My Plan Administration Account
(My PAA)
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 My Plan Administration Account (My PAA). A PIA is used to evaluate privacy vulnerabilities and risks and their implications on My PAA. 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 My PAA. 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 My PAA. My PAA is PBGC owned by PBGC's Financial Operations Department. My PAA 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. My PAA 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 My PAA 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 My PAA were used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

My PAA is PBGC's front-end application to the Premium Accounting System and transfers the data to the Premium Accounting System for processing. Plan sponsors and administrators of covered pension plans are required to file and pay premiums to PBGC under ERISA §4006 and 4007, 29. U.S.C. §1306 and 1307. My PAA enables the practitioner to electronically submit all PBGC premium filings for plan years commencing in 2004 and later. My PAA offers alternative methods for electronic filing, which saves time and reduces the risk of errors. My PAA account information is collected and used to authenticate user access, grant specific permissions, or abilities within the online application, and to monitor access controls. PBGC uses the information to accurately record defined benefit plan premium receipts, generates late notices and premium billings, and calculates applicable penalties and interest for late payments. PBGC also uses the information to communicate with the pension plans and their administrators, sponsors, actuaries, and contacts to issue past due filing notices, statements of account, and correspondence.

V. PIA RESULTS

The PIA evaluation revealed that My PAA contains PII due to the insurance premiums paid by insured pension plans, from investment income and from recoveries in bankruptcy. Only those who support and/or use the components that make up My PAA 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 My PAA. 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.