Agency Security Controls General Support System (ASCGSS)

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

- <u>Purpose</u>

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

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 ASCGSS. 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.

- <u>Scope</u>

A Privacy Impact Assessment was conducted on the ASCGSS system. The ASCGSS is PBGC owned and Contractor operated with oversight by Federal personnel. The ASCGSS is comprised of the perimeter systems and devices (e.g., switches/routers/firewalls, etc.) that present, define, regulate, or monitor data flow between the corporate systems and the external world, including the corporate-wide common controls. The ASCGSS system is located at 1200 K Street NW, Washington, DC and Wilmington, DE, and is accessed by both PBGC and the public. ASCGSS is listed as a General Support System 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 ASCGSS for their response. An Information Security Analyst from PBGC's Enterprise Information Security Office (EISO) met with the ISO and ISSO of the ASCGSS to discuss the questionnaire. Responses from the ISO and the ISSO of ASCGSS were obtained and used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

The ASCGSS hardware is physically housed in the Data Center in PBGC Headquarters. Other hardware is housed in PBGC's Disaster Recovery Facility (DRF). None of these facilities is open to the public.

The ASCGSS controls access to PBGC systems and data which is collected by providing specific protections for all data that traverses the external boundary of the PBGC network. The PBGC enterprise network (ASCGSS) provides connectivity between its Headquarters in Washington DC, the Kingstowne, VA alternate work site, the Wilmington, DE Continuity of Operations (COOP) site, six Field Benefit Administrator (FBA), two Post Valuation Administration (PVA), four Actuarial and Fulfillment sites. Extranet connections to business partners and service providers include but are not limited to JP Morgan, Social Security Administration, Siemens, Bloomberg Data Service, and the Department of the Interior. A complete list of those entities and their respective interconnection agreements are maintained by PBGC and reviewed annually.

The ASCGSS also encompasses servers on which inbound and possibly outbound information may reside for a short period of time until collected by the governing application which may reside in a contractor's environment or within the PBGC network itself and be supported by other general support systems. PBGC major applications or other GSS PIAs further define the types of data collected and its uses for that specific business processing to meet the PBGC mission.

These systems allow the end users at PBGC to access and perform different business functionalities, and integrate with custom applications and data sources.

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 ASCGSS. 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 ASCGSS contains PII due to the transfer of data processed by PBGC major application and/or systems across the external boundary of the PBGC network. Only those who support the components that make up the ASCGSS are authorized to access these components and any data residing thereon, such as network administrators. Based on the analysis performed here, no discrepancies have been discovered.