

**Pension Benefit Guaranty Corporation (PBGC)  
Privacy Impact Assessment (PIA)**



**My Plan Administration Account (My PAA)**

**04/29/2020**

# 1 Privacy Point of Contact

<b>Name</b>	Edward Picard
<b>Title</b>	Information System Security Privacy Officer
<b>Phone</b>	202-326-4100 ext. 3574
<b>Email</b>	Picard.Edward@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 Officer (ISSO). DO what makes sense for you!

# 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

*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.

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
My PAA Administrative Module	Administrative Module users are added to the appropriate Active Directory groups, which control specific functionality within the Administrative Module.	No	N/A	N/A	N/A
My PAA Customer Module	The Customer Module allows practitioners either designated within the business entity or outsourced to an external third party to create and add retirement plans to be managed within My Plan Administration Account.	Yes	PBGC-14, My Plan Administration Account Authentication 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 application system is comprised of two main components, the Customer Module and the Administrative Module.*

*In the FMS PPS 3.16.1 release the FOD plans to publish the following data elements publicly.*

- *EIN*
- *PN*
- *PLAN ID*
- *PLAN NAME*
- *PLAN TYPE*
- *PLAN STATUS*
- *SPONSOR*
- *SPONSOR PHONE*
- *SPONSOR ADDRESS*
- *ADMINISTRATOR*
- *ADMINISTRATOR PHONE*
- *ADMINISTRATOR ADDRESS*
- *PRIOR EIN*
- *PRIOR PN*
- *NEW EIN*
- *NEW PN*

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. Customers acknowledge the following statement:*

*My PAA users are given and must acknowledge the following banner in order to proceed with using the system: SECURITY NOTICE AND WARNING. This website is a U.S. Government information system and is provided for authorized use only. Your usage of this system may be monitored, recorded, and subject to audit by PBGC. PBGC may use communications transmitted through, or data stored on, this information system for any official business purpose. This information system and its data are protected by U.S. federal laws, including, but not limited to, federal privacy laws, Title IV of ERISA, the Homeland Security Act, and the USA PATRIOT Act. Unauthorized use of this information system is prohibited and subject to criminal and civil penalties. Use of this information system by any individual, authorized or unauthorized, constitutes consent to these provisions. If you do not agree with these provisions, please close your browser or enter another URL to leave the site entirely.*

*Individuals have the opportunity to decline to provide information. However, declining to provide information prevents the user from creating a valid My PAA account, accessing the system, and submitting filings electronically. Although it is PBGC's policy that all plan administrators file electronically, exceptions can be granted for plan administrators to submit paper filings.*

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 any controls from an external provider, and there are no ISAs and MOUs in place. There is MOU/ISA is between Treasury and the credit card processing banks.*

5. For the user roles in the system:

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc)	Recertification Date
FOD-MyPAA Rpts Reconcile	27	User's supervisor & ISO	Read	All users on-board as of March 31, 2018 were recertified on June 10, 2019
FOD-MyPAA Rpts Operations	33	User's supervisor & ISO	Read	All users on-board as of March 31, 2019 were recertified on June 10, 2019
FOD-MyPAA Account Mgmt	33	User's supervisor & ISO	Read	All users on-board as of March 31, 2019 were recertified on June 10, 2019
FOD-MyPAA Inbox	30	User's supervisor & ISO	Read/Write	All users on-board as of March 31, 2019 were recertified on June 10, 2019
FOD-MyPAA Rpts Mgmt	24	User's supervisor & ISO	Read	All users on-board as of March 31, 2019 were recertified on June 10, 2019
FOD-MyPAA Inbox Read	4	User's supervisor & ISO	Read	All users on-board as of March 31, 2019 were

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc)	Recertification Date
				recertified on June 10, 2019
FOD-MyPAA Pwd Rules	4	User's supervisor & ISO	Read/Write	All users on-board as of March 31, 2019 were recertified on June 10, 2019
FOD-MyPAA Account Histories	9	User's supervisor & ISO	Read/Write	All users on-board as of March 31, 2019 were recertified on June 10, 2019
FOD-MyPAA Vendor XML Review	3	User's supervisor & ISO	Read	All users on-board as of March 31, 2019 were recertified on June 10, 2019
FILING COORDINATOR	12,009	CCRD	Read, Write	External users are not recertified, but accounts are disabled after 2 years of inactivity
ACCT_HISTORY	18,147	COORDINATOR	Read, Write	External users are not recertified, but accounts are disabled after 2 years of inactivity
PAYING_AGENT	15,016	COORDINATOR	Read, Write	External users are not recertified, but accounts are disabled after 2 years of inactivity
ACTUARY	3,104	COORDINATOR	Read, Write	External users are not recertified, but accounts are disabled after two years of inactivity
PLAN_ADMINISTRATOR	13,696	COORDINATOR	Read, Write	External users are not recertified, but accounts are disabled after two years of inactivity
PREPARER	19,209	COORDINATOR	Read, Write	External users are not recertified, but accounts are disabled after two years of inactivity
PLAN_ADMINISTRATOR_REP	2,002	COORDINATOR	Read, Write	External users are not recertified, but accounts are disabled after two 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.

