Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)

Electronic Complaints and Tracking System (eCATS)

12/11/2020

1 Privacy Point of Contact

Name	Dianne Wood
Title	Information Owner
Phone	202-229-3307
Email	Wood.Dianne@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)*
eCATS	eCATS is a web-based service hosted by a Federal Risk and Authorization Management Program (FedRAMP) provider which facilitates the Equal Employment Opportunity (EEO) complaint process for PBGC.	Yes	EEOC/GOVT-1 SORN	5 U.S.C. 301; 29 U.S.C. 209, 211, 623, 626; 42 U.S.C. 2000e–16c; 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 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 Technologies, a web-based Commercial off-the-Shelf (COTS) software tool. Tyler Technologies (formerly MicroPact) cloud-hosting environment has been granted a Federal Risk and Authorization Management Program (FedRAMP)-compliant Authorization to Operate (ATO) as a Platform as a Service (PaaS) and Software as a Service (SaaS) public cloud provider at the "Moderate" impact level. PBGC leverages this service.

The 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. If an individual asks that PBGC address an EEO-related question or concern without using the formal complaint process, PBGC enters the issue information into eCATS along with any PII needed to track it. PBGC must also track and investigate all accepted formal EEO complaints within 180 days. An individual's PII may be entered into eCATS when he or she initiates a formal or informal EEO complaint, witnesses an alleged discriminatory act, or is named as committing an alleged discriminatory act. PBGC uses PII only as needed to

investigate complaints, and is authorized to collect this information by Title 29, Code of Federal Regulations, Section 1614, Part A.

eCATS aggregates data in order to show trends, whether the information is an aggregate of data, fiscal year data, or benchmark data. The aggregated data is used in Management Directive annual reports and Notification and Federal Employee Anti-Discrimination Retaliation Act of 2002 (No-FEAR) quarterly and annual reports to Equal Employment Opportunity Commission (EEOC) and/or Congress and/or posted on PBGC.gov. In addition, PBGC uses these systems to provide quarterly and annual status reports pursuant to the Notification and Federal Employee Antidiscrimination and Retaliation (No-FEAR) Act.

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 agencies.

The formats in which PII is collected are paper/written form, face-to-face, and via email. See attached forms and Privacy Act Statements.

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	Approver	Access Level (Read, Write, etc.)	Recertification Date
Administrator	1	Dianne Wood	Read/Write	12/4/2020
Informal Processor	4	Dianne Wood	Read/Write	12/4/2020
Formal Processor	2	Dianne Wood	Read/Write	12/4/2020
Administrator	4	Dianne Wood	Read/Write	12/4/2020
Super Processor	9	Dianne Wood	Read/Write	12/4/2020
Master Administrator	6	Dianne Wood	Read/Write	12/4/2020
Product Administrator	1	Dianne Wood	Read/Write	12/4/2020

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 Controls:

eCATS leverages Tyler Technologies 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 Technologies 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 Technologies' 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 Technologies. For example, OEEO conducts annual SA&A process and reviews Tyler Technologies' 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 in order to show trends, whether the information is an aggregate of data, fiscal year data, or benchmark data.

Without the requested PII, the EEOC 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 the data interconnections are noted in CSAM. Be sure to include any MOU, ISA, or Interagency Agreements.

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 CD.
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 or electronic via FedEx, files may be sent electronically to the EEOC via the EEOC's secure EFX portal, or files may be sent via encrypted email.
3. With contractors: Contractor investigators are provided 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 electronic copy and/or provided via FedEx.

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, General Attorney
Date Reviewed	12/11/2020
Expiration Date	12/11/2021
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.