Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)

Risk Management Early Warning (RMEW)

February 2021

1 Privacy Point of Contact

Name	Alexander Reed
Title	Information System Owner (ISO)
Phone	202-229- 6600
Email	Reed.Alexander@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.

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.

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 externally? *(please detail in question 9)*
TeamConnect	RMEW's TeamConnect is a legal matter and case management system that gives RMEW the ability to share common information and coordinate more closely on a wide range of cases and legal matters, including plan termination actions, bankruptcy matters, and reportable event filings.	Yes	PBGC 19	29 U.S.C. 1055, 1056(d)(3), 1310, 1322a, 1341, 1342, 1343, 1350, 4010, 4041, 4042, and 4043; 5 U.S.C. app. 105;	No
Document Management System (DMS)	DMS serves as a document repository for TeamConnect. It is used for the capture, storage, and retrieval of	Yes	PBGC 19	29 U.S.C. 1055, 1056(d)(3), 1310, 1322a, 1341, 1342, 1343, 1350, 4010, 4041, 4042, and 4043; 5 U.S.C. app. 105;	No

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 externally? *(please detail in question 9)*
	documents. DMS adds to RMEW the mechanism to store the content of those documents in a searchable .pdf format.				
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 of the Employees Retirement Security Act (ERISA), which requires certain underfunded plans to report identifying financial and	Yes	PBGC 19	29 U.S.C. 1055, 1056(d)(3), 1310, 1322a, 1341, 1342, 1343, 1350, 4010, 4041, 4042, and 4043; 5 U.S.C. app. 105; 44 U.S.C. 3101	No

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 externally? *(please detail in question 9)*
	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 and insolvency benefit (29 CFR part 4245 or 29 CFR part 4281). The e-Filing Portal also allows practitioners to				

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 externally? *(please detail in question 9)*
	submit annual funding notices and critical or endangering status notices.				

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).

RMEW is the primary case, document, and legal matter management system that is used by:

1. Corporate Finance & Restructuring (CFRD)
2. Multiemployer Program Division (MEPD)
3. Negotiations and Restructuring Actuarial Division (NRAD)
4. Office of the General Counsel (OGC)

Each of these units supports the strategic corporate goal of safeguarding the pension insurance system by 1) the early identification of pension plan risks and 2) providing proper mitigation of those risks through legal action, settlement, or plan termination. RMEW provides ONR and OGC reportable event, litigation, and early warning case tracking for retirement plans at risk for failure, providing those four PBGC departments with the necessary information sharing capabilities.

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 RMEW System does not collect PII directly from individuals. PII may be submitted as part of attachments uploaded by filers. No PII is shared outside of the RMEW.

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.

RMEW inherits no privacy controls from an external provider. There is no applicable ISA nor MOU.

5. For the user roles in the system:

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc)	Recertification Date
User Accounts	196	ISO	Read/Write	May 2020
User Accounts: Read Only	52	ISO	Read	May 2020
System/Interface Accounts	4	ISO	Full	May 2020
System Administrators	4	ISO	Full	May 2020

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 security controls employed to secure the PII in the system include security guards, identification badges, locked offices, and secured facilities. Technical controls employed to secure the PII in the system include password protection, network firewalls, unique user identification names, encryption, and an intrusion detection system. Administrative security controls employed to secure the PII in the system include periodic security audits, annual refresher training for security, privacy and records management, mandatory on-boarding training for security, privacy and records management, and methods to ensure that only authorized personnel have access to PII.

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 limited PII in TeamConnect and DMS is received as a result of ONR mission activities, including, but not limited to, case analysis, actuarial analysis (including single-employer and multiemployer plan actuarial analyses), or as a result of litigation. Any PII contained in the e-Filing Portal is uploaded by pension plan practitioners utilizing the system to submit documentation attachments which may contain PII.

PII is deemed necessary and relevant in certain casework within ONR. NRAD 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.

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.

Any PII in RMEW can be shared with PBGC's Office of Benefits Administration OBA). OBA has a need to review documents in RMEW during pre- and post-trusteeship to support the plan termination process. The information is shared via a secure interface, which automatically moves scanned documents from TeamConnect into OBA's image processing system (IPS) for OBA use.

RMEW interfaces with the following systems:

- Case Management System (CMS) owned by Office of Benefits Administration (OBA).
- Premium & Practitioner System (PPS) is a module of the Consolidated Financial System (CFS), owned by Financial Operations Department (FOD).
- Information Technology Infrastructure Services General Support System (ITISGSS) owned by ITIOD.

These data interconnections are noted in Cyber Security Asset Management (CSAM). Data shared internally within PBGC systems does not require an MOU/ISA.

10. Does the system leverage the commonly offered control for Accounting of Disclosures?

☒ Yes
☐ No

2.3 Privacy Office Review

Name of Reviewer	Drew Kuchinski
Date Reviewed	2/16/2021
Expiration Date	2/16/2022
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.