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

- (1) Physical controls – Security guards, key entry, locked file cabinets, secured facility, closed circuit television, cipher locks, identification badges, and locked offices.*
- (2) Technical controls– Password protection, virtual private network, firewalls, unique user identification names, encryption, intrusion detection, personal identity verification, and public key infrastructure.*
- (3) Administrative controls – security audits, monitoring of user activity, refresher security, privacy, records management, and role-based training, backups secured off-site, encryption of backups, least privilege to restrict access to PII and Personal Identity Verification, and Public Key Infrastructure.*

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.

PBGC needs limited 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); and 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).
- Collect the originating IP address for forensic analysis.

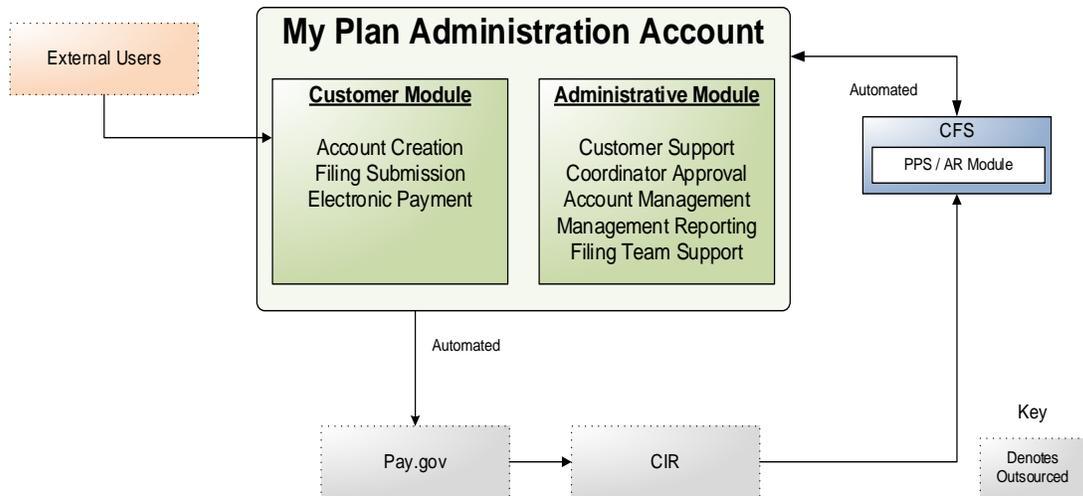
The My PAA account information is collected and used to:

- Authentic user access;
- Grant specific permissions or abilities within the online application; and
- Monitor access controls
- 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.

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 My Plan Administration Account application system is comprised of two main components, the Customer Module and the Administrative Module. The following diagram depicts the data flow.



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); and
- 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).
- 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

<b>Name of Reviewer</b>	
<b>Date Reviewed</b>	
<b>Expiration Date</b>	
<b>Result</b>	<input type="checkbox"/> Approved without conditions <input type="checkbox"/> Approved with conditions (see below). <input type="checkbox"/> Denied

*(For Privacy Office Use Only)*

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

<i>Enter description here.</i>
--------------------------------

Discuss any conditions on Approval

<i>Enter description here.</i>
--------------------------------

## 2.4 Signatures and Approval

Information System Owner/Information Owner	
Name: Raymond Bryant	
Dept/Office: FOD, CCRD	
Phone: 202-326-4065 Ext. 3591	
Email: Bryant.Raymond@PBG.C.Gov	
I certify that this PIA is an accurate representation of the security and privacy controls in place to protect the PII that the system does/will collect or maintain.	
Signature	_____
	_____
Date signed	_____
	_____

Authorizing Official	
Name: Theodore J. Winter, Jr.	
Dept/Office: FOD, Director	
Phone: 202-326-4060 Ext. 6296	
Email: Winter.Theodore@PBG.C.Gov	
I certify that this PIA is an accurate representation of the security and privacy controls in place to protect the PII that the system does/will collect or maintain.	
Signature	_____
	_____
Date signed	_____
	_____

Chief Privacy Officer	
Name: Shawn Hartley	
I certify that I have reviewed this PIA and have fully considered the privacy risks that this system creates.	
Signature	_____
	_____
Date signed	_____
	_____

***This page is for internal routing purposes of documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.***