Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Consolidated Financial Services (CFS)

Privacy Impact Assessment (PIA)

Last Updated: 5/18/2026

1 PRIVACY POINT OF CONTACT

Name	Catherine Diamante
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202-403-4260
Email	Diamante.catherine@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.

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.

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 *(please detail in question 13)*
Premium and Practitioner System (PPS)	PPS functionality is used for: processing annual filings; calculating premium, interest, and penalty owed; and creating accounting ledger entries for PBGC's Consolidated Financial Systems (CFS) accounting system.	Yes	PBGC-2 and 13.	29 U.S.C. 1302; 44 U.S.C. 3101; 5 U.S.C. 301; 31 U.S.C. 6101; 31 U.S.C. 9101, et seq.; 31 U.S.C. 3716. 29 U.S.C. 1302; 31 U.S.C. 3711(a) (1) (2) (3); 44 U.S.C. 3101; 5 U.S.C. 301; Executive Order 1301	Yes
General Ledger	CFS contains 3 ledgers: Revolving Fund, Trust Accounting Fund, and Consolidated Fund. Transaction data from other PBGC systems feeds the Revolving and Trust fund subledgers, which feed the Consolidated Fund.	No			No

2.2 The System as a Whole

1. Please describe the purpose of the system when considered as a whole.

The Consolidated Financial System (CFS) is a major information system with Premium and Practitioner System (PPS) module.

CFS's General Ledger is comprised of the following ledgers:

- *The CFS Revolving Fund Ledger;*
- *The CFS Trust Accounting Ledger; and*
- *The CFS Consolidated Ledger.*

CFS is a production system based on the Oracle Federal Financials (E-Business Suite) Commercial Off-the Shelf (COTS) application product. CFS also includes custom designed interfaces that integrate CFS with other PBGC and non-PBGC systems.

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

Confidentiality	Moderate
Integrity	Moderate
Availability	Moderate

3. Is this a contractor system?

☐Yes
☒No

4. Is this a new or existing information system? If this is an existing information system, please describe the changes.

CFS is an existing system. Since the last review of the system, Concur was removed from the CFS boundary and is now maintained in its own boundary.

5. Does your system collect, process, or maintain any records that describe how any individual exercises their First Amendment rights?

   If so, please describe the information it collects and the purpose for the collection. Please describe whether: 1) an express legal authority authorizes the collection, 2) the collection is pertinent to and within scope of an authorized law enforcement activity, or 3) the individual(s) consents to the collection.

(The First Amendment guarantees an individual's right to the exercise of their religious beliefs, their petitioning the government, their exercise of free speech, their right to peaceably assemble, and the freedom of the press.)

No

6. For the PII in the system, discuss the actual/intended uses of the PII; procedures taken to limit the PII collected to the minimum needed; reasons the PII is necessary and relevant; and procedures taken to periodically review the accuracy, relevance, timeliness, and completeness of PII throughout the information life cycle.

The PII records are maintained for: • *Determining amounts to be paid and in effecting payments by the Department of the Treasury (DoT) 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.* *Restricted fields are in place to limit access to only the minimum necessary PII.*

7. Discuss how your system retrieves PII. Please describe the identifiers used to locate records within a system, such as name, identification number, date of birth, etc.

PII is retrieved by a two-digit identifier

8. Approximately how many individuals' PII is maintained in the system?

Approximately 927 individuals PII is maintained.

9. Is the submission of PII by individuals voluntary or mandatory? If the submission is voluntary, what is the outcome of an individual not submitting PII.

Individuals do not directly submit PII to CFS; rather, it is collected from other systems, such as HRD systems.

10. If your system collects Social Security Numbers:

    a. Please provide a justification for the collection, use, maintenance, and disposal of PII in the form of SSN?

CFS does not collect SSN. The General Accounting Branch (GAB) processes the bi-weekly payroll cost file that contains employee SSN in the file. GAB downloads the file from DOI's FPPS system and processes the file in CFS. GAB will save the bi-weekly cost file to SharePoint site that has limited access by GAB staff. SSNs are used within CFS to process payroll and reimburse employees for travel or other approved expenses.

b. Under which authorized uses, as described in the "Reduction of use of Social Security Numbers (SSN) in PBGC" policy document?

The CFS applications are authorized to use SSNs under Government Data Matching. SSNs are primary identifiers as a primary means for transferring, matching, or checking information with Federal Personnel Payroll System (FPPS) Human Resource Management System, Concur, and Employee Express.

c. If the answer to b., above is "Compelling Business Need," please provide a plan to reduce the use of SSNs, highlighting activities that can be completed in the next 12 months.

