Human Resource Management System
(HRMS)
Privacy Impact Assessment (PIA) 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 Human Resource Management System (HRMS). A PIA is used to evaluate privacy vulnerabilities and risks and their implications on HRMS. 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 HRMS. 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 PIA was conducted on the HRMS system. The HRMS system is managed and operated by the Department of Interior - Interior Business Center (IBC). The HRMS system is accessed by federal employees and contractors with federal oversight. The HRMS system security requirements are consistent with the PBGC security requirements and standards.

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 Owner (IO) and Information System Security Officer (ISSO) of PLUS 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 IO and ISSO responses to the questionnaire. Responses from the IO and the ISSO of PLUS were used to complete the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

The Human Resource Management System (HRMS) system combines a number of subsystems and components into one managed authorization boundary. Although all of these subsystems and components could be viewed individually, it is more effective and efficient to combine them into one since they are owned and hosted by one third-party agency, Department of Interior – IBC, and managed by PBGC's Human Resource Department.

IBC offers a diverse, yet integrated, set of administrative solutions, and is currently the only federal agency designated by both the Office of Management and Budget, and Office of Personnel Management as a financial management and human resources line of business.

V. PIA RESULTS

The PIA evaluation revealed that the HRMS system contains PII due to the collection, storage and processing of PBGC personnel information. Only those who use HRMS are authorized to access it 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 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.