



Pension Benefit Guaranty Corporation

BCA - Ariel Privacy Impact Assessment

Version 1.0

March 2007

Prepared by:

PBGC Office of Information Technology (OIT)
Enterprise Information Security Office (EISO)
1200 K Street NW
Washington, DC 20005

Executive Summary Report

I. INTRODUCTION

Federal agencies are required by law 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 its Benefit Calculation Applications- Ariel (BCA-Ariel) system. A PIA is used to evaluate privacy vulnerabilities and risks and their implications on BCA-ARIEL.

The PIA provides a number of benefits to Office of the Benefit Administration Payment Division (BAPD); 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 BCA-Ariel. 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: BCA-Ariel is cited on the PBGC Sensitive System List and reported via capital asset plans and business cases (Exhibit 300s). A Privacy Impact Assessment was conducted on the BCA-Ariel application. It is also listed as a Major Application on the Information Systems Inventory Report. The BCA-Ariel is used for the valuation support of the terminated pension plans and the calculation of benefits due plan participants and their beneficiaries.

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 Impact Act of 1975, 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 BCA-Ariel application for their response. An Information Security Analyst from the TechGuard Security, LLC and the Enterprise Information Security Office (EISO) staff met with the ISO and SME of the BCA-Ariel to discuss the questionnaire. Responses from the ISO and the SME of BCA-Ariel were obtained and used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

The system is physically housed by Morneau Sobeco located in downtown Montreal. ARIEL and the Citrix applications used to access ARIEL are run on Intel based systems using Microsoft Windows 2000. These systems have RAID disk arrays. Windows password authentication, NTFS and Windows Domains using trust relationships are used to protect the data. These systems also run Symantec Antivirus Corporate version 8.0 and Veritas backup software. Morneau Sobeco systems are connected to a LAN which connects to the Corporate WAN. Internet access is also available with firewalls between the corporate network and any Internet access points.

V. PIA RESULTS

The PIA evaluation revealed that the BCA-Ariel application contains PII and only those who are authorized to use the application have access to it and the information contained therein. The users are utilizing the information for the sole purpose of performing their assigned duties. No discrepancies have been discovered.

VI. SUMMARY

BCA contains PII in secure online databases. Security is consistent and the servers where the applications and data are stored are physically secured and password protected. Only staff who are authorized to use the application have access to it and the information contained therein. Staff utilizes the information for the sole purpose of performing their assigned duties. Further information can be requested by contracting PBGC's Disclosure Officer.