Pension Benefit Guaranty Corporation (PBGC)

Privacy Impact Assessment (PIA)

Consolidated Financial System (CFS)

04/29/2021

1 Privacy Point of Contact

Name	Mary Sasscer
Title	(Acting) Information System Security Privacy Officer
Phone	202-326-4100 ext. 3654
Email	Sasscer.Mary@pbgc.gov

2 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.

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.

2.1 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 internally
Concur (bi-directional flow)	Concur processes travel vouchers and claims for authorized government travel.	Yes	GSA/GOVT-4, Contracted Travel Services Program (June 3, 2009).	29 U.S.C. §§ 1302, 31 U.S.C. § 3711(e) and 44 U.S.C. § 3101.	Yes
Secured Payment System (bi-directional flow)	Secure Payment System is an application that provides a mechanism which allows personnel at PBGC and Federal Program Agency locations to create payment schedules in a secure fashion	Yes	PBGC-2, Disbursements – PBGC 83 FR 6254 (February 13, 2018); PBGC-3, Payroll, Leave, and Attendance Records – PBGC 83 FR 6256 (February 13, 2018); PBGC-13, Debt Collection – PBGC 83 FR 6264 (February 13, 2018)	29 U.S.C. §§ 1302, 1306, 1307, 1341, 1343, 31 U.S.C. §§ 3711(e) and 44 U.S.C. §§ 3101.	Yes
Data Act Schema	The Data Act Schema combines information from	No	Not applicable	Not applicable	Not applicable

	CFS and the Federal Procurement data System (FPDS), (PD and MEPD) that is uploaded to a Data Act broker maintained by the U.S. Department of the Treasury. The Data Act Schema contains the same PII in CFS or is made publicly available in FPDS.				

2.2 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)

The Consolidated Financial System (CFS) is a major information system within the Financial Operations Department (FOD). The CFS addresses the Pension Benefit Guaranty Corporation's budgetary, fiscal, financial, management, and reporting needs for the enterprise revolving fund, trust accounting, and consolidated financial operations. It is comprised of the following ledgers: CFS Revolving Fund, CFS Trust Accounting, and CFS Consolidated Ledgers. CFS includes custom designed interfaces with other PBGC and non-PBGC systems, including Concur.com, which is a web-based end-to-end travel service application, and WebTA, which is a DOI-run payroll application."

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.

CFS uses PII that is collected by the following interconnected systems: My Plan Administration Account (My PAA), GSA (Concur), Case Management System (CMS), Federal Personnel Payroll System (FPPS), Secured Payment System (SPS), Comprizon, FedDebt, and US Bank.

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.

CFS does not inherit any controls from an external provider, and there are ISAs and MOUs in place between Treasury (SPS) and GSA (Concur). The privacy applicable portions of those documents pertain to the descriptions in Section 2.1 The Components of the System.

5. For the user roles in the system:

Role Name	Number of Users in that role	Approver/Sign off	Access Level (Read, Write, etc)	Recertification Date
Analyst CRM	22	Raymond Bryant	Read, Write and Edit	07/01/2020
CCD Analyst TCA	20	Raymond Bryant	Read, Write and Edit	07/01/2020
CCD Supervisor TCA	4	Raymond Bryant	Read, Write and Edit	07/01/2020
CCRD CRM	6	Raymond Bryant	Read, Write and Edit	07/01/2020
CFS User CRM	5	Raymond Bryant	Read, Write and Edit	07/01/2020
Contractor Supervisor CRM	3	Raymond Bryant	Read, Write and Edit	07/01/2020
Federal Accountant CRM	6	Raymond Bryant	Read, Write and Edit	07/01/2020
Federal Approval CRM	17	Raymond Bryant	Read, Write and Edit	07/01/2020
Federal CCD Manager CRM	5	Raymond Bryant	Read, Write and Edit	07/01/2020
Federal Lead Accountant CRM	1	Raymond Bryant	Read, Write and Edit	07/01/2020
Federal Senior Accountant CRM	6	Raymond Bryant	Read, Write and Edit	07/01/2020
OGC - BLT User CRM	1	Raymond Bryant	Read, Write and Edit	07/01/2020
PBGC CCD Analyst TCA	9	Raymond Bryant	Read, Write and Edit	07/01/2020
PBGC CCD Manager TCA	7	Raymond Bryant	Read, Write and Edit	07/01/2020
STCD User CRM	1	Raymond Bryant	Read, Write and Edit	07/01/2020

