Premium Accounting System
(PAS)
Privacy Impact Assessment (PIA) Executive Summary

I. BACKGROUND

Federal agencies are required 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, integrity, and availability of the information contained within the Premium Accounting System (PAS). A PIA is used to evaluate privacy vulnerabilities and risks and their implications on PAS. The PIA provides a number of benefits to PBGC; 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 PAS. 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.

- Scope

A Privacy Impact Assessment was conducted on the PAS system. PAS is PBGC owned by PBGC's Financial Operations Department. The PAS system is located at 1200 K Street NW, Washington, DC and Wilmington, DE, and is accessed by both PBGC and a select group of support contractors in the course of their jobs. PAS is listed as a Major Application on the PBGC FISMA Information Systems Inventory 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 Information System Security Officer (ISSO) of PAS 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 ISO and ISSO responses to the questionnaire. Responses from the ISO and the ISSO of PAS were used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

The Premium Accounting System (PAS) is PBGC's revenue system; records defined benefit plan premium receipts, generates late notices, premium billings, and calculates applicable penalties and interest for late payments. PAS is a client-server application designed to process filing information, and to calculate the premium, interest, and penalty revenue due from each pension plan. It also applies the cash received from each plan against amounts due to PBGC, generates plan specific Statement of Accounts (SOAs) for unpaid premiums, interest, and penalties. It also generates Past Due Filing Notices (PDFNs) to be sent to those plan administrators who fail to file. Most of the filings are electronically submitted via PBGC's premium e-filing application called My Plan Administration Account (My PAA). Payments can be made via paper check sent to our lockbox bank, electronic funds transfer outside of My PAA, or submitted via My PAA (electronic funds transfer). My PAA then forwards the filings/payments to PAS.

V. PIA RESULTS

The PIA evaluation revealed that PAS contains PII due to its standard use to record define benefit plan premium receipts, generate late notices and premium billings and calculates applicable penalties and interest for late payments. Only those who support and/or use the components that make up PAS are authorized to access these components and any data residing thereon.

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 PAS. These controls are in accordance with those recommended by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 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.