Risk Management Early Warning
(RMEW)

Privacy Impact Assessment (PIA) 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, integrity, and availability of the information contained within the Risk Management Early Warning (RMEW) system. A PIA is used to evaluate privacy vulnerabilities and the associated risk implications with RMEW. The PIA provides a number of benefits to PBGC; including enhancing policy 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 RMEW. 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 RMEW system. RMEW is a customized COTS application that is owned by PBGC. RMEW is comprised of three components which are used in the course to request actuarial work, store documents relating to plan sponsor and plan terminations. The RMEW 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. RMEW is listed as a Major Application on the PBGC's Federal Information Security Management Act (FISMA) 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, as amended, 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 RMEW for their response. An Information Security Analyst from PBGC's Enterprise Cybersecurity Division (ECD) 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 RMEW were used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

RMEW provides an integrated legal, financial, and actuarial case management capability and integrated document management system, and workflows for obtaining concurrence on significant recommendations presented by the departments within Office of Negotiations and Restructuring. RMEW consist of an application built on TeamConnect for Legal matters which is supported by the Document Management System.

V. PIA RESULTS

RMEW does not directly collect PII, although PII is often inherited during the course of PBGC functions. RMEW contains data on PBGC-insured pension plans (both single-employer and multiemployer), as well as data on plan sponsors such as reportable event filings, distress termination filings, bankruptcy filings, and other information on other types of pre-termination investigations conducted by PBGC. Only those who use 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 RMEW. 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.