Role Name	Number of Users in that role	Approver/Sign off	Access Level (Read, Write, etc)	Recertification Date
Suspense Approver CRM	5	Raymond Bryant	Read, Write and Edit	07/01/2020
Suspense Federal Approver CRM	14	Raymond Bryant	Read, Write and Edit	07/01/2020
Grand Total	132	-		-

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.

The CFS has the following Physical, Technical, and Administrative controls in place.

(1) Physical controls – Security guards, key entry, locked file cabinets, secured facility, closed circuit television, cipher locks, identification badges, and locked offices.

(2) Technical controls– Password protection, virtual private network, firewalls, unique user identification names, encryption, intrusion detection, and personal identity verification.

(3) Administrative controls – security audits, monitoring of user activity, refresher security, privacy, records management, and role-based training, backups secured off-site, encryption of backups, least privilege to restrict access to PII and Personal Identity Verification.

(4) Access and least privilege controls-The Financial Operations Department documents its access procedures in the 6.0 System Access and Production Support document.

Users are granted access via GetIT, the PBGC network process. Requests are approved by the user's supervisor and the primary or alternate Information System Owner. The user's supervisor determines system responsibility, as approved by the primary or alternate Information System Owner. Quarterly, a review is performed to verify that users still have an active Local Area Network account. Annually, a recertification of all active users and their roles is conducted by the Financial Operations Department, Policies Procedures and Control Division, as per the 2.0 User Recertification document.

The Financial Operations Department also separates duties of individuals as necessary. Unique roles and responsibilities are established to promote separation of duties and to prevent one user from having access that would allow them to violate internal control. Roles and responsibilities that may pose a conflict have been identified. Any new roles and responsibilities are reviewed to ensure that the Financial Operations Department retains separation of duties. When users request access via GetIT, the user's supervisor and the information system owner are required to review and approve the request before the access is granted. The Financial Operations Department, Financial Systems Branch also reviews each request to ensure that separation of duties is maintained for each user, and the requested access does not violate the conflicts that have already been identified. In those cases where conflicts are identified, the Financial Systems Branch will not grant the access until the conflict has been resolved.

