Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)

Case Legal Management System

(CLMS)

11/25/2024

1 Privacy Point of Contact

Name	Lisa Hozey
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202-229-5607
Email	hozey.lisa@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)*
Case Legal Management System (CLMS) *(replaces TeamConnect)*	Case/Legal Management System (CLMS) is a single modernized enterprise case management system built on Microsoft Dynamics and hosted in Microsoft Azure that is used to identify and mitigate pension plan risks through reportable event, litigation, early warning, standard termination, and multiemployer case and matter tracking for plan sponsors or pension plans necessitating an open case or matter. It will also be used to manage litigation, procurement, ethics, and other matters handled by the Office of General Counsel (OGC)'s General Law and Operations Department (GLOD).	Yes	PBGC-19 Office of Negotiations and Restructuring/Office of General Counsel Case Management System	29 U.S.C. 1055, 1056(d)(3), 1302, 1303, 1310, 1321, 1322a, 1341, 1342, 1343, 1350; 1431, and 1432; 5 U.S.C. app. 105; 5 U.S.C. 301, 552(a), 552a(d), 7101; 42 U.S.C. 2000e, et seq.; 44 U.S.C. 3101.	Yes
e-Filing Portal	e-Filing Portal is an online application that allows pension plan practitioners to file annual financial and actuarial information and create and submit 4010 tax filings per section 4010 and 4043 of the Employees Retirement Security Act (ERISA), which requires certain underfunded plans to report identifying financial and	Yes	PBGC-19 Office of Negotiations and Restructuring/Office of General Counsel Case Management System	29 U.S.C. 1055, 1056(d)(3), 1302, 1303, 1310, 1321, 1322a, 1341, 1342, 1343, 1350; 1431, and 1432; 5 U.S.C. app. 105; 5 U.S.C. 301, 552(a), 552a(d), 7101; 42 U.S.C. 2000e, et seq.; 44 U.S.C. 3101.	Yes

	actuarial information to PBGC. Multiemployer plan practitioners also use the e-Filing Portal to file notices and applications, along with any corresponding documentation. The following filings are required to be submitted to PBGC using the e-Filing Portal: notices of termination (29CFR part 4041A) and notices of insolvency, insolvency benefit level, and applications for financial assistance (29 CFR part 4245 or 29 CFR part 4281), and applications for special financial assistance (29 CFR Part 4262). The e-Filing Portal also allows practitioners to submit annual funding notices and critical or endangering status notices.				
File Room	The document capture functionality in CLMS enables the OGC File Room and other select users to categorize and upload paper documents (e.g., mail to PBGC) into the system. It also provides Optical Character Recognition (OCR) functionality to make the documents searchable for users within CLMS.	Yes	PBGC-19 Office of Negotiations and Restructuring/Office of General Counsel Case Management System	29 U.S.C. 1055, 1056(d)(3), 1302, 1303, 1310, 1321, 1322a, 1341, 1342, 1343, 1350; 1431, and 1432; 5 U.S.C. app. 105; 5 U.S.C. 301, 552(a), 552a(d), 7101; 42 U.S.C. 2000e, et seq.; 44 U.S.C. 3101.	Yes
CLMS-G *(formerly known as OGCInternal/LTP/LMS a.k.a. LEW)*	CLMS-G, the Office of the General Counsel (OGC) system, is designed to store information pertinent to legal matters, compiled by OGC attorneys, facilitating the practice of law in their related	Yes	PBGC-19 Office of Negotiations and Restructuring/Office of General Counsel Case Management System	29 U.S.C. 1055, 1056(d)(3), 1302, 1303, 1310, 1321, 1322a, 1341, 1342, 1343, 1350; 1431, and 1432; 5 U.S.C. app. 105; 5 U.S.C. 301, 552(a), 552a(d), 7101; 42 U.S.C. 2000e, et seq.; 44 U.S.C. 3101.	Yes

	matters such as litigation, procurement ethical considerations.				

