Legal Technologies Program

(LTP)

Privacy Impact Assessment (PIA) 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 Office of the General Counsel Legal Technologies Program, (LTP). A PIA is used to evaluate privacy vulnerabilities and risks and their implications on LTP. The PIA provides a number of benefits to PBGC; 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 LTP. 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 LTP system. LTP is a system boundary which includes the Legal Management System, (LMS), the Appeals tracking system (ARTIS), and the read-only legacy Freedom of Information Act and Privacy Act tracking system (eDisclosure). LTP is completely internal to PBGC and used only by authorized personnel of the Office of the General Counsel. The LTP system is located at 1200 K Street NW, Washington, DC and Wilmington, DE, and is accessed by both PBGC and its support contractors in the course of their jobs. LTP is listed as a Major Application on the PBGC Federal Information Security Management Act (FISMA) Systems Inventory 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 LMS for their response. An Information Security Analyst from PBGC's Cybersecurity Division (ECD) along with a member of the PBGC Privacy Office reviewed the ISO and ISSO responses to the questionnaire. Responses from the ISO and the ISSO of LMS were used to fill in the final PIA and analysis.

IV. SYSTEM CHARACTERIZATION

The three information systems within the LTP boundary consist of the following;

- The Legal Management System (LMS) is used by the Legal Divisions to track matters (legal cases), including document management for all documents related to a matter (both documents which are processed by the File Room and documents which are added directly to the matter), the list of associated personnel, key dates for the matter, case facts, and any discovery results.

- ARTIS is used by the Appeals Division to track participant appeals from their initial submission to PBGC through appeal assignment, caseload balancing, case research, final determination, and all correspondence with the appealing party.

- eDisclousre is a legacy system previously used by the Disclosure Division to track Privacy Act requests (PA) and Freedom of Information Act requests (FOIA). In October 2013, eDisclosure was replaced by an interagency shared service (EPA's FOIAonline). The eDisclosure system is now in a read-only state for historical recordkeeping only.

V. PIA RESULTS

The PIA evaluation revealed that LTP contains PII due to its function. Only those who use LTP are authorized to access these components and any data residing thereon.

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 LTP. 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.