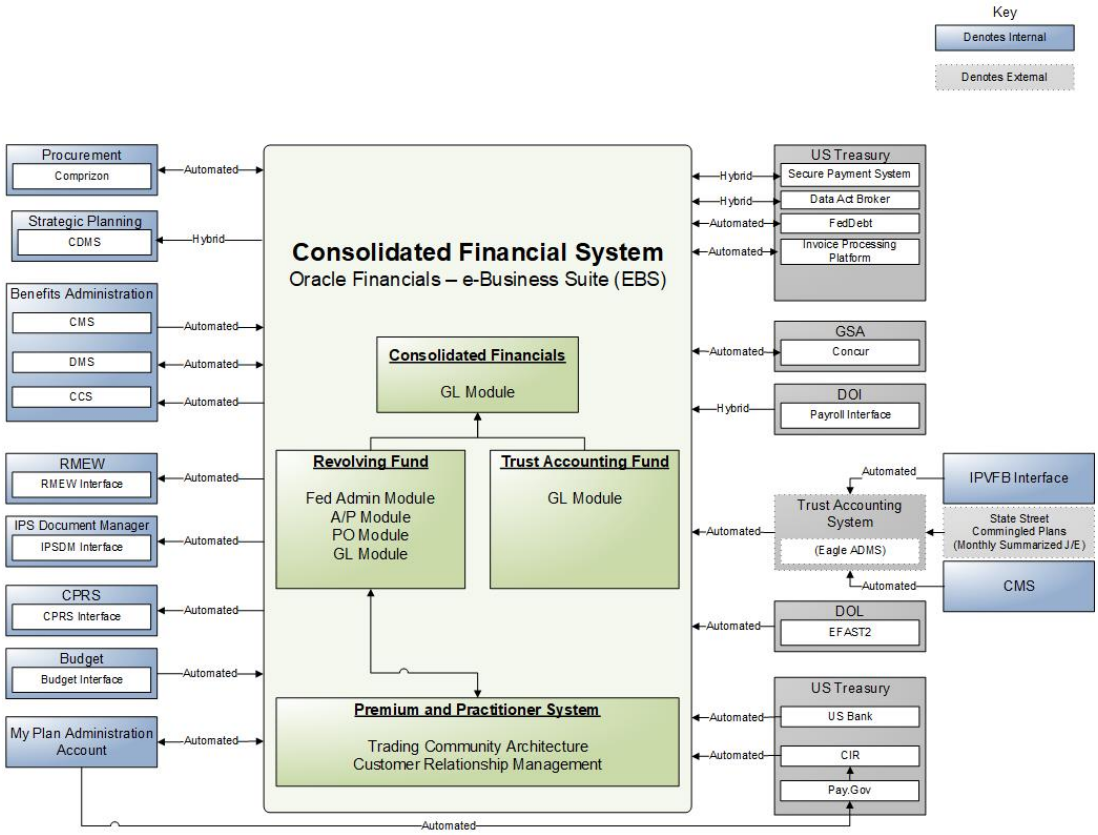
8. Discuss the Physical, Technical, and Administrative controls that are employed to secure the PII in the system.

The PII records are maintained for:

- Determining amounts to be paid and in effecting payments by the Department of the Treasury on behalf of PBGC.
- Collecting debts owed to PBGC by various individuals, including, but not limited to, pension plans and/or sponsors owing insurance premiums, interest and penalties; PBGC employees and former employees; consultants and vendors; participants, alternate payees, and beneficiaries in terminating and terminated pension plans covered by ERISA; and individuals who received payments from PBGC to which they are not entitled.
- Facilitating PBGC's compliance with the Debt Collection Improvement Act of 1996.

9. 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 Consolidated Financial System (CFS) is a major information system within the Financial Operations Department (FOD). The CFS addresses the Pension Benefit Guaranty Corporation's budgetary, fiscal, financial, management, and reporting needs for the enterprise revolving fund, trust accounting, and consolidated financial operations. The following diagram depicts data flows.



While Section 2.1 Components of the System describe the dataflows and Section 8 describes routine uses*, information is transmitted via electronic connections occurring within the boundaries of the PBGC internal network infrastructure to external parties. These interconnections are listed in the Cyber Security Assessment and Management Tool (CSAM), System Security Plan (SSP). The ISAs and MOUs are available in CSAM, but the interagency agreements are not available to security personnel.*

Information is transmitted via electronic connections occurring within the boundaries of the PBGC internal network infrastructure as well as hard and soft copy reports with the following offices:

- *Office of the General Counsel (OGC)*
- *Corporate Finance & Restructuring Department (CFRD)*
- *Policy, Research and Analysis Department (PRAD)*
- *Office of Benefits Administration (OBA)*
- *Multiemployer Program Division (MEPD)*
- *Procurement Department (PD)*

PII is shared with Contractors for Operations and Maintenance (O&M) of the system. These are not interconnections and are not identified in the CSAM, SSP.

10. 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.

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

    ☒ Yes
    ☐ No

2.3 Privacy Office Review

Name of Reviewer	
Date Reviewed	4/29/21
Expiration Date	4/29/22
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.