Pension Benefit Guaranty Corporation (PBGC)
Privacy Impact Assessment (PIA)

Corporate Performance Systems (CPS)
05/14/2018

Privacy Point of Contact

Name	Peter Sperry
Title	CPS ISO
Phone	202-236-400 x6502
Email	Sperry.Peter@pbgc.gov

TIP!

This point of contact should be the person you want the Privacy Office to work with in completing this PIA. For some systems it might be the Information Owner (IO) or Information System Owner (ISO). Many business units identify this as the Information System Security Officer (ISSO). DO what makes sense for you!

1 Privacy Impact Assessment

A Privacy Impact Assessment (PIA) is an analysis of how information is/will be handled:

i. To ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy,
ii. To determine risks and effects of collecting, maintaining, and disseminating information in an identifiable form in an electronic information system, and
iii. To examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks.

Privacy concerns are highest for systems that contain Personally Identifiable Information (PII). PII is defined as information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual. Because there are many types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad.

TIP!

Information that either alone or when considered with other information that uniquely identifies a person is Personally Identifiable Information (PII). Combining pieces of information whether private or publicly available has powerful implications for uniquely identifying an individual.

For example, consider a person named Mary Jones. There are over 200 million results in an internet search for this name. But if we combine information such as a date of birth, the last four digits of a (or worse, an entire) Social Security Number, or a spouse's name, the number of persons to whom we could be referring begins to narrow quite rapidly. These types of information are considered identifiers. Identifiers that uniquely identify a person are the focus of privacy protection.

1.1 The Components of the System

Name of component	Describe the component (1 or 2 sentences)	Does this component contain PII	In what system of records (SORN) is this information stored	What is the Legal Authority for collection of this information	Does this system share PII externally *(please detail in question 9)*
Corporate Data Management System (CDMS)	CDMS serves as a data warehouse solution providing access in part to participant information in support of Pension Plan termination and trusteeship operations and analyses.	Yes	PBGC-6, Plan Participant and Beneficiary Data PBGC-14, My Plan Administration Account Authentication Records	CPS does not collect PII; information is populated from other PBGC databases. The PII contained in those source databases is collected pursuant to 29 U.S.C § § 1055, 1056(d)(3), 1302, 1306, 1307, 1321, 1322, 1341, 1342, 1343, and 1350.	No
Corporate Performance Reporting System (CPRS)	CPRS delivers corporate performance measurement, analysis and reporting primarily through the use of the Cognos tool. This performance reporting fosters	Yes	PBGC-6, Plan Participant and Beneficiary Data PBGC-14, My Plan Administration Account Authentication Records	CPS does not collect PII; information is populated from other PBGC databases. The PII contained in those source databases is collected pursuant to 29 U.S.C § § 1055, 1056(d)(3), 1302,	No

	and improves corporate-wide understanding and use of established performance measures and improves the overall level of information sharing between departments.			1306, 1307, 1321, 1322, 1341, 1342, 1343, and 1350.	

1.2 The System as a Whole

1. Please describe the purpose of the system, when considered as a whole, please include if this is an existing system (either an annual recertification update or a major change)

CDMS is a major information system owned and operated by the Quality Management Department (QMD). It was developed to allow users to aggregate data from several systems in one place. It is comprised of a CDMS Portal, CDMS Web Server (Middle Tier) and CDMS Database (Back End). CPRS is a Cognos software based application reporting tool. Cognos is licensed, owned, and operated by QMD. It is a data mart and analytics business intelligence tool that supports corporate performance measurement and balanced scorecard analysis and reporting.

2. What are the Confidentiality, Availability, and Integrity ratings for the system as a whole?

Confidentiality	Moderate
Integrity	Moderate
Availability	Low

3. List and discuss the sources from which the system collects PII (for instance, from an individual, another federal agency, etc.); the format in which PII is collected (for instance, via a form, face-to-face, phone, etc.); the notification given at time of collection from an individual regarding the Privacy Act and the ability to opt-out of collection (and the consequences of opting out). Include a copy of all forms and Privacy Act statements used to collect information.

CPS is not the originating data system as CDMS pulls data from Genesis/Spectrum, Case Management, Customer Relationship Management (CRM), and Premium Accounting systems. Data are extracted and loaded into CPRS on ADMPROD on a monthly basis with the help of OWB ETL mappings and DB cron jobs each month on the first business days. CPRS is not the originating system.

