

# eDiscovery

## 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 eDiscovery system. A PIA is used to evaluate privacy vulnerabilities and risks and their implications on eDiscovery. 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 eDiscovery. 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 eDiscovery. eDiscovery is an externally hosted product and no technical contractors or contractors from non-legal departments will be provided access to the eDiscovery service. eDiscovery 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) 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 eDiscovery were used to fill in the final PIA and analysis.

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

eDiscovery is an externally hosted service, (Symantec's Clearwell product, hosted by CDS or Complete Discovery Systems). This system is used by all legal divisions of the agency (including the Office of the Chief Counsel and five divisions in the Office of the General Counsel) to perform electronic discovery functions required by law and by the Federal Rules of Civil Procedure. This system holds copies of agency records and allows legal teams to perform analysis, coding, and production functions to meet litigation discovery requirements.

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

The PIA evaluation revealed that eDiscovery contains PII due to its function as an eDiscovery tool. Only those who use eDiscovery 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 eDiscovery. 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.