Electronic Complaint and Tracking System

(eCATS)

Privacy Impact Assessment PIA Executive Summary

I. BACKGROUND

Federal agencies are required by law to ensure the protection of the personally identifiable information (PII) they collect, store, and transmit. The Pension Benefit Guaranty Corporation (PBGC) is responsible for ensuring proper protections of the information contained within its information systems, including PII. To that end, PBGC developed a Privacy Impact Assessment (PIA) to evaluate whether a system that contains PII meets legal privacy requirements.

II. PURPOSE AND SCOPE

- Purpose

PBGC is responsible for ensuring the confidentiality, and integrity of the information contained within eCATS. A PIA is used to evaluate privacy vulnerabilities and risks to PII and their implications regarding eCATS.

The PIA provides a number of benefits to the Office of Equal Employment Opportunity and Diversity (EEOD) to manage and report on the overall Equal Employment Opportunity (EEO) program, including enhancing policy decision-making and system design, anticipating the public's possible privacy concerns, and generating confidence that privacy objectives are addressed in the development and implementation of eCATS. The PIA Questionnaire provides a framework by which agencies can ensure that they have complied with all relevant privacy policies, regulations, and guidance, both internal and external to PBGC.

eCATS assists the EEOD to manage and report on the overall EEO program. This includes monitoring and reporting in an efficient and effective manner on informal and formal complaints of discrimination. eCATS consists of Micropact's Icomplaints software and is hosted by Micropact.

- Scope

A Privacy Impact Assessment was conducted on eCATS. The system is a custom-developed application that is owned and operated by Micropact on behalf of PBGC. The eCATS system is located at 1200 K Street NW, Washington, DC and Wilmington, DE, and is accessed by both PBGC and its support contractors in the course of their jobs. It is listed as a Major Application on the PBGC FISMA Information Systems Inventory Report, and its security needs are consistent with those of PBGC.

III. PIA APPROACH

A questionnaire was developed in accordance with the FIPS 199 - Standards for Security Categorization of Federal Information and Information Systems, Office of Management and Budget (OMB) requirements, Section 208 of the E-Government Act of 2002, The National Institute of Standard and Technology (NIST) recommendations, and the Federal Enterprise Architecture Business Reference Model (BRM). The questionnaire was developed in order to identify any PII.

The questionnaire was given to the Information System Owner (ISO) and the Information System Security Officer (ISSO) of eCATS for their response. An Information Security Analyst from PBGC's Enterprise Information Security Office (EISO) along with a member of the PBGC Privacy Office reviewed the IOS and ISSO responses to the questionnaire. Responses form the ISO and the ISSO of eCATS were used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

Icomplaints is an application that is owned and operated by Micropact on behalf of PBGC. Authorized PBGC users connect to Icomplaints at the Micropact facility Herndon, VA. eCATS is used by PBGC to track and process both informal and formal EEO complaints. Only authorized EEOD personnel have access to eCATS. PBGC must also track and respond to all formal EEO complaints and process formal complaints within regulatory timeframes established in 29 CFR 1614. In addition, PBGC must file EEOC Form 462 Annual Federal Equal Employment Opportunity Statistical Reports annually, and provide quarterly and annual reports in compliance with the Notification and Federal Employee Antidiscrimination and Retaliation Act of 2002.

V. PIA RESULTS

The PIA evaluation revealed that eCATS contains PII due to statutory requirements. Only those who are authorized to use the application have access to it and the information contained therein. The users are utilizing the information for the sole purpose of performing their assigned duties.

The primary privacy risk identified is a potential data breach and subsequent loss or unauthorized disclosure of PII. The risk of a data breach is mitigated by security controls implemented and documented for eCATS. These controls are in accordance with those recommended by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 3 for a moderate risk system in accordance with Federal Information Processing Standards (FIPS) 199 evaluation. Based on the analysis performed here, no discrepancies have been discovered.