2.2 The System as a Whole

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

Case/Legal Management System (CLMS) *is a single modernized enterprise case management system built on Microsoft Dynamics and hosted in Microsoft Azure. CLMS is managed by two sponsoring business units, the Office of General Counsel (OGC) and the Office of Negotiation and Restructuring (ONR). CLMS replaces the Risk Management Early Warning (RMEW) system (including TeamConnect, Document Management System (DMS), Capture, and eFiling Portal), Case Management System (CMS) (for Standard Termination and Coverage Determination (STCD) users, and Legal Management System (LMS) (for a broad range of legal issues being addressed by OGC's General Law and Operations Department (GLOD)).*

This system is used to identify and mitigate pension plan risks through reportable event, litigation, early warning, standard termination, and multiemployer case and matter tracking for plan sponsors or pension plans necessitating an open case or matter. It is also used to manage litigation, procurement, ethics, and other matters handled by GLOD. CLMS is a child of the parent ITISGSS system and is not FISMA reportable.

2. What are the Confidentiality, Availability, and Integrity ratings for the system as a whole?

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

3. Is this system owned and/or controlled by PBGC or an external party? If so, who owns and/or controls the system?

CLMS is a child system owned by PBGC and is managed by two sponsoring business units, the Office of General Counsel (OGC) and the Office of Negotiation and Restructuring (ONR).

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.)

CLMS does not directly collect or process any records that describe how an individual exercises their First Amendment rights. However, records from other systems that collect or process this information may be maintained in case files within CLMS.

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.

All documents associated with a given case (legal matter) might contain any type of PII either as information in a free-form document or within relevant copies of records from other PBGC systems; however as described above, this PII data is not collected directly from the individual by the CLMS. These documents, and thus all data within the documents, have been deemed relevant to the matter by the analysts or attorneys who are assigned to that matter.

CLMS receives limited PII as a result of mission activities including, but not limited to, case analysis, actuarial analysis (including single-employer and multiemployer plan actuarial analyses), insolvent multiemployer plan audits, standard termination audits, as a result of litigation in both pension plan liability cases and PBGC employee and contractor disputes. Any PII contained in the e-Filing Portal is uploaded by pension plan practitioners to submit documentation attachments which may contain PII.

PII is deemed necessary and relevant in certain casework, and actuaries may use individual data for analysis (when aggregate data is not available). However, outputs are in aggregate so as to limit access to PII.

PII included in the system for GLOD matters is limited to that necessary to address personnel matters, litigation, or to address ethics matters. The information is added by the attorneys or other personnel assigned to the matter and access is restricted to those assigned to a specific matter.

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.

PII is incidentally received in documents via the e-Filing Portal and is associated with Plan Sponsors or Pension Plans.

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

Up to 95,000

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.

NA, please see number 10 below.

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

While SSNs are received from other PBGC systems which collect them directly from plan sponsors, or litigants, they are reviewed as part of legal discovery or used to resolve any case or matter handled by OGC or ONR, CLMS does not collect SSNs directly from individuals.

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

Not Applicable

    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.

Not Applicable

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.

CLMS does not collect any new PII directly from the subject individual; rather, it compiles PII that exists in documents uploaded by filers or users.

Once a "case" (case or legal matter) has been created, the case will include one or more documents that may originate from any outside source, including additional physical documents (scanned and added to the case), records from any other PBGC system (copies of documents which are extracted from another system and added to the case), and new original free-text documents created by a CLMS user and added to the case (as with an attorney's case notes). These case-related documents are not keyed to specific PII values but could contain various forms of PII, including key values from other PBGC systems.

As CLMS does not collect PII directly from a subject individual, it does not have any relevant Privacy Act Statements. Since the CLMS system needs to work with documents/records from other systems, the information on those documents should not be "corrected" or otherwise changed unless notified by the originating system.

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.

No privacy controls are inherited from external providers. CLMS does not interconnect with any external systems, therefore no ISAs or MOUs are required

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 (including 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.

CLMS's data repository in Microsoft Dataverse (Dynamics365 backend) will initially be populated with data obtained from TeamConnect, Case Management System (CMS), Standard Termination and Coverage Determination (STCD) cases, Legal Management System (LMS), FileNet, file shares, and SharePoint. Initial data population will occur using a suite of data and document migration tools that includes Kingsway Soft (SSIS Jobs), Proventeq Migration Accelerator, and Sharegate. Once operational, database scan listeners will detect new data received into databases supporting the RMEW system, eFiling Portal, LMS, CMS, and Premium Practitioner System (PPS); CLMS will then automatically import that data into Dataverse. Documents will be migrated from the Image Processing System (IPS) (STCD documents) and DMS FileNet repositories to SharePoint Online sites that are integrated with CLMS. Additionally, new documents that are received by the file room shall be scanned and processed into the CLMS system SharePoint Online sites via Kofax TotalAgility.

