

**Pension Benefit Guaranty Corporation (PBGC)  
Privacy Impact Assessment (PIA)**



**eDiscovery  
05/10/2019**

# 1 Privacy Point of Contact

<b>Name</b>	Daniel Wheeler
<b>Title</b>	Information Owner
<b>Phone</b>	202-326-4000, ext. 6873
<b>Email</b>	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.

*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 internally <i>(please detail in question 9)</i>
eDiscovery	eDiscovery is an externally hosted litigation support service that provides an environment to support Office of the General Counsel (OGC). It allows OGC to perform electronic discovery functions as required by applicable federal law and the federal Rules of civil procedures.	Yes	eDiscovery does not operate as a system of records but rather processes information from other PBGC systems for which there are current Systems of Records Notice (SORN)s.	29 CFR part 4000, the federal Rules of Civil procedure and orders issued by the court or other adjudicative bodies	No

## 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)

The purpose of eDiscovery is to support the mandatory production of documents, including agency records, in pending civil litigation. Records in eDiscovery are compiled and created, which then allows legal teams to access copies of records gathered from other PBGC systems for review, analysis and coding. eDiscovery is an existing system, but it is changing vendors and seeking a new ATO.

2. What is 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.

eDiscovery collects PII from other PBGC systems. The nature of those records may vary from case to case. Generally, documents uploaded to the eDiscovery service have been gathered by PBGC counsel or provided by outside counsel as part of the discovery phase in a legal matter.

eDiscovery is not a primary information collection system. Any right or opportunity to consent or decline occurs at the point of original collection from the individual and is described in the relevant SORN for that record-keeping system, program or activity from which the eDiscovery data is gathered. Since the litigation discovery process is compulsory, PBGC may have little or no discretion when controlling how individual records are disclosed and may only request that the court limit public disclosure of eDiscovery information by placing the information under seal or obligating the other parties to abstain from further disclosure without court permission.

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

eDiscovery does not inherit privacy controls from the vendor. eDiscovery has no persistent interconnection; therefore, the Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU) does not apply to eDiscovery.

that document.

5. For the user roles in the system:

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc)	Recertification Date
Case Users	80	Thom Verratti, Paul Chalmers	Read-only	09/26/2019
Case Administrators	6	Paul Calmers, Thom Verratti	Read and write	09/26/2019

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.

eDiscovery physical security controls employed to secure the Personally Identifiable Information (PII) in the system include: security guards, identification badges, locked offices and secured facilities.

eDiscovery technical controls employed to secure the PII in the system include: password protection, network firewalls, unique user identification names, encryption and intrusion detection systems.

Administrative security controls employed to secure the PII in the system include: periodic security audits, annual refresher training for security, privacy and records management, encryption of backups containing sensitive data, 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.

PII may become part of the data set as part of collection of all files relevant to the individual cases but is not collected specifically for use in any case.

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.

The data flow within eDiscovery comes from other PBGC systems. The information stored in eDiscovery may be shared with other federal agencies that serve as adjudicative bodies, such as the Equal Employment Opportunity Commission, the Merit Systems Protection Board, and the Federal Labor Relations Authority. It might also be shared with a court. PBGC shares information stored and processed in eDiscovery with the Department of Justice and any outside agency requested to opine on or concur with the disclosure of responsive information during civil proceedings, or any other adjudicative body. The information is not shared externally by the system, but is provided manually, and may include encrypted secure email or delivery of the data on portable storage media or paper.

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

- Yes
- No

### 2.3 Privacy Office Review

<b>Name of Reviewer</b>	Shawn Hartley
<b>Date Reviewed</b>	05/10/2019
<b>Expiration Date</b>	05/10/2020
<b>Result</b>	<input checked="" type="checkbox"/> Approved without conditions <input type="checkbox"/> Approved with conditions (see below). <input type="checkbox"/> Denied

*(For Privacy Office Use Only)*

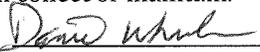
Discuss analysis of risks and compensating controls (or other mitigation steps.

*Enter description here.*

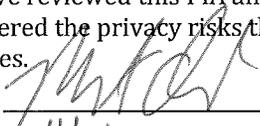
Discuss any conditions on Approval

*Enter description here.*

## 2.4 Signatures and Approval

Information Owner	
Name:	Daniel Wheeler
Dept/Office:	Office of the General Counsel
Phone:	202-326-4000, ext. 6873
Email:	wheeler.daniel@pbgc.gov
I certify that this PIA is an accurate representation of the security and privacy controls in place to protect the PII that the system does/will collect or maintain.	
Signature	
Date signed	4/3/19

Authorizing Official	
Name:	Paul Chalmers
Dept/Office:	Office of the General Counsel
Phone:	202-326-4400, ext. 3555
Email:	chalmers.paul@pbgc.gov
I certify that this PIA is an accurate representation of the security and privacy controls in place to protect the PII that the system does/will collect or maintain.	
Signature	
Date signed	4/3/19

Chief Privacy Officer	
Name:	Margaret Drake
I certify that I have reviewed this PIA and have fully considered the privacy risks that this system creates.	
Signature	
Date signed	4/3/19

***This page is for internal routing purposes of documentation of approvals. Upon final approval, this page must be removed prior to publication of the PIA.***