Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)

Financial Disclosure Online (FDonline)

04/16/2025

1 Privacy Point of Contact

Name	Daniel Wheeler
Title	Information Owner
Phone	202-229-6873
Email	wheeler.daniel@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 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.

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.

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)*
FDonline	FDonline is a solution for automating the annual financial disclosure process. FDonline facilitates the automation of the United States Office of Government Ethics (OGE) Form 450.	Yes	OGE/GOVT-2 Executive Branch Confidential Financial Disclosure Reports Privacy Act system of records notice.	5 U.S.C. Chapter 131-Ethics in Government and 5 CFR Part 2634, Subpart I-Confidential Financial Disclosure Reports of the Office of Government Ethics regulations require the reporting of this information.	No

2.2 The System as a Whole

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

FDonline electronically notifies filers of the requirement to file and provides a link to a program that walks the filer through the entire form-filing process. The application automatically reminds filers of their need to file as due dates approach, allows for electronic filing, and automates management reports of non-filers. FDonline is an existing system that goes through annual recertification

2. What is 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.

No changes have been made to the system since its last review

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, the system does not collect, process, or maintain any records that describe how any individual exercises their First Amendment rights.

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, -

The information in FDonline is used only for review by Government officials of the federal employee's agency and determining compliance with applicable federal conflict of interest laws and regulations.

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.

There should be no PII. All users' info is their PBGC info

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

200 Filers

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

The submission of PII is mandatory

10. If your system collects Social Security Numbers (SSNs):
    a. Please provide justification for the collection, use, maintenance, and disposal of PII in the form of SSN?

FDonline does not collect SSN

    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.

FDonline does not have or ask for PII. Nevertheless, the potential for inadvertent and unsolicited disclosure of PII by a user warrants a PIA for this system. If FDonline asks for a work address, some users may mistakenly put their home address instead of their work address, resulting in PII in the system.

System users access the system via a Hypertext Transfer Protocol Secure (HTTPS) connection and complete the OGC form. PII is uploaded into the Intelliworx system via an online form.

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),

PBGC does not inherit any privacy controls from the service provider. No MOU, ISA, or similar documents are required because there is no dedicated connection. To complete the online form, system users access the system via an HTTPS connection or similar document is in place, please summarize the privacy applicable portions of that document.

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.

Application users access the system and input and manipulate data solely through HTTPS TLS security via their Web browser.

14. For the user roles in the system:

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc)	Recertification Date
Filer	200	Daniel Wheeler, Thom Verratti, or James Burns	Access only to their own files.	09/18/2024
Administrator Reviewer	4		Review and edit.	
Super Administrators	2		Full access to the system.	

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

All users sign a non-disclosure agreement.

Staff (employees and contractors) receive security and privacy training.

Access to PII is restricted to authorized personnel only.

Access to PII is monitored and tracked through the comments/review section within FDonline.

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

N/A

17. Does the System leverage 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).

Records containing personally identifiable information (PII) are maintained and destroyed in accordance with the National Archives and Records Administration's (NARA) Basic Laws and Authorities (44 U.S.C. 3301, et seq.) and with PBGC-specific records disposition schedules approved by NARA. These retention schedules ensure that records are kept for the minimum period necessary to satisfy business, legal, and historical requirements.

The following PBGC and General Records Schedules (GRS) govern retention and destruction of CLMS records:

PBGC 1.7, PBGC 1.8, PBGC 2.2, PBGC 2.3, GRS 1.1 (Item 001), GRS 2.3 (Item 050),

GRS 2.8 (Items 010, 020, 050, 100, 101), GRS 3.2 (Item 010), GRS 4.2 (Items 001, 020, 160, 161), GRS 5.1 (Item 010), GRS 5.7 (Item 050)

Retention requirements within these schedules range from 1 year to 135 years, or are triggered by specific events, ensuring alignment with PBGC's operational and legal needs.

2.3 Privacy Office Review

Name of Reviewer	Loretta Dennison
Date Reviewed	04/16/2025
Expiration Date	04/16/2026
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.