

# **BAPD Applications Suite (BAS)**

## **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 Benefits Applications Suite (BAS). A PIA is used to evaluate privacy vulnerabilities and risks and their implications on BAS. 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 BAS. 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 BAS system. BAS is PBGC owned and contractor operated with oversight by Federal personnel. BAS is comprised of 5 major components, including client and server applications and a number of utility tools. The BAS systems are located at 1200 K Street NW, Washington, DC and Wilmington, DE, and are accessed by both PBGC and its support contractors in the course of their jobs. BAS is listed as a Major Application on the PBGC 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, 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 BAA 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 BAA used to fill in the final PIA and analysis.

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

The Benefits Administration and Payment Department (BAPD) Application Suite (BAS) system boundary consists of Benefits Administration Applications (BAA), Benefits Calculation Valuation (BCV), eTalk, Integrated Present Value Future Benefits (IPVFB) and MyPBA, and a list of client and server applications, in addition to a list of tools that support these applications. The BAS system supports the BAPD mission, which is to ensure participants are paid their full benefit permitted by law, and to provide quality service through accurate, timely, and uninterrupted benefit payments and administration. This PIA is being documented to address the privacy data managed and hosted by the BAS system.

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

The PIA evaluation revealed that BAA contains PII due to the collection, storage and processing of pension participants and their beneficiaries in order to meet the mission of PBGC in paying appropriate benefits. Only those who support and/or use the components that make up BAA 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 BAA. 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.