Client Interface General Support System (CIGSS)

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**

PBGC is responsible for ensuring the confidentiality, integrity, and availability of the information contained within the Client Interface General Support System (CIGSS). A PIA is used to evaluate privacy vulnerabilities and risks and their implications on the CIGSS.

The PIA provides a number of benefits to the Office of Information Technology (OIT); 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 CIGSS. 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 CIGSS system. The CIGSS is PBGC owned and Contractor operated with oversight by Federal personnel. The CIGSS functions predominantly as the internal facing portion of the infrastructure. It is comprised of internal systems and devices, i.e. switches/routers, servers, desktops, and databases that handle the flow and support the processing of data internal to the PBGC network. The communications infrastructure is an enterprise network providing connectivity between and within PBGC Headquarters in Washington, DC, the Kingstowne, VA alternate work site, the Wilmington, DE Continuity of Operations (COOP) site, 6 Field Benefit Administrator (FBA) sites, 5 Actuarial sites, and the ASCGSS. CIGSS is listed as a General Support System (GSS) on the Information Systems Inventory Report, 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 CIGSS for their response. An Information Security Analyst from PBGC's Enterprise Information Security Office (EISO) met with the ISO and ISSO of the CIGSS to discuss the questionnaire. Responses from the ISO and the ISSO of CIGSS were obtained and used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

The CIGSS hardware is physically housed in each Local Area Network (LAN) location throughout the United States. These locations would include PBGC Headquarters, Washington, DC, Kingstowne, VA, Wilmington, DE, six Field Benefit Administrator (FBA) offices, two Post Valuation Administration (PVA) offices, and four Actuarial and Fulfillment sites. All LAN locations would be supported through the Data Center in PBGC Headquarters. None of these facilities is open to the public.

The CIGSS controls access to PBGC systems and data which is collected by providing specific protections for all data transmitted, stored, or processed within the system boundary of the internal PBGC network. It is comprised of internal systems and devices, i.e. switches/routers, servers, desktops, and databases that handle the flow and support the processing of data internal to the PBGC network. These systems allow the end users at PBGC to access and perform different business functionalities, and integrate with custom applications and data sources. CIGSS does not connect to any external systems.

As a GSS, the CIGSS does not directly collect PII from any parties. It contains servers that may store and/or process information, including SSNs and other PII, in support of PBGC major information systems/applications. The CIGSS may, as the result of extracts from the major applications result in spreadsheets, word processing documents, and images containing PII that would then be saved onto a file system within the GSS system boundary. PBGC major applications further define the types of data collected and its uses for that specific business processing to meet the PBGC mission.

V. PIA RESULTS

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 CIGSS. 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. The PIA evaluation revealed that the CIGSS contains PII due to data being transmitted, processed, or stored by PBGC major application and/or systems within the system boundary of the internal PBGC network. Only those who support the components that make up the CIGSS are authorized to access these components and any data residing thereon, such as network and database administrators. Based on the analysis performed here, no discrepancies have been discovered.