Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)

PBGC.gov

05/15/2025

1   Privacy Point of Contact

Name	Timothy Green
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202-229-3664
Email	green.timothy@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 13*)?
Employers & Practitioners: Pending Proposed Rules	This page displays comments on the proposed regulations sent to PBGC Office of the General Counsel (OGC).	Yes – Rulemaking comments submitted by individuals may contain name, contact information, or other PII.	PBGC-25: PBGC.gov Comment Management System	The Administrative Procedure Act 5 USC §551 et seq. (1946)	No
General web content	Content provided on PBGC.gov about the mission of the agency, its operations, forms and instructions, data, and how to contact the agency.	No	N/A	N/A	No

2.2 The System as a Whole

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

> PBGC.gov uses Acquia Cloud, a Platform as a Service (PaaS) provided by the Certified Cloud Service Provider (CSP), Acquia. Acquia Cloud received the Federal Risk and Authorization Management Program (FedRAMP) authorization on 04/13/2016. Drupal is the web content management system (CMS) used by PBGC.gov. The website, including Drupal code and modules, are hosted by Acquia. PBGC.gov upgraded to Drupal 10 includes updated modules and continued support from the open-source development community. The Drupal 10 code base is very similar to Drupal 9.5, and the upgrade required significantly less effort than when PBGC migrated from Drupal 7 to 9. There was no impact on privacy.
>
> PBGC.gov is an official government website that disseminates information to the public. PBGC's mission is to enhance retirement security by preserving and encouraging the continuation of private pension plans and by protecting the benefits of workers and retirees in traditional pension plans. PBGC.gov plays a vital role in accomplishing that mission. PBGC.gov's visitors include workers and retirees, employers and pension practitioners, policymakers, and the general public. The website contains information about PBGC's mission, pension benefits, and premium filings, along with press releases and a variety of other content. Visitors can access resources like PBGC's contact information, details about trusteed pension plans, and lists of which pension plans PBGC insures

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.

> 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, timeliness, and completeness of PII throughout the information life cycle.

The PBGC Office of the General Counsel (OGC) emails comments collected from https://www.reginfo.gov or submitted directly to OGC on proposed regulations for display on PBGC.gov. OGC reviews comments received before forwarding for posting to the website. There are no intended uses of the PII.

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.

N/A

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

Several hundred.

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 is voluntary. Users can also choose to remove or redact their PII when submitting comments on pending regulations.

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 (PBGC.gov 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.

> PBGC.gov may collect PII from the sources listed below:
>
>   1. Individuals
>   2. OGC
>
> The PBGC Office of the General Counsel (OGC) provides comments collected from https://www.reginfo.gov or submitted directly to OGC on proposed regulations to the Communications, Outreach & Legislative affairs Department (COLAD) for display on PBGC.gov. Since PII is not collected from the individual within this boundary, the Privacy Act Statement is not applicable to PBGC.gov.

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 Acquia, and no ISA is required since there is no dedicated or persistent connection between PBGC and Acquia.

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.

The PBGC Office of the General Counsel (OGC) emails comments collected from https://www.reginfo.gov or submitted directly to OGC on proposed regulations for display on PBGC.gov. OGC reviews comments received before forwarding for posting to the website. Once the information is posted on PBGC.gov, it is publicly available.

14. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Administrator	3	Michael Rucki	Read/Write/Approve/ Publish	5/8/2025
Editor	12	Michael Rucki	Read/Write/Approve	5/8/2025
Author	25	Michael Rucki	Read/Write	5/8/2025
Reviewer	3	Michael Rucki	Read	5/8/2025
Site Manager	11	Michael Rucki	Read/Write/Approve/ Publish	5/8/2025

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

Physical security controls employed to secure the PII in the system included: security guards, key entry, secured facility, closed circuit television, identification badges and locked offices.

Technical controls employed to secure the PII in the system included: IP address restrictions, firewalls, unique user identification names, passwords, encryption, and intrusion detection system.

Administrative controls employed to secure the PII in the system include Periodic security audits, regular monitoring of user activities, annual refresher training for security, privacy and records management, backups secured offsite, role-based training, methods to ensure that only authorized personnel have access to PII, and mandatory on-boarding training for security, privacy, and records management.

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 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).

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	Duane Dodson
Date Reviewed	05/15/2025
Expiration Date	05/15/2026
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