

# Consolidated Financial Systems (CFS)

## Privacy Impact Assessment (PIA) Executive Summary

### I. BACKGROUND

Federal agencies are required to ensure the protection of 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 Consolidated Financial Systems (CFS). A PIA is used to evaluate privacy vulnerabilities and risks and their implications on CFS. 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 CFS. 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 CFS which is owned by PBGC, Financial Operations Department. The CFS is located at 1200 K Street NW, Washington, DC and Philadelphia, PA, and are accessed by both PBGC and its support contractors in the course of their jobs. CFS 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 CFS Information System Owner (ISO) and Information System Security Privacy Officer (ISSPO) 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 CFS ISO and the ISSO were used to fill in the final PIA and analysis.

#### **IV. SYSTEM CHARACTERIZATION**

The CFS addresses the PBGC's budgetary, fiscal, financial, management, and reporting needs for the enterprise revolving fund, trust accounting, and consolidated financial operations. The CFS integrates three logical general ledgers; three modules (Accounts Payable, Purchasing, & Fed Admin (Funds Control)); and their related interfaces into one web-based application, also known as Oracle Federal Financials.

#### **V. PIA RESULTS**

The PIA evaluation revealed that CFS contains PII due to the collection; storage and processing of financial data for PBGC to accurately carry out and record PBGC's financial activity. Only those who support and/or use the components that make up CFS 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 CFS. 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.