

# **IT Infrastructure Services General Support System (ITISGSS)**

## **Privacy Impact Assessment (PIA) Summary**

### **I. BACKGROUND**

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 the IT Infrastructure Services General Support System (ITISGSS). A PIA is used to evaluate privacy vulnerabilities and risks and their implications on ITISGSS. The PIA provides a number of benefits to PBGC; including enhancing policy 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 ITISGSS. 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 ITISGSS system. The ITISGSS is PBGC owned and contractor operated with oversight by Federal personnel. The ITISGSS assumes a custodial role over the egress and ingress of the boundaries of PBGC's network. ITISGSS is accessed by both PBGC and the public. ITISGSS is listed as a General Support System on the PBGC FISMA 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 PII.

The questionnaire was given to the Information System Owner (ISO) and Information System Security Officer (ISSO) of the ITISGSS for their response. An Information Security Analyst from PBGC's Enterprise Cybersecurity Division (ECD) met with the ISO and ISSO of the ITISGSS to discuss the questionnaire. Responses from the ISO and the ISSO of ITISGSS were obtained and used to fill in the final PIA and analysis.

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

The ITISGSS is a general support system owned and operated by the Office of Information Technology (OIT) IT Operations Department (OIT/ITIOD).

The ITISGSS provides support in the form of network infrastructure services, database platform services, remote access services, backup data services, data storage services, messaging services, security services, change and configuration management services, network identification and authentication services, operating system platform services, web platform services, program and project management support services, and address validation services. These services may store and/or process information, including Social Security Numbers (SSNs) and other PII, in support of PBGC major information systems/applications. This includes information processed internally and through the ingress/egress of information through interconnections with external organizations.

Information transactions vary per PBGC major information system/application. Descriptions of application-based transactions occurring within the ITISGSS system boundary are documented in the PBGC major information systems/applications respective PIA.

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

The PIA evaluation revealed that the system 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 ITISGSS 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.

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 ITISGSS. 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.