Administar Privacy Impact Assessment
Executive Summary Report

I. Background

The Federal Government has recognized both the advantages and risks of using information technology (IT) to serve the public. Members of the public and private-sector organizations interacting with the Federal Government must be assured that their sensitive personal information is protected. In order to protect the privacy of personal information held by Federal IT systems, the Federal Government requires Federal agencies to comply with requirements established by public laws, regulations and Executive Orders including the E-Government Act of 1996 (HIPAA). One of the key requirements for managing privacy risk is the privacy impact assessment (PIA).

The Pension Benefit Guaranty Corporation (PBGC) is responsible for providing proper protections for the information contained within its information systems, including personally identifiable information (PII). The Financial and PII in the Administar Application demands an increased level of attention to security and privacy from PBGC. This IT PIA uses guidelines established by PBGC's Enterprise Information Security Information Assurance Handbook (IAH) – Volume 4: Privacy Impact Methodology and Assessment.

II. Purpose and Scope

- *<u>Purpose</u> – Administar is part of the Remedy suite which supports the Page/Collins Settlement.*
- *<u>Scope</u> – The Administar MA data consists of name, mailing address, Social Security Numbers and personal financial information. Both the Administar Server and the Administar Workstations reside at PBGC's headquarters at 1200 K Street, NW, Washington, DC. . The users consist of Contractors supporting data entry, Federal staff review and approval and Contractor System Administrators (SA). The traditional SAs who manage the other Windows systems at PBGC do not manage the Administar server.*

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, The Privacy Act of 1974, 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 Personal Identifiable Information (PII).

The questionnaire was given to the Information System Owner (ISO) and Subject Matter Expert (SME) of the Ariel application for their response. An Information Security Analyst from the TechGuard Security, LLC met with the ISO and SME of the Ariel to discuss the questionnaire. Responses from the ISO and the SME of Ariel were obtained and used to fill in the final PIA and analysis.

IV. System Characterization by ASSERT

All communication between the Administar Server and the workstations occurs over the Administar's private LAN. This LAN is a switch located at 1200 K Street building. Administar is a stand alone system and is not connected to the PBGC network. The system cannot access the internet or any other internal PBGC systems, either directly or indirectly. All information that is imported into the system must either be imported through the use of approved portable media or input manually.

V. PIA Results

The PIA evaluation revealed that the Administar Application contains PII and only those who are authorized to use the application have access to it and information contained therein. The users are utilizing the information for the sole purpose of performing their assigned duties. Only the users explicitly authorized to use Administar have access to the application.

VI. Summary

The system is not part of the PBGC LAN or WAN, but it does contain PII information about participants who receive benefits from the Page/Collins settlement. If this information was disclosed to the public it could result in negative publicity for PBGC. If this information was disclosed to unauthorized parties it could also lead to financial penalties for PBGC.