Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

eDiscovery (RelativityOne Government)

Last Updated: 05/13/2026

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)*
eDiscovery	eDiscovery is an externally hosted litigation support service that provides an environment to support the 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 Procedure.	Yes	PBGC-13, 19	29 U.S.C. §§ 1055, 1056(d)(3), 1302, 1303, 1310, 1321, 1322a, 1341, 1341a, 1342, 1343, 1350; 1431, and 1432; 5 U.S.C. §§ 301, 552(a), 552a(d), 7101; 42 U.S.C. § 2000e, et seq.	Yes

2.2 The System as a Whole

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

The purpose of eDiscovery is to support the mandatory production process, i.e., the collection and legal processing of documents, including agency records, in pending civil litigation. Copies of records are compiled and uploaded to eDiscovery, which then allows legal teams to access copies of records gathered from other PBGC systems for review, analysis, and coding.

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.

This is an existing system and there are currently no changes.

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.)

eDiscovery collects records from other PBGC systems and by manual upload. The nature of those records may vary from case to case. Records in eDiscovery which pertain to First Amendment rights may be processed in relation to litigation, e.g., religious information. 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. Legal

authority is found in 29 U.S.C. §§ 1302, 1303, 1310, 1321, 1322a, 1341, 1341a, 1342, 1343, 1350; 5 U.S.C. §§ 301, 552(a), 552a(d), 7101; 42 U.S.C. § 2000e, et seq..

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.

PII will be contained in the system to support a litigation action and may be necessary to the litigation's nature. The legal team reviews information collected as part of its legal action to ensure it is accurate, complete and timely. Access to the eDiscovery workspace hosting such information is restricted to only the litigation team assigned to the matter. However, in most cases, eDiscovery does not collect personal information directly from individuals but instead receives copies of records obtained from other PBGC systems, manual upload, and third-party sources. Therefore, eDiscovery relies on the PBGC program or entity that originally collected the information to ensure the accuracy and completeness of PII. As discovery usually requires information "relevant" to the legal action, PII included may initially be over-inclusive of the team's needs but can be removed following such a determination. Additionally, PBGC does not use eDiscovery as an authoritative source for PII about individuals or use the tools to alter PII in the original records. Any inaccurate or incomplete information, when identified, can be corrected in the source systems. Following the conclusion of the litigation matter, the related eDiscovery workspace is completely removed from the system (all of its information, attorney tagging, and history, including all related PII) and the system generates a Certificate of Destruction document which is retained by the eDiscovery maintenance team.

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.

Users can utilize the search function using various identifiers, such asname, date of birth, personal phone number(s), or personal email addresses, that are available from the collection to locate records. Though SSNs are sometimes contained in this system, because the system receives copies of records from other PBGC systems it is possible that collected SSNs will be in those records and can be used as identifiers. However, SSNs will be removed from the system in accordance with normal closing procedures for the litigation matter. eDiscovery supports a range of searching needs from filtering on fields and simple keyword searches to the development of complex queries.

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

Variable: each case will have its own information collection requirements.

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.

Neither. 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.

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?

    Because SSNs can be received from other PBGC systems or from litigants and need to be reviewed as part of legal discovery or to resolve a matter handled by OGC, documents in eDiscovery may contain them. However, eDiscovery, as a system, does not collect SSNs.

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

    NA

    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.

    NA

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.

eDiscovery may collect information from other PBGC systems and this information might contain PII, in its original format at the time of collection. The nature of those records may vary from case to case, but some examples include financial records, medical records, and employment records. Additionally, 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 and may also be manually uploaded to the system.

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 involves other actors (e.g., opposing counsel, litigants, witnesses), 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.

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.

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) do not apply to eDiscovery.

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 JCAM. Be sure to include any MOU, ISA, or Interagency Agreements.

PBGC may need to produce and share eDiscovery documents with courts, opposing counsel, defendants, or other entities or individuals as authorized or required by law. When a set of documents is produced by eDiscovery to be shared with any external entity, the security rules for the system state that these new documents must be imported into a PBGC system and become new records in that system of records.

14. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	ICAM Reporting Date
Reviewer	32	Daniel Wheeler or Thom Verratti	Read workspace that they have access to, and code documents associated with workspaces	05/01/2026
Maintenance	12	Daniel Wheeler or Thom Verratti	Read all workspaces and access to the SFTP server	05/01/2026

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	ICAM Reporting Date
(Advanced Privilege accounts/ Cyberark)	2	Daniel Wheeler	Can access prda-relativityone-admin safe to perform user provisioning activities	05/01/2026

15. 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.

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

No additional training

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).

PBGC maintains data in eDiscovery for the duration of the legal matter. The law or ruling also establishes the retention guidelines. PBGC also retains the records in eDiscovery in accordance with PBGC Records Retention Schedules and follows guidance on permanent and temporary records disposition issued by the National Archives and Records Administration (NARA). OGC certifies when records can be destroyed. However, due to business rules and storage limits within eDiscovery, the records that are uploaded to and processed may be deleted from the system after processing and production, and retained for the requisite amount of time elsewhere. Occasionally, there will be times when records are kept in eDiscovery, due to ongoing litigation. To ensure that storage limits are not reached, users receive periodic housekeeping notices to review any maintained files and delete those no longer needed.

2.3 Privacy Office Review

Name of Reviewer	Zoe Wadge
Date Reviewed	5/12/2026
Expiration Date	5/12/2027
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
