Pension Benefit
Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Disclosure Access Portal (DAP) Privacy Impact Assessment (PIA)

Last Updated: 04/24/2024

1 PRIVACY POINT OF CONTACT

Name	Les Hockman
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.3879
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)*
FOIAXpress (FX)	The FOIAXpress application processes requests for release of FOIA and privacy data from PBGC.	Yes	PBGC-29: Freedom of Information Act and Privacy Act Request Records	5 U.S.C. § 552, The Freedom of Information Act (FOIA), and 5 U.S.C. § 552a, The Privacy Act of 1974 (PA); Parts 4901 and 4902 of Title 29 of the Code of Federal Regulations.	Yes
Public Access Link (PAL)	The PAL application is the public-facing web portal that complements FOIAXpress to provide efficient and secure communication between citizens and PBGC. Information like address, email address is entered into the system for it to assist PBGC in tracking, managing, and reporting correspondence, FOIA and Privacy Act (PA) requests. PAL will allow requestors to: • Submit a FOIA request online. • Check the status of an existing request.	Yes	PBGC-29: Freedom of Information Act and Privacy Act Request Records	5 U.S.C. § 552, The Freedom of Information Act (FOIA), and 5 U.S.C. § 552a, The Privacy Act of 1974 (PA); Parts 4901 and 4902 of Title 29 of the Code of Federal Regulations.	Yes

Name of component	Describe the component (1 or 2 sentences)	Does this componen t 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)*
	• E-Mail the PBGC POC assigned to their request; • Upload documentation, such as a Request Description, Fee Waiver Request, or a Request for Expedited Processing; • Download the material deemed responsive to a request along with agency correspondence for a request; and • Submit an appeal.				
FOIAXpress Collaboration Portal	The FOIAXpress Collaboration Portal enables FOIAXpress users to collaborate securely with external parties outside of the FX application. Non-users can locate responsive documents and work with FOIA staff on requests without accessing the FX application.	Yes	PBGC-29: Freedom of Information Act and Privacy Act Request Records	5 U.S.C. § 552, The Freedom of Information Act (FOIA), and 5 U.S.C. § 552a, The Privacy Act of 1974 (PA); Parts 4901 and 4902 of Title 29 of the Code of Federal Regulations.	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).

The Disclosure Access Portal (DAP), a Software as a Service (SaaS) *is built on the* ***eCase*** *adaptive case management platform that offers PBGC a single unified application for managing the entire lifecycle of FOIA and Privacy Act (PA) requests and appeals - from initial inquiry request receipt through the Public Access Link (PAL) requester portal to document request, review, redaction, to delivery of documents through archiving and deletion according to agency retention rules. The DAP SaaS Solution includes: the FOIAXpress application (FX), the Public Access Link (PAL) application, and the FOIAXpress Collaboration Portal (an additional application, named eCase, is included with the DAP cloud service but is not used by PBGC).*

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.

The sources from which DAP collects PII include electronic forms, regular mail, email, and fax. The PII collected includes name, organization (if any), address, and phone number. DAP does not require requestors to provide or directly collect their SSN, Customer ID, Birth Date, or Driver's/Non-Driver's license number. PII is collected from Requestors who have submitted FOIA requests, PA requests, or combined FOIA and PA requests for records or information and administrative appeals or have litigation pending with a federal agency; individuals whose requests, appeals or records have been referred to PBGC by other agencies. However, some requestors provide this information voluntarily in the request description field. The system login page will include a link to the full Privacy Act statements related to the system.

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 any external provider.