4. Discuss any privacy controls that PBGC inherits from an external provider (cloud provider, third party provider, another government agency, etc.) If an Interconnection Security Agreement (ISA), Memorandum of Understanding (MOU),

or similar document is in place, please summarize the privacy applicable portions of that document.

CPS do not inherit any privacy controls from an external provider. There is no applicable ISA or MOU.

5. For the user roles in the system:

Role Name	**Number of Users in that role**	**Approver**	**Access Level (Read, Write, etc)**	**Recertification Date**
CDMS User	13	Peter Sperry	Read only	September 2017
CDMS User (FOD)	2	Peter Sperry	Read only	September 2017
CDMS User (CPRD)	1	Peter Sperry	Read only	September 2017
CDMS O&M Support	1	Peter Sperry	Read only	September 2017
CPRS (Cognos) User	66	Peter Sperry	Read only	September 2017
CPRS (Cognos) Author	13	Peter Sperry	Read only	September 2017
CPRS (Cognos) Admin	3	Peter Sperry	Read/Write	September 2017
CPRS (Cognos) Manual Metrics	4	Peter Sperry	Read/Write	September 2017

6. Does the System leverage the Enterprise Access Controls?

☒ Yes

☐ No

7. Discuss the Physical, Technical, and Administrative controls that are employed to secure the PII in the system.

Physical security controls employed to secure the PII in the system include: security guards, identification badges, locked offices and secured facility.

Technical controls employed to secure the PII in the system include: password protection, Network firewalls, unique user identification names, encryption and intrusion detection system.

Administrative security controls employed to secure the PII in the system include: periodic security audit, annual refresher training for security, privacy and records management, mandatory on-boarding training for security, privacy and records management and methods to ensure that only authorized personnel have access to PII.

8. For the PII in the system, discuss the actual/intended uses of the PII; the steps taken to limit the PII collected to the minimum needed; and the reasons the PII is necessary and relevant.

The social security number (SSN) displays only the last four digits, the rest of the number is masked. There is one (1) report (BPR100 - List of Benefit Applications Processed), that has names and the last four digits of the SSN, no other information such as address, birthdays are used.

The intended use is to allow approved users access to granular information to make meaningful inquires and to provide necessary values for informed decisions where applicable.

Note: Still exploring all options for CPS replacement, which includes decommissioning CPS entirely. A decision has not been reached yet, neither has a budget been requested for 2020.

9. Discuss the data flows within the system (include sources of data for data flowing into the system, destinations for data flowing out of the system, and any routine uses applicable to the system). For any information that is shared internally, be sure to discuss whether these data interconnections are noted in CSAM. Be sure to include any MOU, ISA, or Interagency Agreements.

PII in CPS is stored in a database secured within PBGC network. Data is not shared internally/externally with any system.

Name, last four digits of social security number(SSN) and plan type is the only PII used for one (1) report generated in CPRS. All other PII is not used.

10. Does the system leverage the commonly offered control for Accounting of Disclosures?

☒ Yes
☐ No

1.3 Privacy Office Review

Name of Reviewer	Stefan Ducich, Contract Attorney
Date Reviewed	06/07/2018
Expiration Date	
Result	☒Approved without conditions ☐Approved with conditions (see below). ☐Denied

(For Privacy Office Use Only)

Discuss analysis of risks and compensating controls (or other mitigation steps.

Enter description here.

Discuss any conditions on Approval

Enter description here.

1.4 Signatures and Approval

Information System Owner/Information Owner	
Name:	PETER B SPERRY
Dept/Office:	QMD / EED
Phone:	X 6502
Email:	SPERRY.PETER@PBGC.GOV
I certify that this PIA is an accurate representation of the security and privacy controls in place to protect the PII that the system does/will collect or maintain.	
Signature	Peter B Sperry
Date signed	6/19/18

Authorizing Official	
Name:	DIANE BRAUNSTEIN
Dept/Office:	QMD
Phone:	X 3617
Email:	BRAUNSTEIN.DIANE@PBGC.GOV
I certify that this PIA is an accurate representation of the security and privacy controls in place to protect the PII that the system does/will collect or maintain.	
Signature	Diane Braunstein
Date signed	6/19/18

Chief Privacy Officer	
Name:	
I certify that I have reviewed this PIA and have fully considered the privacy risks that this system creates.	
Signature	
Date signed	6/20/18

This page is for internal routing purposes of documentation of approvals. Upon final approval, this page <u>must</u> be removed prior to publication of the PIA.