Pension Benefit Guaranty Corporation

Case and Legal Management System (CLMS)

Privacy Impact Assessment (PIA)

Last Updated: 2/15/2024

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)*
Case Legal Management System (CLMS) ***(formerly known as 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.	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 Employee Retirement Security Act (ERISA), which requires certain underfunded	Yes	PBGC-19 Office of Negotiations and Restructuring/Office of General Counsel Case Management System	See first table entry.	Yes

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)*
	plans to report identifying financial and 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 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	See first table entry	Yes

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)*
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 matters such as litigation, procurement, and ethical considerations.	Yes	PBGC-19 Office of Negotiations and Restructuring/Office of General Counsel Case Management System	See first table entry	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).

Case/Legal Management System (CLMS) *is a single modernized enterprise case management system built on Microsoft Dynamics and hosted in Microsoft Azure. CLMS will be 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 will be 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 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. 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 will not collect any new PII directly from the subject individual; rather, it will compile 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.

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.

No privacy controls are inherited from external providers. The e-Filing Portal portion of CLMS connects to Login.gov and there is an Inter-agency Agreement in place for this connection.

5. 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	316	Service/Application Owner	Read/Write	N/A*
Regular User – Read Only	36	Service/Application Owner	Read	N/A*
AP Users (CyberArk)	29	Service/Application Owner	Read/Write	N/A*
Service Accounts	15	Service/Application Owner	Read/Write	N/A*

*N/A meaning not yet recertified because it is a new system.

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.

CLMS is entirely in Azure Government (Azure-G). Azure-G lives in the Microsoft data center. Physical controls are not managed by PBGC.

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.

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.

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.

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.

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.

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).

Relevant 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. PBGC has an IAA in place with GSA to reflect the one external connection between the E-Filing Portal and Login.gov.

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?

While SSNs are received from other PBGC systems, plan sponsors, or litigants, and 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 within the purview of this question.

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

2.3 Privacy Office Review

Name of Reviewer	Bill Black
Date Reviewed	2/16/2024
Expiration Date	12 months from the date of concurrence by 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.