Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

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

Last Updated: 10/16/2024

1 PRIVACY POINT OF CONTACT

Name	Lisa Hozey
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.5607
Email	hozey.lisa@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)*
Login.gov (LG) Identity Provider (IDP)	Supports LG production, public user, and system data Production and migration. LG IDP Virtual Private Cloud (VPC) contains one Management network and one Operations network.	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
Security Operations Center (SOC) Virtual Private Cloud (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 network and Redshift cluster networks.	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 Software as a Service (SaaS) offering from General Services Administration (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.*

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 accessing PBGC systems through Login.gov. PII of PBGC employees is collected to facilitate access to various systems within PBGC. Public users who log on to various systems through Login.gov provide PII via the 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. 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 some privacy controls for the system with PBGC providing the other applicable privacy controls. Privacy Controls provided by Login.gov include:

- *DM-01 Minimization Of Personally Identifiable Information*
- *TR-01 Privacy Notice*
- *TR-02 System Of Records Notices And Privacy Act Statements*
- *UL-02 Information Sharing With Third Parties*

All remaining privacy controls are provided by PBGC.

Attachment B "Description of Description of login.gov Services v.2" within an ISA between PBGC and Technology Transformation Services (TTS) within the General Services Administration (GSA)'s Federal Acquisition Service (FAS) details relevant privacy content that is summarized below:

System of Records Used. *The GSA System of Records Notice (SORN) used for purposes of this information exchange is entitled "login.gov" (GSA/TTS–1).*

Privacy Act Statement. *GSA will provide users with statements that comply with subsection (e)(3) of the Privacy Act, 5 U.S.C. 552a(e)(3).*

Privacy Impact Assessment. *GSA has conducted and posted a Privacy Impact Assessment under Section 208 of the E-Government Act of 2002.*

Data Management. *If [PBGC] and GSA agree to extend the use of the data beyond the period of performance identified in the 7600B, [PBGC] and GSA must ensure appropriate SORN(s) are in place.*

Privacy Safeguards, Restrictions on Disclosure, and Records Retention*. Parties shall extend Privacy Act protections to all PII exchanged to the maximum extent practicable. Both Parties acknowledge that the use and disclosure of the data and other information provided by the Parties may also be subject to limitations under law, regulation, and policy. [PBGC] and GSA/TTS will retain and dispose of any electronic or paper records containing information exchanged in accordance with the applicable NARA approved Federal Records Retention Schedules (44 U.S.C. § 3303a).*

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
Privileged Users	21	Federal Managers/CORs	Access is role-based and is based on ACLs needed to perform duties as assigned	May 30, 2024
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 and Environmental Protection (PE) 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*

****Administrative Controls are provided by PBGC. Administrative controls provided by PBGC only apply to PBGC users, not external users.*

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 MyPBA, MyPAA, eCase/DAP.Employee Express and QuickTime are used for employees. The collection of PII is needed to verify the user. Login.gov is hosted by GSA and limits the PII collected by only collecting information needed to verify users, which has been predetermined by PBGC.

9. Discuss the data flows within the system (including 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.

Login.gov (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).

The information collected by LG is stored within the LG system and protected through encryption. The Verified Accounts 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.

LG only provides authentication, and PBGC is responsible for authorizing access. Following authentication, LG forwards the required PII data elements to PBGC's cloud-based applications such as MyPBA, MyPAA, Employee Express, eCase/DAP, and QuickTime. Applications evaluate the data provided and thereby authorize the external user's access to the appropriate roles within the system, based upon application-specific criteria, rulesets, and logic.

PBGC and GSA have completed and signed an ISA as of 7/14/2022. Attachment B "Description of Description of login.gov Services v.2" within an ISA between PBGC and Technology Transformation Services (TTS) within the General Services Administration (GSA)'s Federal Acquisition Service (FAS).

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

☐ Yes

☒ No

11. If your system collects, Social Security Numbers:

a. Please provide a justification for the collection, use, maintenance, and disposal of PII in the form of SSN?

PBGC does not collect SSNs from LG. LG collects, uses and maintains user's SSN. Please refer to the Login.gov PIA from GSA for use of SSNs. (https://www.gsa.gov/system/files/Login.gov_PIA_%28May_2024%29.docx.pdf)

b. Under which authorized uses, as described in the "Reduction of Use of Social Security Numbers (SSN) in PBGC" policy document?

Not applicable

c. If the answer to b., above is "Compelling Business Need," please provide a plan to reduce the use of SSNs, highlighting activities that can be completed in the next 12 months.

Not Applicable

2.3 Privacy Office Review

Name of Reviewer	Ashley Church
Date Reviewed	10/22/2024
Expiration Date	10/22/2025
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.