have access to the logs generated from LG-e from the GSA network or via cloud services. Security personnel can create queries on logs from the production environment and generate alerts based on those queries. Security personnel only have access to the production LG-e environment in order to perform emergency shutdown procedures. All security personnel functions that interact with production systems require multi-factor authentication. Auditors are privileged users who have access to "read" but not alter the state and data of LG-e

systems. Auditors can query machines in the production environment, and report data from those queries. All auditor actions in production systems require multi-factor authentication. All auditor actions are logged and reported upon.

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 contractors do not have access to the LG-e system.

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 Staff will not have access to the LG-e system. All GSA personnel are trained on how to identify and safeguard PII. In addition, each employee must complete annual privacy and security training. Many staff receive additional training focused on their specific job duties. Those who need to access, use, or share PII as part of their regular responsibilities, complete additional role-based training

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

8.4a If Yes, provide:

1. *The Security Plan Status:* Current
2. *The System Security Plan Status Date:* 9/9/2021
3. *The Authorization Status:* Authorized
4. *The Authorization Date:* 9/9/2021
5. *The Authorization Termination Date:* Initial ATO
6. *The Risk Review Completion Date:* 9/9/2021
7. *The FIPS 199 classification of the system (LOW/MODERATE/HIGH):* Moderate

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

8.4b If No or In Process, provide your ***Initial Operating Capability (IOC) date.***

n/a

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), Desktop as a Service (DaaS), Mobile Backend as a Service (MBaaS), Information Technology Management as a Service (ITMaaS). 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*. (Refer to question 3.3.1 of the PTA)*

LG-e is a FedRAMP authorized system hosted on Amazon Web Services (AWS), owned and operated by GSA. LG-e is FedRAMP Authorized at moderate impact level

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). (*Refer to question 3.3.2 of the PTA) This question is related to privacy control AR-3, Privacy Requirements for Contractors and Service Providers.*

Servicing Agency IAA#: LGVA210001Parties shall extend Privacy Act protections to all PII exchanged in accordance with this IAA as required by law, agency regulation and/or policy.

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.

LG-e keeps de-identified metadata related to the user's account and transactional data for analytic and debugging purposes. For example, metadata is used to identify user-interaction types, including which types of browsers access LG-e, which multi-factor methods are used, and how many LG-e users access each agency partner site.

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.

In the Interagency Agreement (IAA), VA/OIT and GSA/TTS agreed to comply with applicable law and regulations for ensuring the administrative, technical, and physical security of the information exchanged and the results of such programs, including the following:

Applicable Federal Information Security Laws and Regulations 1. VA/OIT and GSA/TTS will comply with the Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541 et seq., as amended by the Federal Information Security Modernization Act of 2014 (Pub. L. 113-283); Federal Information Processing Standards (FIPS), Mandatory Security Processing Standards 199 & 200; related Office of Management and Budget (OMB) circulars and memoranda, including OMB Circular No A-108 "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act"; OMB Memorandum 17-12 "Preparing for and Responding to a Breach of Personally Identifiable Information"; NIST directives; and the Federal Acquisition Regulations (FAR). These laws, regulations, and directives provide requirements for safeguarding Federal information systems and PII used in Federal agency business processes, as well as related reporting requirements. 2. FISMA requirements apply to all Federal contractors, organizations, or sources that possess or use Federal information, or that operate, use, or have access to Federal information systems on behalf of an agency. Each agency receiving information under this IAA is responsible for oversight and compliance of its contractors and agents with FISMA requirements.

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 they provided in this Privacy Impact Assessment is true and accurate.

Tonya L. Facemire 234776

Digitally signed by Tonya L. Facemire 234776
Date: 2023.06.05 15:24:19 -04'00'

Privacy Officer,Tonya Facemire

Carol K. Phan 1125928

Digitally signed by Carol K. Phan 1125928

Information System Security Officer, Carol Phan

SCOTTIE ROSS

Digitally signed by SCOTTIE ROSS
Date: 2023.06.05 13:46:00 -04'00'

Information System Owner, Scottie Ross

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).

Privacy Act Notice for IAL1/AAL2:

GSA is asking for your email address in order to create your account. You are not required to provide it; however, if you do not, you won't be able to create a LG-e account.

This collection of information is authorized by 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and 40 USC § 501. GSA uses your email address to create your account and may disclose this information pursuant to its published Privacy Act system of records notices (SORNs), GSA/TTS-1:

https://www.federalregister.gov/documents/2017/01/19/2017-01174/privacy-act-of-1974-notice-of-anew-system-of-records (Original/New SORN)

https://www.federalregister.gov/documents/2017/08/10/2017-16852/privacy-act-of-1974-system-ofrecords (Modified SORN)

Privacy Act Notice for IAL2/AAL2:

GSA is asking for your personal information in order to verify your identity. You are not required to provide any personal information. However, if you do not, you won't be able to access services that require a verified LG-e account.

This collection of information is authorized by 6 USC § 1523 (b)(1)(A)-(E), the E-Government Act of 2002 (44 USC § 3501), and 40 USC § 501. GSA will use this information to attempt to verify you and may disclose this information pursuant to its published Privacy Act system of records notices (SORNs), GSA/TTS-1:

https://www.federalregister.gov/documents/2017/01/19/2017-01174/privacy-act-of-1974-notice-of-anew-system-of-records (Original/New system of records notice/SORN)

https://www.federalregister.gov/documents/2017/08/10/2017-16852/privacy-act-of-1974-system-ofrecords (Modified SORN)

HELPFUL LINKS:

Record Control Schedules:

https://www.va.gov/vhapublications/rcs10/rcs10-1.pdf

General Records Schedule 1.1: Financial Management and Reporting Records (FSC):

https://www.archives.gov/files/records-mgmt/grs/grs01-1.pdf

National Archives (Federal Records Management):

https://www.archives.gov/records-mgmt/grs

VHA Publications:

https://www.va.gov/vhapublications/publications.cfm?Pub=2

VA Privacy Service Privacy Hub:

https://dvagov.sharepoint.com/sites/OITPrivacyHub

Notice of Privacy Practice (NOPP):

VHA Notice of Privacy Practices

VHA Handbook 1605.04: Notice of Privacy Practices