Corporate Data Management System
(CDMS)

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

CDMS is the PBGC's corporate data management system. CDMS stores data from major information systems for a variety of uses across the corporation, including reporting and analysis. Data is captured from core business systems to a decision support environment. PBGC initially developed CDMS to reduce the impact of data requests on major operational systems, thereby easing the burden on main systems during core hours of operations. A PIA is used to evaluate privacy vulnerabilities and risks and their implications on CDMS.

The PIA provides a number of benefits to the Budget and Organizational Performance Department. 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 CDMS system. The CDMS is PBGC owned and Contractor operated with oversight by Federal personnel. The CDMS is comprised of three components: portal, Web server, and database. The CDMS system is located at 1200 K Street NW, Washington, DC and is accessed by both PBGC and its support contractors in the course of their jobs. CDMS 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 Personally Identifiable Information (PII).

The questionnaire was given to the Information System Owner (ISO) and Information System Security Officer (ISSO) of the CDMS 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 CDMS were obtained and used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

The Corporate Data Management System, (CDMS) stores data from major information systems for a variety of uses across the corporation, including reporting and analysis. Data is captured from core business systems, to a decision support environment. CDMS is comprised of three major components: a portal, Web server, and database. The CDMS portal interacts with Oracle Forms and launches Oracle Report to provide the information requested by the user. The Web server runs the Oracle Forms and Reports and interacts with other CDMS components. The CDMS database retrieves the information requested from the major operational systems. PII is populated from the major operational systems.

V. PIA RESULTS

The PIA evaluation revealed that CDMS contains PII due to its function as a data warehouse for PBGC. The PII is populated by the systems CMS, eALG, Genesis, and PAS for pension plan retirees and participants as well as limited PII of plan sponsors. Only those who are approved by the system owner and pass all ELAN documentation requirements are authorized to access the components that apply to their job functions.

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 the CDMS. These controls are in accordance with those recommended by the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53 revision 3 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.