Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

My Plan Administration Account (My PAA) Privacy Impact Assessment (PIA)

Last Updated: 02/18/2026

1 PRIVACY POINT OF CONTACT

Name	Catherine Diamante
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202-403-4260
Email	Diamante.catherine@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.

TIP!

Information that either alone or when considered with other information that uniquely identifies a person is Personally Identifiable Information (PII). Combining pieces of information whether private or publicly available has powerful implications for uniquely identifying an individual.

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 13)*
My PAA	The My PAA Customer Portal allows pension plan practitioners to submit their premium filings, while the Agent Web allows PBGC Agents to provide Customer Support, Account Management, and Plan Management.	Yes	PBGC-14, My Plan Administration Account	29 U.S.C. §§ 1302, 1306, 1307, 1343, and 44 U.S.C. §§ 3101	Yes, with the Premium Practitioner System (PPS)

2.2 The System as a Whole

1. Please describe the purpose of the system when considered as a whole.

My Plan Administration Account (My PAA) allows pension plan practitioners to submit their premium filings electronically to the Pension Benefit Guaranty Corporation. The My Plan Administration Account runs on Oracle Service Cloud as a Software as a Service product.

The My Plan Administration Account is a system running on Oracle Service Cloud services. The My Plan Administration component that is available to practitioners is the Customer Portal, while the Agent Web is used by internal PBGC individuals to provide Customer Support, Account Management, and Plan Management. The Oracle Intelligent Advisor (OIA) is used by PBGC internal users to model and deploy business rules, and the OIA users do not have access to the My PAA data.

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

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

3. Is this a contractor system?

☐Yes
☒No

4. Is this a new or existing information system? If this is an existing information system, please describe the changes.

My PAA is an existing system. Although since last reviewed, My PAA has undergone a series of maintenance updates aimed at improving the usability of the My PAA and to ensure security and compliance, none of these maintenance updates had an impact on the way My PAA collects, processes and maintains PII.

All changes have been documented where applicable in the My PAA baseline configuration. Security Testing and Evaluation (ST&E) report and Security Impact Assessments (SIA) are conducted as part of the development and maintenance process of My PAA as needed.

5. Does your system collect, process, or maintain any records that describe how any individual exercises their First Amendment rights?

   If so, please describe the information it collects and the purpose for the collection. Please describe whether: 1) an express legal authority authorizes the collection, 2) the collection is

pertinent to and within scope of an authorized law enforcement activity, or 3) the individual(s) consents to the collection.

(The First Amendment guarantees an individual's right to the exercise of their religious beliefs, their petitioning the government, their exercise of free speech, their right to peaceably assemble, and the freedom of the press.)

No

6. For the PII in the system, discuss the actual/intended uses of the PII; procedures taken to limit the PII collected to the minimum needed; reasons the PII is necessary and relevant; and procedures taken to periodically review the accuracy, relevance, timeliness, and completeness of PII throughout the information life cycle.

The My PAA account information is collected and used to:

- *Authenticate user access.*
- *Grant specific permissions or abilities within the online application.*
- *Monitor access controls; and*
- *Display certain multi-and single employer plan information on PBGC.GOV to help the public determine if a plan is covered by PBGC.*

Where applicable, signatures and payment authorizations are acquired electronically from appropriate e-filing team members.

Per the System of Records (SORN),

Information about covered individuals may be disclosed without consent as permitted by the Privacy Act of 1974, 5 U.S.C. 522a(b), and:
Names, addresses and phone numbers of plan sponsors, plan administrators, pension practitioners, actuaries and pension benefit professionals who submit plan information to My PAA may be disclosed to the public in order to ensure the public has access to contact information for those individuals submitting information regarding pension plans and those responsible for the administration of pension plans covered by the Employee Retirement Income Security Act of 1974 (ERISA).

7. Discuss how your system retrieves PII. Please describe the identifiers used to locate records within a system, such as name, identification number, date of birth, etc.

My PAA retrieves information using unique identifiers

8. Approximately how many individuals' PII is maintained in the system?

Approximately 48,124 individuals' PII is maintained.

