Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Login.gov (LG) Privacy Impact Assessment (PIA)

Last Updated: 09/21/2022

1 PRIVACY POINT OF CONTACT

Name	Les Hockman
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.3879
Email	hockman.lester@pbgc.gov

2 PRIVACY IMPACT ASSESSMENT

A Privacy Impact Assessment (PIA) is an analysis of how information is/will be handled:

i. To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
ii. To determine risks and effects of collecting, maintaining, and disseminating information in an identifiable form in an electronic information system, and
iii. To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy concerns are highest for systems that contain Personally Identifiable Information (PII). PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.

For example, consider a person named Mary Jones. There are over 200 million results in an internet search for this name. But if we combine information such as a date of birth, the last four digits of a (or worse, an entire) Social Security Number, or a spouse's name, the number of persons to whom we could be referring begins to narrow quite rapidly. These types of information are considered identifiers. Identifiers that uniquely identify a person are the focus of privacy protection.

2.1 The Components of the System

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII	In what system of records (SORN) is this information stored	What is the Legal Authority for collection of this information	Does this system share PII internally *(please detail in question 9)*
LG IDP	Supports LG production, public user, and system data Production and migration. LG IDP VPC contains one Management subnet and one Operations subnet.	Yes	GSA/TTS-1	E-Government Act of 2002 (Pub. L. 107–347, 44 U.S.C. 3501 note), 6 U.S.C. 1523 (b)(1)(A)–(E), and 40 U.S.C. 501.	Yes
SOC VPC	Supports LG production, public user, and system data Production and migration. SOC VPC contains Nessus operating on Ubuntu 14.04 and uses ELK Security Module.	Yes	GSA/TTS-1	5 U.S.C. 552a(b)(3)E-Government Act of 2002 (Pub. L. 107–347, 44 U.S.C. 3501 note), 6 U.S.C. 1523 (b)(1)(A)–(E), and 40 U.S.C. 501.	Yes
RedShift Analytics	Supports LG production, public user, and system data Production and migration. Redshift VPC contains a Redshift Analytics Lambda subnet and Redshift cluster subnets.	Yes	GSA/TTS-1	E-Government Act of 2002 (Pub. L. 107–347, 44 U.S.C. 3501 note), 6 U.S.C. 1523 (b)(1)(A)–(E), and 40 U.S.C. 501.	Yes

2.2 The System as a Whole

1. Please describe the purpose of the system, when considered as a whole, please include if this is an existing system (either an annual recertification update or a major change).

Login.gov *(LG) is a SaaS offering from GSA that allows public users to access Government services from the Internet using a federated single sign-on (SSO) method. LG performs user identification and authentication functions; consuming agencies such as PBGC are then responsible for authorizing access to its public-facing application or service. PBGC authorizes access to the user through the user's existing login.gov account details which includes email address, password, plus one of the two-factor authentication methods. Unlike many other cloud services, LG implements Privacy controls to protect PII entered or provided to the service by its public users.*

2. What are the Confidentiality, Availability, and Integrity ratings for the system as a whole?

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

3. List and discuss the sources from which the system collects PII (for instance, from an individual, another federal agency, etc.); the format in which PII is collected (for instance, via a form, face-to-face, phone, etc.); the notification given at time of collection from an individual regarding the Privacy Act and the ability to opt-out of collection (and the consequences of opting out). Include a copy of all forms and Privacy Act statements used to collect information.

PII is collected from public users and employees accessing PBGC website through Login.gov. Public users who log on to various systems through Login.gov provide PII via Login.gov website. The information collected by LG is considered PII and is stored within the LG system and protected through encryption. Login.gov provides a Privacy Act Statement on its website: Privacy & security: Our privacy act statement | Login.gov. *The statement also mentions that "If at any time users no longer agree to the Privacy Policy or any other relevant terms of the Login.gov, the user may close the account."*

4. Discuss any privacy controls that PBGC inherits from an external provider (cloud provider, third party provider, another government agency, etc.) If an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU), or similar document is in place, please summarize the privacy applicable portions of that document.