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
FOIA Administrator	1	James Burns	Full Access to All Role Permissions (other than configuration) (Read, Write, Delivery, Deletion,	4/19/2024
Government Information Specialists	14	James Burns	Access to All Request Type Role Permissions and File Cabinet Drawer Permissions Only (Read, Write, Delivery & Deletion Capabilities)	4/19/2024
FOIA Appeals	6	James Burns	Access to the Appeals Adjudication Functions and File Cabinet Drawer Permissions (Read, Write, & Delivery Capabilities)	4/19/2024
FOIA Professional	1	James Burns	Limited Request Type Role Permissions (Read & Write Capabilities)	4/19/2024
CyberArk	4	Paul Chalmers	Access to Configuration Capabilities (Can access maintenance console via CyberArk to change limited system settings, and do ICAM and Splunk reporting)	4/19/2024

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 Mission*
- ○ *Access Control for Output Devices*
- ○ *Monitoring Physical Access*
- ○ *Visitor Control*
- ○ *Access Records*
- ○ *Power Equipment and Power Cabling*
- ○ *Emergency Shutoff*
- ○ *Emergency Power*
- ○ *Emergency Lighting*
- ○ *Fire Protection*
- ○ *Temperature and Humidity Controls*
- ○ *Delivery and Removal*
- ○ *Alternate Work Site*
- ○ *Location of information Components*
- ○ *Information Leakage*

**Physical Controls are provided by both PBGC and the Cloud Service Provider (CSP)*

Technical Controls - Technical controls employed to secure the PII in the system include:*

- ○ *Account Management*
- ○ *Access Enforcement*
- ○ *Authenticator Management*
- ○ *Cryptographic Module Authentication*
- ○ *Information Flow Enforcement*
- ○ *Separation of Duties*
- ○ *Least Privilege*
- ○ *Unsuccessful Login Attempts*
- ○ *Remote Access*
- ○ *Wireless Access*
- ○ *Audit Events*
- ○ *Audit Review, Analysis, and Reporting*
- ○ *Time Stamps*
- ○ *Audit Record Retention*
- ○ *Non-repudiation*
- ○ *Session Audit*

- *Public Key Infrastructure Certificates*
- *Denial of Service*
- *Network Disconnect*
- *Session Authenticity*
- *Protection of Information at Rest*

***Technical Controls are provided by both PBGC and the CSP*

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*

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.

The intended use of PII provided by requestors is to aid the processing of requests for records made under the provisions of the FOIA and PA, and to assist PBGC in carrying out other responsibilities relating to FOIA and PA including operational, management, and reporting purposes. PII collection is limited to only that information needed to complete the purpose for which the PII is requested.

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.

PAL users encompass any individual who goes to the PAL web address and submits an account registration request. An account will be created, along with an associated user ID and password. Requestors will log onto the system by accessing the designated URL and enter their respective login/password credentials. Users/Requestors can then submit and track the status of FOIA and PA requests over the internet. FX users are PBGC employees who log into the FOIAXpress system by accessing the designated URL and enter their respective login/password credentials. Information received by the FX user from the public may include personal identification information and financial information related to the processing of FOIA request. FOIAXpress stores files within the correspondence log for a request. The FOIAXpress Collaboration Portal enables users to collaborate securely with *external parties outside of FOIAXpress. Requestors can locate responsive documents and work with the FOIAXpress user on requests through the FOIAXpress Collaboration Portal without accessing the FOIAXress application. Also, files are stored within the document management module (for responsive records) which may include but are not limited to the following:*

Correspondence from the requester (which may contain their name, address, phone#, etc.)

- *Incoming request letter*
- *Clarification letter*
- *Fee agreement letter*

Correspondence to the requester (which may contain their name, address, phone #, etc.)

- *Acknowledgement letter*
- *Final response letter*
- *Redacted responsive records*

Document management files

- *Original (un-redacted) responsive records*
- *Redacted responsive records*

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?

The Disclosure Division collects SSN in limited circumstances when the Privacy Act records requestor does not have a PBGC Customer ID Number, other information provided is insufficient to confirm the requester's identity, and the individual is requesting Privacy Act records.

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

Compelling Business Need

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.

The Disclosure Division and Privacy Office has reviewed and amend the Certification of Identity Form eliminating the collection of SSN as a primary identifier in connection with Privacy Act requests.

2.3 Privacy Office Review

Name of Reviewer	Margaret Drake
Date Reviewed	4/24/2024
Expiration Date	12 months from the date of Privacy Office review
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
