

RMEW/TeamConnect Privacy Impact Assessment

Executive Summary Report

I. 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.

Purpose

PBGC is responsible for ensuring the confidentiality, integrity, and availability of the information contained within Risk Management Early Warning (RMEW). A PIA is used to evaluate privacy vulnerabilities and the associated risk implications on RMEW.

The PIA provides a number of benefits to Insurance Program Office/Department of Insurance Supervision and Compliance and Office of Chief Council (IPO/DISC-OCC); including enhancing policy decision-making and system design, anticipating the public's possible privacy concerns, and creating confidence that those privacy objectives are appropriately addressed in the development and implementation of RMEW. 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 PIA was conducted on the RMEW applications of TeamConnect (TC) and its sub-component, the Document Management System (DMS). RMEW is cited on the PBGC's System List and reported on either the PBGC's Exhibit 53 or the capital planning and investment control (Exhibit 300s) process. It is also listed as a Major Application and is a customized COTS application that is owned by PBGC.

RMEW investment consists of an application built on the Commercial off-the-shelf (COTS) product TeamConnect for Legal Matters which is supported by the DMS component that is built on IBM FileNet. Both components of RMEW have web front-ends. Images and content of documentation such as letters and email are scanned and/or processed through the PBGC's enterprise FileNet infrastructure and stored as searchable documents in the FileNet image store. The DMS database stores metadata and indexing to pull those images from the PBGC Enterprise FileNet image store. The security controls of FileNet are documented with the Image Processing System (IPS) minor application within its associated System Security Plan (SSP), Benefit Administration. RMEW is an aggregation of the data from DMS, e4010, CMS, and CDMS PBGC datastores.

II. PIA APPROACH

PBGC developed a questionnaire 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) publications, and the Federal Enterprise Architecture Business Reference Model (BRM). PBGC developed the questionnaire in order to identify any Personally Identifiable Information (PII).

The questionnaire was given to the Information System Owner (ISO) of the RMEW application for completion. A PBGC Information Security Analyst met with the ISO of RMEW to discuss the questionnaire. Responses from the ISO of RMEW were obtained and used to fill in the final PIA and analysis.

III. SYSTEM CHARACTERIZATION

TC is comprised of three components: TC Legal Matters a COTS application, TC Data Mart, and the TC Reports component. The TC COTS application is accessed via a web interface as the TC Data Mart is hosted on web supporting infrastructure. The TC Data Mart provides defined and ad-hoc reporting from data sources linked to the TC database. Reports are deployed to Reports Server and are used to track operational metrics.

DMS is built on the IBM FileNet COTS application suite and the existing FileNet infrastructure, but also adds the mechanism to store the content of those images in a searchable .pdf file format. Emails and other documents are also easily imported into the DMS content repository. The searchable .pdf files are produced after scanning by the OCR software installed on the FileNet PE.

TC and DMS share a database, while using separate schemas within that database which is maintained by the PBGC Enterprise DBAs. Each schema is allotted space on the PBGC Database server hosted PBGC's infrastructure. The FileNet Business Process Manager (BPM) implementation consists of database servers and application servers. The servers are managed by PBGC Infrastructure Administration (IA) and patched per PBGC policy. The security of the FileNet system is documented in the PBGC Image Processing System (IPS) System Security Plan.

Security considerations are all subject to the PBGC Information Assurance Handbook (IAH) policies and procedures. There are several connections made through TC and DMS and any system password for those connections are encrypted. The transmission of these passwords is not currently designed for all channels, however this is planned to be remediated in the next release. Each connection that is currently encrypted is detailed within this RMEW System Security Plan (SSP). Encrypted channels are not required for data transfer for this system since there is no PII or sensitive data being transferred.

TC aggregates data from the following data stores:

- DMS – Document Management System is the system which inputs and indexes the images and content of images for TC.

- CAS/CMS – TC pulls data from the CAS database. TC also pushes data (10-20 data fields) through CMS web-service into the CAS database to open a case and update the plan assets and liabilities.
 - CDMS – TC does a regular lookup and update of Form 1/Schedule A filings in CDMS. Updates of these filings are pulled into the TC database. This ensures that DISC always has access, via TC to the most current premium filing information on the companies it monitors. Once the desired results are obtained, they are interpreted in TC and the appropriate Object record and fields are updated. Appropriate error logs are defined to capture error conditions including connection failures and other problems.
 - e-4010 – TC pulls data from the e-4010 database - to ensure that DISC always has access, via TC to the most current e-4010 filing information on the companies it monitors.
- The RMEW Production Servers are located in PBGC's computer room at 1200 K Street NW, Washington, D.C. 20005. The RMEW failover meets PBGC's disaster recovery plan and server redundancies for Continuity of Operations Plan. PAS – TC pulls 5500 Plan data from PAS

Servers that are part of the General Support Systems (GSS) or are covered by other SSP's are not listed below. Configurations of all support servers for TC and DMS are documented in the IPS or the GSS SSPs. The servers hosting the data being pulled into the TC database are also outside of the boundary.

IV. PIA RESULTS

The PIA evaluation revealed that the RMEW/TeamConnect application does contain PII, as well as sensitive information. Only those who are authorized to use the application have access to it and the information contained therein. The users are utilizing the information for the sole purpose of performing their assigned duties. No discrepancies have been discovered.

V. SUMMARY

During the assessment of RMEW/TeamConnect no discrepancies in the handling of PII have been discovered.