Login.gov provides privacy controls for the system

5. For the user roles in the system:

Role Name	Number of Users in that Role (AD)	Approver	Access Level (Read, Write, etc.)	Recertification Date
Regular Users	19	Federal Managers/CORs	Access is role-based and is based in ACLs needed to perform duties as assigned	June 1, 2022
Participants/Public Users	84,468	Service/Application Owner	Read/Write to own records	N/A

6. Does the System leverage the Enterprise Access Controls?

☒ Yes
☐ No

7. Discuss the Physical, Technical, and Administrative controls that are employed to secure the PII in the system.

- *Physical Controls* -. Physical security controls employed to secure the PII in the system include:*
  - *Physical Access Authorizations*
  - *Physical Access Control*
  - *Access Control for Transmission Medium*
  - *Access Control for Output Devices*
  - *Monitoring Physical Access*
  - *Visitor Access Records*
  - *Emergency Shutoff*
  - *Emergency Power*
  - *Emergency Lighting*
  - *Fire Protection*
  - *Alternate Worksite*
  - *Water Damage Protection*

  **Physical Controls are provided by the Cloud Service Provider (CSP)*

- *Technical Controls** - Technical controls employed to secure the PII in the system include:*
  - *Password protection*
  - *Firewalls*
  - *Encryption*
  - *Intrusion Detection and Prevention Systems (IDPS)*
  - *Public Key Infrastructure (PKI) Certificates*
  - *Identification and Authentication*
  - *Device Identification and Authentication*

- *Identifier Management*
- *Authenticator Management*
- *Remote Access*
- *Wireless Access*
- *Publicly Accessible Content*

***Technical Controls are provided by both PBGC and the Cloud Service Provider (CSP)*

- *Administrative Controls - Administrative controls employed to secure the PII in the system include:*
  - *Periodic Security Audits*
  - *Regular Monitoring of User's Activities*
  - *Annual Security, Privacy, and Records Management Refresher Training*
  - *Backups Secured Offsite*
  - *Encryption of Backups containing sensitive data*
  - *Role-Based Training*
  - *Least Privilege Access*
  - *Mandatory on-boarding training for security, privacy, and Records management personnel*

8. For the PII in the system, discuss the actual/intended uses of the PII; the steps taken to limit the PII collected to the minimum needed; and the reasons the PII is necessary and relevant.

PII is used to authenticate and grant access (by users) to PBGC public facing online services, as well as QuickTime for employees. Login.gov is hosted by GSA therefore and limits the PII it collects to that which it needs to verify the identity of the user.

9. Discuss the data flows within the system (include sources of data for data flowing into the system, destinations for data flowing out of the system, and any routine uses applicable to the system). For any information that is shared internally, be sure to discuss whether these data interconnections are noted in CSAM. Be sure to include any MOU, ISA, or Interagency Agreements.

LG performs user identification and authentication functions for PBGC which then authorizes access to the respective service. LG validates users' identity at two different Identity Assurance Levels (IAL):

- *IAL1 requires a valid email address and phone number*
- *IAL2 requires the user's full name, date of birth, home address, and Social Security number (SSN) in addition to the IAL1 requirements*

The information collected by LG is considered PII and is stored within the LG system and protected through encryption. IAL2 level identity verification is provided by third-party identity proofing services (e.g., LexisNexis, American Association of Motor Vehicle Administrators (AAMVA), Acuant Verify). Once identity proofing has been completed, LG supports customer access with a username/password plus any one of these MFA mechanisms: (a) a one-time password generated by a Time-based One-Time Password (TOTP) application such as

Google Authenticator, (b) an OTP delivered to the user via a voice call or text message, (c) a FIDO2 WebAuthn physical device such as Yubikey, or (d) a Personal Identity Verification (PIV) card. OTPs delivered via a voice call or text message can be "remembered" for a 12-hour window via a protected browser cache; if the "remember browser" checkbox is checked, login.gov authentication will only require a username and password through that web browser window. LG only provides authentication, PBGC is responsible for authorizing access.

PBGC and GSA have completed and signed an ISA as of 7/14/2022.

10. Does the system leverage the commonly offered control for Accounting of Disclosures?

☐ Yes
☒ No

2.3 Privacy Office Review

Name of Reviewer	Margaret Drake
Date Reviewed	10/6/22
Expiration Date	10/6/23
Result	☒ Approved without conditions ☐ Approved with conditions (see below). ☐ Denied

(For Privacy Office Use Only)

Discuss analysis of risks and compensating controls (or other mitigation steps).

Enter description here.

Discuss any conditions on Approval

Enter description here.