Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)

My Plan Administration Account (My PAA)

05/08/2023

1 Privacy Point of Contact

Name	Carol Richardson
Title	Information System Security and Privacy Officer
Phone	202-229-3289
Email	Richardson.Carol@pbgc.gov

TIP!

This point of contact should be the person you want the Privacy Office to work with in completing this PIA. For some systems it might be the Information Owner (IO) or Information System Owner (ISO). Many business units identify this as the Information System Security and Privacy Officer (ISSPO). DO what makes

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
MyPAA	The MyPAA Customer Portal allows pension plan practitioners to submit their premium filings, while the Agent Web allows for PBGC Agents to provide Customer Support, Account Management, and Plan Management.	Yes	PBGC-14, My Plan Administration Account Records – PBGC. 75 Fed. Reg. 37,842, 37,853.	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, please include if this is an existing system (either an annual recertification update or a major change)

My Plan Administration Account 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. 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.

Individuals (Plan Administrators) submit filings electronically that contain the PII noted previously. Users are given a link to the Privacy Act Notices on the Homepage. Customers acknowledge the following statement:

Security and Privacy Notices

Published 02/17/2023 12:59 PM | Updated 03/01/2023 09:29 AM

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 7247 (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.

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 will not inherit privacy controls from Oracle Service Cloud. MyPAA will be hosted on Oracle Service Cloud and the details of the connection is documented in the System Security Plan, Contract, and Configuration document. There is also a MOU/ISA between Treasury and the credit card processing banks for Pay.gov with the Consolidated Financial System.

5. 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[1]**
Hub Administrator	2	User's supervisor & ISO	Read, Write	Users will be recertified between May 2nd and June 1st 2023.
Author (Default Collection)	2	User's supervisor & ISO	Read, Write	Users will be recertified between May 2nd and June 1st 2023.
Manager	2	User's supervisor & ISO	Read, Write	Users will be recertified between May 2nd and June 1st 2023.
Determinations API (Default Collection)	0	User's supervisor & ISO	Read, Write	Users will be recertified between May 2nd and June 1st 2023.

1. All users are recertified by the Business Owner using the ITIOD's SailPoint tool.

Agent Web Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date[1]
MyPAA API	2	User's supervisor & ISO	Read, Write	Users will be recertified between May 2nd and May 16th 2022.
My PAA Admin Knowledge Manager	4	User's supervisor & ISO	Read, Write	Users will be recertified between May 2nd and May 16th 2023.
My PAA Agent CSR	22	User's supervisor & ISO	Read, Write	Users will be recertified between May 2nd and May 16th 2023.
My PAA Agent Read Only	13	User's supervisor & ISO	Read	Users will be recertified between May 2nd and May 16th 2023.
My PAA Full Access	3	User's supervisor & ISO	Read, Write	Users will be recertified between May 2nd and May 16th 2023.
My PAA Knowledge Owner Agent	7	User's supervisor & ISO	Read, Write	Users will be recertified between May 2nd and May 16th 2023.
My PAA Security Report Users	1	User's supervisor & ISO	Write	Users will be recertified between May 2nd and May 16th 2023.
Filing Preparer	87319	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 2 years of inactivity
Filing Coordinator	78430	Automated Approval as this is the default role.	Read, Write	External users are not recertified, but accounts are disabled after 2 years of inactivity
Payment Preparer	45381	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 2 years of inactivity
Actuary	31951	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 2 years of inactivity
Plan Admin	23701	Filing Coordinator	Read, Write	External users are not recertified, but accounts

				are disabled after 2 years of inactivity
Plan Admin Rep	19680	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 2 years of inactivity
Upload Preparer	37721	Filing Coordinator	Read, Write	External users are not recertified, but accounts are disabled after 2 years of inactivity

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.

MyPAA 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, backups secured off-site, least privilege to restrict access to PII, and Personal Identity Verification.

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.

MyPAA stores Names, Addresses and Telephone numbers. Email addresses, bank account numbers, and universally unique identifier (UUID) are the only sensitive information.

The My PAA account information is collected and used to:

- Authentic 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),

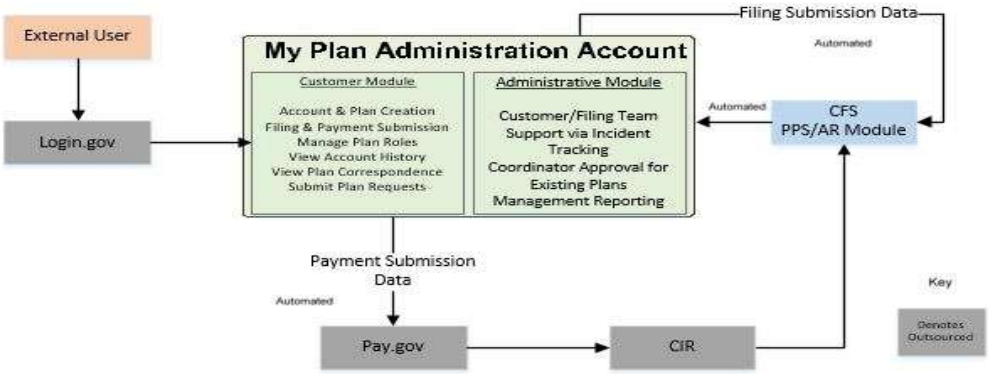
Information about covered individuals may be disclosed without consent as permitted by the Privacy Act of 1974, 5 U.S.C. 522a(b), and:

1. General Routine Uses G1, G4 through G7, G9, G10, and G12 through G14 apply to this system of records (see Prefatory Statement of General Routine Uses).

2. 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).

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.

My Plan Administration Account allows pension plan practitioners to submit their premium filings electronically to the Pension Benefit Guaranty Corporation. My Plan Administration Account is available 24 hours a day, seven days a week. The following diagram depicts the data flow with upcoming Login.gov solution.



My PAA 2.0_High Level Design Flow_0

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.

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

☒ Yes
☐ No

2.3 Privacy Office Review

Name of Reviewer	Bill Black
Date Reviewed	
Expiration Date	12 months from date of signature from the Chief Privacy Officer
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.