9. Is the submission of PII by individuals voluntary or mandatory? If the submission is voluntary, what is the outcome of an individual not submitting PII.

The submission of PII by individuals (My PAA users) is mandatory for the intended uses stated in section 6 of this PIA above.

10. 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?

N/A

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

N/A

    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.

N/A.

11. 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.

PBGC users who access the MyPAA functionality, which is available exclusively through the PBGC intranet, have their PII collected electronically by PBGC. Prior to gaining access to the PBGC intranet, users are presented with the applicable Privacy Act Statement and Security Notices. *Plan Administrators submit filings electronically through MyPAA that contains PII. A link to the Privacy Act Statement is also provided on the MyPAA homepage. Users must acknowledge the Privacy Act Statement prior to submitting information.*

PRIVACY ACT NOTICE

You are accessing a computer system operated by the Pension Benefit Guaranty Corporation, a wholly owned corporation of the United States Government. It is for authorized use only, in compliance with the PBGC Policy on the Use of Information Technology Resources and federal statutes, and when use is authorized, such use may not exceed the scope of authorization.

AUTHORITIES: PBGC is authorized to collect your personal information pursuant to 29 U.S.C. §§ 1302, 1306, 1307, 1343; 44 U.S.C. §§ 3101; and System of Records Notice PBGC-14, My Plan Administration Account Records – Last published at 83 FR 6265 (February 13, 2018). Failure to provide the requested information may result in the denial of services using My PAA

PURPOSE: This system of records is maintained for use in verifying the identity of individuals who register to use the My Plan Administration Account (My PAA) application to create PBGC filings, receiving, authenticating, processing, and keeping a history of filings and premium payments submitted to PBGC by registered users. Information from this system is used to provide the public with contact information for plan sponsors, plan administrators, pension practitioners, actuaries, and pension benefit professionals who submit plan information through My PAA.

ROUTINE USES: We will use the information you provide such as your name, email address, bank account, and other contact information to process the transactions you request through My PAA. This information may also be shared internally within PBGC or with other Federal agencies to administer your account or for statistical, auditing, or archiving purposes. We may also share the information with law enforcement agencies investigating, prosecuting, or enforcing a violation of civil or criminal law or with other agencies for the purpose of implementing a statute, rule, or order. You are not required by law to provide this information, but if you do not provide it, it may not be possible to process the actions you request on this Web site. Additionally, we will share business contact information with the public.

WARNING!!! WARNING!!! WARNING!!!

Use of this system is subject to audit, and all files and transmissions on this system may be intercepted, monitored, recorded, copied, or inspected to ensure that use is authorized, for management of the system, to facilitate protection against unauthorized access, to verify security procedures, and for such other purposes as may be deemed necessary, consistent with federal law.

Unauthorized or improper use of this system may result in administrative action, civil, and/or criminal penalties. Any information collected during an audit or monitoring may be used in administrative, civil, or criminal actions and may be disclosed to authorized officials of other agencies, both domestic and foreign. Examples of unauthorized or improper use include, but are not limited to: uploading or changing the information presented on this system with intent to damage this system; attempting to gain unauthorized access to data; attempting to redirect authorized users away from this system; or attempting to deny service to authorized users By using this system, the user consents to the auditing, interception, monitoring, recording, copying, inspection, and disclosure as described above. Clicking below or otherwise continuing to use this system indicates your awareness of and consent to these terms and

conditions of use. Leave this site, cease use or log off immediately if you do not agree to the conditions stated in this warning.

12. 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 Oracle Service Cloud. My PAA is hosted on Oracle Service Cloud and the details are documented in the System Security Plan and Contract.

13. Is the PII shared with external (non-PBGC) organizations? If so, identify with whom the PII is shared and the purpose. 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.

