



Protecting America's Pensions

Pension Benefit Guaranty Corporation
MyPAA
Privacy Impact Assessment

Version 1.0

March 2007

Prepared by:

PBGC Office of Information Technology (OIT)
Enterprise Information Security Office (EISO)
1200 K Street NW
Washington, DC 20005

Executive Summary Report

I. INTRODUCTION

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, integrity, and availability of the information contained within its My Plan Administrator Account (MyPAA) system. A PIA is used to evaluate privacy vulnerabilities and risks and their implications on MyPAA. The PIA provides a number of benefits to the Benefit Administration Payment Division (BAPD); 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 MyPAA. 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 MyPAA application. MyPAA is cited on the PBGC Sensitive System List and reported on either the PBGC's Exhibit 53 or via capital asset plans and business cases (Exhibit 300s). It is also listed as a Major Application on the Information Systems Inventory Report. The system is a distributed-tiered web major application that is owned by 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, The Privacy Impact Act of 1975, 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 Personal Identifiable Information (PII).

The questionnaire was given to the Information System Owner (ISO) and Subject Matter Expert (SME) of the MyPAA application for their response. An Information Security Analyst from the TechGuard Security, LLC and the Enterprise Information Security Office (EISO) staff met with the ISO and SME of the MyPAA to discuss the questionnaire. Responses from the ISO and the SME of MyPAA were obtained and used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

MyPAA is a Web-based PBGC application that enables pension plan practitioners to submit premium filings electronically. MyPAA was developed as a .NET system that utilizes XML, SOAP, and Web services with a presentation tier, business logic tier, and data tier.

V. PIA RESULTS

The PIA evaluation revealed that the MyPAA application contains a PII and 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. No discrepancies have been discovered.

VI. SUMMARY

MyPAA contains PII in secure online databases. Security is consistent and the servers where the applications and data are stored are physically secured and password protected. Only staff authorized to use the application have access to it and the information contained therein. Staff utilizes the information for the sole purpose of performing their assigned duties. Further information can be requested by contracting PBGC's Disclosure Officer.