EDSGSS Privacy Impact Assessment

Executive Summary

08/03/2010

PBGC

Protecting America's Pensions

Table of Contents

1   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.

1.1   Purpose

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

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 EDSGSS. 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.

1.2   Scope

A Privacy Impact Assessment was conducted on the EDSGSS system. The EDSGSS is PBGC owned and Contractor opertated. The EDSGSS provides the direct support in housing the Corporation's core Oracle based databases and supporting Oracle middle tier infrastructure. The EDSGSS system is located at 1200 K Street NW, Washington, DC and Wilmington, DE, and is accessed by both PBGC and the public. EDSGSS is listed as a General Support System on the Information Systems Inventory Report, and its security needs are consistent with those of PBGC.

2   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 EDSGSS application for their response. An Information Security Analyst from the TechGuard Security, LLC met with the ISO and SME of the EDSGSS to discuss the questionnaire. Responses from the ISO and the SME of EDSGSS were obtained and used to fill in the final PIA and analysis.

2.1   SYSTEM CHARACTERIZATION

The EDGSS 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 EDGSS system is comprised of the following collection of resources:
o   EDGSS are hosted on UNIX and LINUX servers.
o   The Systems are running on Solaris and LINUX Operating Systems.
o   The Systems utilize Oracle Database Server Enterprise Edition. Oracle Database Servers run on the Solaris Operating System.
o   The Systems utilize Oracle Application Server as a Middle Tier framework for running J2EE applications, Web Services, Portal, Business Intelligence, E-Business, and Identity Management. Oracle Application Servers run on Solaris and LINUX Operating Systems.
o   The Systems utilize Oracle Applications E-Business suite releases – Oracle Financials and Customer Relationship Management (CRM). The Oracle E-Business suite servers run on Solaris and LINUX Operating Systems.
o   Oracle Enterprise Manager Gird Control is utilized as the central administrative, management and monitoring framework and tool for EDGSS systems.

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

System data flow is application-specific. Please refer to the Major Business System security plans and documentation for further information.

The system functions and the type of information and processing depend on the user community. Please refer to the Major Business System security plans and documentation for further information.

There are systems that have direct external user, such as MyPBA, and MyPAA. Please refer to the security plans and documentation of these systems for further information.

Additionally, there are direct and indirect connections between the UNIX Solaris servers and external PBGC partners, such as State Street Corporation (SSC), the Social Security Administration (SSA), Morneau Sobeco (Ariel), and the Department of Interior (DOI). These connections are performed with a combination of internet connectivity as well as direct links between 1200 K St. and Wilmington (further referenced below).

The EDSGSS is located at Washington, DC and at Wilmington, Delaware.

Internal users and the system data flow are specific to the major application. Please refer to the specific, applicable major application system security plan (SSP) for documentation and further information.

Remote access to the EDSGSS systems exists through the corporate remote access system, which relies on dual factor authentication for initial access. Please refer to the client interface general support systems security plan for more information.

2.2 PIA RESULTS

The PIA evaluation revealed that the EDSGSS system indirectly contains PII due to housing the corporate Oracle databases which act as the home for the PII entrusted to the PBGC. Only those who are authorized to use the corporate applications have access to it and the information contained therein. Users utilize the information for the sole purpose of performing their assigned duties. No discrepancies have been discovered.

2.3 SUMMARY

During the assessment of EDSGSS, no discrepancies in the handling of the information have been discovered.