My Plan Administration Account allows pension plan practitioners to submit their premium filings electronically to the Pension Benefit Guaranty Corporation. My Plan Administration Account data is shared with Oracle Service Cloud as they are the cloud provider and Login.gov as users are required to authenticate through Login.gov prior to access. Information shared internally with Consolidated Financial System, Office of Benefits Administration Applications Suite, and My Pension Benefit Access are documented in the data connections in JCAM.

PBGC needs the information collected in the practitioner's premium filing to:

- Identify the plan and plan year for which the filing is made;

- Identify the type of premium being reported (estimated or final);

- Determine the amount of the premium due to the PBGC under the Title IV of the Employee Retirement Income Security Act of 1974 (ERISA) and the PBGC's premium filing regulations (29 CFR Parts 4006 and 4007); and

- Collect the originating IP address for forensic analysis

14. For the user roles in the system:

Oracle Intelligent Advisor Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Permissions Administrator	4	User's supervisor	Read, Write	Users were recertified during the annual

		& ISO		recertification period between 5/5/25 and 6/20/25
Author (Default Collection)	6	User's supervisor & ISO	Read, Write	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25
Manager (Default Collection)	6	User's supervisor & ISO	Read, Write	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25
Connections Administrator	4	User's supervisor & ISO	Read, Write	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25
Viewer (Default Collection)	2	User's supervisor & ISO	Read, Write	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25

Agent Web Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
MyPAA API	2	User's supervisor & ISO	Read, Write	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25
My PAA Admin Knowledge Manager	4	User's supervisor & ISO	Read, Write	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25
My PAA Agent CSR	29	User's supervisor & ISO	Read, Write	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25

Agent Web Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
My PAA Agent Read Only	5	User's supervisor & ISO	Read	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25
My PAA Full Access	2	User's supervisor & ISO	Read, Write	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25
My PAA Knowledge Owner Agent	6	User's supervisor & ISO	Read, Write	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25
My PAA Security Report Users	1	User's supervisor & ISO	Write	Users were recertified during the annual recertification period between 5/5/25 and 6/20/25
Filing Preparer	127,670	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 450 days of inactivity.
Filing Coordinator	105,222	Automated Approval as this is the default role.	Read, Write	External users are not recertified, but accounts are disabled after 450 days of inactivity.
Payment Preparer	127,670	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 450 days of inactivity.
Actuary	43,127	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 450 days of inactivity.
Plan Admin	23,242	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 450 days of inactivity.

Agent Web Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Plan Admin Rep	38,222	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 450 days of inactivity.
Upload Preparer	127,670	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 450 days of inactivity.

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

My PAA has the following Physical, Technical and Administrative controls in place

(1) Physical controls - Identification badges, close circuit television, road barriers, security guards, visitor sign-in sheet, key cards, and safeguards for environment hazards.

(2) Technical Controls - Password protection, two-factor authentication, virtual private network, firewalls, unique user Identification, single sign-on, encryption, and intrusion detection.

(3) Administrative controls - Security audits, monitoring of administrator and user activity, refresher security, privacy, and role-based training, backup secured off-site, least privilege to restrict access to PII, and Personal Identity Verification

16. Please discuss additional training for users, other than the PBGC mandatory annual training, for protecting information in the system.

Besides PBGC mandatory training (Information Security & Privacy Awareness, Privacy Literacy, Insider Threat, and Rules of Behavior), internal My PAA users are offered additional on the job training and other privacy refreshers by the Learning and Development Division via FedTalent Learning Management. Plan practitioners with access to Customer Portal are provided training on plan filing and account management.

17. Does the System leverage the Enterprise Access Controls?

☒ Yes
☐ No

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

☒ Yes
☐ No

19. Discuss the process in place for retention and destruction of PII. Cite the applicable retention schedule(s).

PBGC retains and destroys PII in accordance with National Archive and Records Administration (NARA) records and PBGC Simplified Records Schedules- Schedule. Refer to FOD File Plan Dashboard. Oracle Service Cloud maintain and dispose of electronic records according to the NARA schedule.

2.3 Privacy Office Review

Name of Reviewer	Loretta Dennison
Date Reviewed	February 18, 2026
Expiration Date	February 18, 2027
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