Pension Benefit
Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

MyPBA/QuEST Privacy Impact Assessment (PIA)

Last Updated: 05/24/2024

1 PRIVACY POINT OF CONTACT

Name	Lester Hockman
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.286.3879
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)*
Quick.Easy.Secure.Transparent (QuEST)	QuEST is a service that supports the mission of the OBA to ensure participants are paid their full benefit permitted by law and to provide quality service through accurate, timely, and uninterrupted benefit payments & administration. This service, a cloud-based modernization of the Customer Relationship Management (CRM) system which was formerly part of the OBA Applications Suite (BAS), provides a central repository for all PBGC participant interactions and enables customer service representatives to pull data from enterprise databases to answer questions for service plan participants, beneficiaries, and managers.	Yes	PBGC-6, Plan Participant and Beneficiary Data,PBGC-9, Unclaimed Retirement Fund, PBGC-10, Administrative Appeals File	29 U.S.C. 1055, 1056(d)(3), 1203, 1302, 1321, 1322, 1322a, 1341, 1342, and 1350; 26 U.S.C. 6103; 44 U.S.C. 3101; 5 U.S.C. 301; 29 U.S.C. ch. 18; 29 CFR 4003.1; 29 CFR 4003	Yes
My Pension Benefit Account (MyPBA)	MyPBA consists of a web-based self-service application available for use by participants in plans that have been trusteed by PBGC. Authenticated users may conduct business transactions such as form submissions and data	Yes	PBGC-6, Plan Participant and Beneficiary Data	29 U.S.C. § 1055, 1302, & 1322; 44 U.S.C. § 3101; 5 U.S.C. § 301.	Yes

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)*
	updates electronically with PBGC through the use of functions implemented within the Dynamics 365 SaaS and by selected platform services within the Azure Government subsystem. Users are authenticated by the Login.gov subsystem as augmented by the Business to Consumer (B2C) component of the Azure Commercial cloud offering.				

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).

MyPBA enables participants in plans that have been trusteed by PBGC to electronically submit their forms and update records as needed. QuEST ensures that participants are paid their full benefit permitted by law and provides quality service through accurate, timely, and uninterrupted benefit payments and administration. MyPBA and QuEST were previously authorized for operation as component services of the ITISGSS system but have now been extracted into a dedicated FISMA child to provide better visibility by the Privacy Office and more direct control by the OBA-based Service Owner.

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 plan sponsors and administrators of trusteed plans, individuals, and federal agencies. The format for collecting PII includes submitted forms via email, phone and/or via a website or agency database. Any data collection forms via email and website include the PBGC Privacy & Paperwork Act Notices.* SHORT PRIVACY ACT NOTICE (pbgc.gov). *Individuals can opt out of this collection of PII as participant response on a PBGC form is voluntary. However, failure to provide information to PBGC may delay or prevent PBGC from calculating and paying the participant's pension benefits. After PBGC becomes the statutory trustee of a pension plan, a participant may contact the PBGC Customer Contact Center, or access MyPBA to update or modify the information that is used by PBGC.* Forms for Workers and Retirees | Pension Benefit Guaranty Corporation (pbgc.gov)

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.

PBGC does not inherit privacy controls from the following external providers: Address Validation System (AVC), FedACH, Spectrum, and State Street Bank (SSBT). An interconnection is maintained between PBGC and State Street Bank and Trust Company (SSBT) for the purpose of exchanging data between MyPBA (owned by PBGC) and the MyPenPay web services (owned by Voya and SSBT). This interconnection is utilized to retrieve payment history information (including check images, if applicable), and any tax forms that may be available for the MyPBA user on PBGC's behalf. PBGC and SSB have an ISA that has been uploaded into the CSAM. The data exchanged between PBGC and Voya, considered Controlled Unclassified Information (CUI), contains Personally Identifiable Information (PII) that is covered by the Privacy Act.

5. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Regular User	647	Service Owner(s)	Access is role-based and is based in ACLs needed to perform non-privileged duties as assigned.	5/14/2024
Non-Organizational Users	145,496	Service Owner(s)	Non-Organizational Users only have read permission into MyPBA.	N/A*
AP User	7	Service Owner(s)	Access is role-based and is based in ACLs needed to perform privileged duties as assigned. This includes network, system, and database administrators.	5/14/2024

* Non-Organizational Users are not recertified.

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 Controls for Azure datacenters are provided by Microsoft and these controls are externally inherited from the CSP. Azure G by Microsoft provides Physical Controls which includes:*
  - *Physical Access Authorization*
  - *Physical Access Control*
  - *Access Control for Transmission Medium*
  - *Access Control for Output Devices*
  - *Monitoring Physical Access*
  - *Visitor Access Records*

- *Alternate Work site*
- *Location of Information System Components*
- *Emergency Lighting*
- *Emergency Power*
- *Fire Protection*

- *Technical controls employed to secure the PII in the system include:*
  - *Password Protection*
  - *Virtual Private Network (VPN)*
  - *Firewalls*
  - *Unique User Identification Names*
  - *Encryption*
  - *Intrusion Detection System (IDS)*
  - *Personal Identity Verification (PIV) card access*
  - *Public Key Infrastructure (PKI) Certificates*
  - *Remote Access*
  - *Wireless Access*
  - *Access Control for Mobile Devices*
  - *Network Accessible Storage Device*
  - *Single sign-on (Login.gov)*
  - *Privacy Controls (Login.gov)*
  - *Azure C provides Wireless Access Restrictions, Information Sharing and Publicly Accessible Content.*
  - *Azure G provides extra layer of protection for storage of customer data which includes: Device Identification and Authentication and Authentication Feedback.*

- *Administrative Controls - All PBGC users are required to complete privacy training annually. 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*

The controls provided by the Cloud Service Provider (CSP) are implemented in the Cloud and at the CSP's facilities.

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 manage pension plan data; value pension plans and associated liabilities for which PBGC is, or may be, obligated to pay; calculate and provide pension benefits; and

report tax information to the Internal Revenue Service (IRS) and other tax authorities. PII is also used to correctly identify pension plan participants enabling them to review pertinent information through the MyPBA web portal.

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.

The QuEST and MyPBA services share PII with the Address Validation System (AVS), FedACH, Spectrum, State Street Bank using the PLUS system, and the Image Processing System (IPS). PBGC and SSB have an ISA.

AVS validates Participant and Third-Party Contact addresses and reformats the addresses into USPS standards. FedACH is an existing web service used to validate bank routing numbers. Spectrum is a PBGC on-premises application that processes payments to retirees and their beneficiaries and also manages participant demographic data such as addresses, names, SSNs, etc. IPS is responsible for storing documents received by PBGC. PII information from these interfacing systems will be stored in QuEST.

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?

SSN is used to correctly identify pension plan practitioners when other identifiers (e.g., Customer ID) are not available, manage pension plan data, calculate and provide pension plan benefits; and report tax information to the Internal Revenue Service (IRS) and other tax authorities.

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

***Interactions with financial institutions**. Federal law requires that individuals who hold accounts with financial institutions must provide an SSN as part of the process to open accounts. Thus, PBGC may be required to provide the SSN for systems, processes, or forms that interface with financial institutions.* ***Federal taxpayer identification**. The application of Federal and state income tax programs rely on the use of the SSN. Thus, systems that have any function that pertains to the collection, payment, or record keeping of this use must contain the SSN. In addition, individuals who operate a business under their own name may use their SSN as the tax number for that business function.* ***Government Data Matching**. Systems, processes, or forms that interact with other government agencies or non-Federal databases may require the continued use of the SSN as a primary identifier as a primary means for transferring, matching, or checking information. These applications should be rigorously scrutinized to determine the availability of some other means of conducting these transactions.*

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	Margaret Drake
Date Reviewed	5/21/24
Expiration Date	5/22/25
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.