Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Electronic Complaints and Tracking System (eCATS) Privacy Impact Assessment (PIA)

Last Updated: 3/25/2024

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)*
Entellitrak	Entellitrak is a platform which allows OEEO to track, manage resolution, and report on discrimination complaints at PBGC effectively and efficiently for both informal and formal complaints.	Yes	EEOC/GOVT-1 Equal Employment Opportunity in the Federal Government Complaint and Appeal Records	5 U.S.C. 301; 29 U.S.C. 211, 29 U.S.C. 623, 29 U.S.C. 626; 42 U.S.C. 2000e–16 (b) and (c); 44 U.S.C. 3101.	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).

The Office of Equal Employment Opportunity (OEEO) supports the Pension Benefit Guaranty Corporation's (PBGC) goal of integrating EEO requirements (Title 29 C.F.R. Part 1614) with PBGC's work environment, strategic missions, and corporate initiatives; and developing and maintaining a diverse, discrimination-free work environment. This includes an annual review and analysis of multiple areas, including the following:

•Management and program accountability

•Proactive prevention of discrimination

•Providing regulatory and reporting requirements

•Recommendations and plans for improving the EEO program

•Pursuit of a model EEO program

The OEEO oversees PBGC's Affirmative Employment and EEO Complaints Process using the OEEO Electronic Complaint and Tracking System (eCATS).

The eCATS application is a web-based solution that runs on the Entellitrak platform, which allows OEEO to track, manage resolution, and report on discrimination complaints at PBGC effectively and efficiently for both informal and formal complaints. The application is a Software as a Service (SaaS) hosted by Tyler Federal.

eCATS uses both Personally Identifiable Information (PII) and non-PII data to record, track, and manage OEEO complaints filed against PBGC. These complaints are recorded, investigated, and can be submitted either formally or informally. Access to eCATS is limited to those who need to know the information to perform job functions based on pre-defined user roles and permissions.

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 sources from which the system collects PII consist of an individual and/or other federal agency. The formats in which PII is collected are paper/written form, face-to-face, and via email. The formal complaint of DiscriminationPAS form includes the Privacy Act statement below:
Privacy Act Statement
***AUTHORITY**: 42 U.S.C. § 2000e-16; 29 U.S.C. § 1302; 29 C.F.R. § 1614*
***PURPOSE**: To provide counseling, conduct investigations, process and adjudicate complaints of alleged violations of employment discrimination and related appeals brought by applicants and current and former PBGC employees.*
***ROUTINE USES:** PBGC may disclose information to any individual who may be required by regulation, policy, or procedure of the EEOC to provide information in connection with this complaint, including individuals who may be identified as responsible for the alleged acts or events at issue and potential witnesses as appropriate and necessary. PBGC may also disclose this form or information from this form to any individual engaged by PBGC to carry out the agency's responsibilities required by regulation, policy, or procedure of the EEOC. Other disclosures may be: (1) to appropriate federal, state, or local agencies when related to a violation or potential violation of civil or criminal law or regulation; (2) to a federal agency, a court, or a party in litigation before a court, or in an administrative proceeding being conducted by a federal agency, when the U.S. Government is a party to the judicial or administrative proceeding; (3) to a congressional office from the record of an individual in response to an inquiry made at the request of the individual; or (4) in response to a request for discovery or for appearance of a witness when the information is relevant to the subject matter involved in a pending judicial or administrative proceeding.*
***DISCLOSURES:** Providing information on this form is voluntary; however, failure to provide the information may delay or prevent PBGC from processing your complaint.*

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.

There are no privacy controls that PBGC inherits from the external provider. An Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU) are not applicable.

5. For the user roles in the system:

Role Name	Number of Users in that Role (AD)	Approver	Access Level (Read, Write, etc.)	Recertification Date
Administrator	1	Dianne Wood	Read/Write	09/06/2023
Informal Processor	3	Dianne Wood	Read/Write	09/06/2023
Formal Processor	2	Dianne Wood	Read/Write	09/06/2023
Super Processor	3	Dianne Wood	Read/Write	09/06/2023
Master Admin	1	Dianne Wood	Read/Write	09/06/2023

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 Controls:

eCATS leverages Tyler Federal physical security controls employed to secure the PII in the system. These controls include security guards, key entry, and secured facility.

Technical Controls:

eCATS leverages Tyler Federal technical security controls employed to secure the PII in the system. These controls include password protection, configuration management, contingency planning, audit logging, firewalls, unique user identification names, encryption, intrusion detection systems, and vulnerability scanning.

PBGC is responsible for reviewing and approving PBGC user access requests and performing annual user account recertifications.

Administrative Security Controls:

eCATS fully leverages Tyler Federal incident response controls to secure the PII in the system. Awareness and Training, Incident Response, Personnel Security, Planning, Security Assessment and Authorization (SA&A) controls are hybrid between OEEO and Tyler Federal. For example, OEEO conducts annual SA&A process and reviews Tyler Federal's' SA&A package on FedRAMP marketplace at least annually.

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 information collected is used to properly administer and adjudicate EEO complaints. The type and frequency of correspondence is mandated by EEOC regulations according to 29 C.F.R. § 1614.
Any legal documents that may contain PII are maintained as part of a case file in accordance with EEOC regulations.
Data collected for use by eCATS is limited to that which is authorized under 29 C.F.R § 1614. eCATS may also aggregate data to show trends, whether the information is an aggregate of data, fiscal year data, or benchmark data.
Without the requested PII, the OEEO would be unable to process the EEO complaint. Additionally, eCATS may also use the aggregated data to meet regulatory mandates.

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.

None of the PII sharing is through the eCATS system and the internal or external sharing is performed manually. Therefore, an ISA is not required.

1.Within PBGC: Case information is shared with Office of General Counsel (OGC) when they defend the agency in EEO matters. The information is shared via electronic LeapFile. LeapFile is a PBGC-approved method of sending large files >10kb.

2.With other Federal agencies: PII can be shared with the EEOC, Merit Systems Protection Board, U.S. Department of Justice, and a court of competent jurisdiction. The information is shared several ways. Some recipients may receive a hard copy via FedEx, files may be sent electronically to the EEOC via the EEOC's secure FEDSEP portal, or files may be sent via encrypted email.

3.With contractors: Contractor investigators are provided with the necessary documents to prepare for the investigation, which may contain PII. Additionally, they collect PII from the complainant and witnesses during the investigation. The information is shared via encrypted email.

4.With other third parties: PII may be shared with outside counsel and the Independent Union of Pension Employees for Democracy and Justice (IUPEDJ). When outside counsel or IUPEDJ represent a complainant, they would receive the Report of Investigation (ROI), which may contain PII via hand delivered hard copy and/or provided via FedEx.

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?

Not Applicable. eCATS 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?

Not Applicable. eCATS does not collect SSNs

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. eCATS does not collect SSNs

2.3 Privacy Office Review

Name of Reviewer	Bill Black
Date Reviewed	3/28/2024
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.