Routine uses for PII data stored in CLMS will be the same as the legacy systems (LMS and RMEW) as listed in SORN PBGC-19 (OGC Case Management System).

PII stored in CLMS for consumption by ONR and OGC users (other than GLOD users with confidential matters) can be shared with PBGC's Office of Benefits Administration (OBA) for review during pre- and post-trusteeship to support the plan termination process. This information will be shared via a secure interface for OBA use via CLMS-CMS one-way interface for data and via SharePoint Online access for documents. This interconnection will be documented on the Relationships page of the CLMS record in CSAM and will be governed by an Interface Control Document (ICD) to be developed by the CLMS program. Because CLMS is an internal system and is not connected to an external system, no Interconnection Security Agreement (ISA) is required.

14. For the user roles in the system:

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc)	Recertification Date
Regular User	339	Service/Application Owner	Read, Write	May 2024
Regular User- Read Only	123	Service/Application Owner	Read	May 2024
AP User (Cyber Ark)	20	Service/Application Owner	Privileged, Admin	May 2024
Service Accounts	17	Service/Application Owner	Privileged, Admin	May 2024

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

CLMS is entirely in Azure Government (Azure-G). Azure-G lives in the Microsoft data center. ***Physical controls*** *provided by the CSP Includes:*

- *Physical Access Authorizations*
- *Physical Access Control*
- *Access Control For Transmission Medium*
- *Access Control For Output Devices*
- *Monitoring Physical Access*
- *Visitor Access Records*
- *Power Equipment and Cabling*
- *Emergency Shutoff*
- *Emergency Power*
- *Emergency Lighting*
- *Fire Protection*
- *Temperature and Humidity Controls*
- *Water Damage Protection*
- *Alternate Work Site*
- *Location of Information System Components*

Technical controls *employed to secure the PII in the system include Access Enforcement, Information Flow enforcement, Least Privileges, System Use Notification, Session Lock, Personal Identity Verification (PIV) card access, Session Termination, Remote Access, Time Stamps, Identifier Management, Authenticator Management. Technical Controls are provided by PBGC*

Administrative controls *include periodic security audits, annual refresher training for security, privacy, insider threat and records management, role-based training, and mandatory training during onboarding for security, and privacy and record management. Administrative Controls are provided by PBGC.*

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

The Agency Records Officer offers training and guidance to stakeholders (including system administrators, ONR, and OGC) on retention schedules, proper disposal methods, and the handling of potential exceptions (e.g., litigation holds).

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.

Applicable Records Schedules

The Case Legal Management System (CLMS) and related systems (e.g., CLMS-G) house pension benefit claims and related data, often covering beneficiaries' lifetimes. As such, retention periods can be substantial—sometimes spanning several decades—to accommodate long-term service needs.

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 (e.g., final payment, closure of a case, end of participant/beneficiary's life), ensuring alignment with PBGC's operational and legal needs.

CLMS-Specific Retention

Due to the nature of pension benefits, CLMS retains records—including any incidental PII—for the life of the pensioner or beneficiary, plus any additional time frames specified by PBGC policy or NARA-approved schedules. This extended retention

ensures that PBGC can effectively service beneficiaries' needs throughout their lifetimes and address any subsequent legal or programmatic requirements.

Destruction Authority and Methods

Paper Records: Hardcopy files are shredded or otherwise destroyed beyond recognition.

Electronic Records: E-records stored in CLMS or associated repositories (e.g., SharePoint) are permanently deleted once retention periods are met. This may include a multi-stage process (e.g., recycle bin, secondary recycle bin, final deletion) to ensure data is irretrievable.

The Agency Records Officer coordinates official disposal actions, validating that retention requirements have been met and that destruction is conducted securely and completely. When necessary, the Office of the General Counsel (OGC) may also be involved.

Event-Based and Time-Based Dispositions

Depending on the record series, destruction timelines may start at an event (e.g., date of final payment, end of beneficiary coverage) or after a fixed period (e.g., 7 years, 75 years, etc.).

Records that reach their disposal date are reviewed to ensure no ongoing legal holds, investigations, or audits require further retention.

2.3 Privacy Office Review

Name of Reviewer	Bill Black
Date Reviewed	2/12/2025
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

Enter description here.