N/A

11. 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), SAP Concur (Concur Gov), Federal Personnel Payroll System (FPPS), Premium and Practitioner System (PPS), QuickTime, and Employee Express. Since CFS does not collect PII directly from individuals, a Privacy Act Statement is unnecessary.

12. 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.

No privacy controls are inherited from an external provider.

13. Is the PII shared with external (non-PBGC) organizations? If so, identify with whom the PII is shared and the purpose. 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.

Yes, CFS shares limited PII externally with the DoT to support authorized federal financial operations, including employee expense reimbursement via SPS and mandatory debt collection processes. Internally, CFS receives PII from HRD, FPPS payroll cost files, and GAB data entry, and shares outputs with HRD, GAB, Budget, and secure internal SharePoint repositories. These data flows must be reflected in CSAM, and any associated interagency agreements (DoT SPS, FPPS) constitute the governing sharing framework for these exchanges.

14. For the user roles in the system:

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Analyst CRM	18	Brad Porter	Read, Write and Edit	05/26/2025
CCD Analyst TCA	18	Brad Porter	Read, Write and Edit	05/26/2025
CCD Supervisor TCA	3	Brad Porter	Read, Write and Edit	05/26/2025
CCRD CRM	3	Brad Porter	Read, Write and Edit	05/26/2025
CFS User CRM	5	Brad Porter	Read, Write and Edit	05/26/2025
Contractor Supervisor CRM	3	Brad Porter	Read, Write and Edit	05/26/2025
Federal Accountant CRM	3	Brad Porter	Read, Write and Edit	05/26/2025
Federal Approval CRM	13	Brad Porter	Read, Write and Edit	05/26/2025
Federal CCD Manager CRM	3	Brad Porter	Read, Write and Edit	05/26/2025
Federal Lead Accountant CRM	2	Brad Porter	Read, Write and Edit	05/26/2025
Federal Senior Accountant CRM	6	Brad Porter	Read, Write and Edit	05/26/2025
PBGC CCD Analyst TCA	7	Brad Porter	Read, Write and Edit	05/26/2025
OGC - BLT User CRM	0	Brad Porter	Read, Write and Edit	05/26/2025
OGC-PLPD User CRM	0	Brad Porter	Read, Write and Edit	05/26/2025
PPS Analyst Suspense	16	Brad Porter	Read, Write, and Edit	05/26/2025
PPS Approver Suspense	6	Brad Porter	Read, Write and Edit	05/26/2025

Role Name	Number of Users in that Role	Approver	Access Level (Read, Write, etc.)	Recertification Date
PPS Fed Approver	13	Brad Porter	Read, Write and Edit	05/26/2025
PPS Super Analyst Suspense	2	Brad Porter	Read, Write and Edit	05/26/2025
STCD User CRM	2	Brad Porter	Read, Write and Edit	05/26/2025
Suspense Approver CRM	5	Brad Porter	Read, Write and Edit	05/26/2025
Suspense Federal Approver CRM	11	Brad Porter	Read, Write and Edit	05/26/2025
Grand Total	**139**	-	-	-

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

Physical Controls - Physical security controls employed to secure the PII in the system include:*

- *Physical Access Authorizations*
- *Physical Access Control*
- *Access Control for Transmission Mission*
- *Access Control for Output Devices*
- *Monitoring Physical Access*
- *Visitor Control*
- *Access Records*
- *Power Equipment and Power Cabling*
- *Emergency Shutoff*
- *Emergency Power*
- *Emergency Lighting*
- *Fire Protection*
- *Temperature and Humidity Controls*
- *Delivery and Removal*
- *Alternate Work Site*
- *Location of information Components*
- *Information Leakage*

**Physical Controls are provided by both PBGC and the Cloud Service Provider (CSP)*

*Technical Controls** - Technical controls employed to secure the PII in the system include:*

- *Account Management*
- *Access Enforcement*
- *Authenticator Management*
- *Cryptographic Module Authentication*
- *Information Flow Enforcement*

- *Separation of Duties*
- *Least Privilege*
- *Unsuccessful Login Attempts*
- *Remote Access*
- *Wireless Access*
- *Audit Events*
- *Audit Review, Analysis, and Reporting*
- *Time Stamps*
- *Audit Record Retention*
- *Non-repudiation*
- *Session Audit*
- *Public Key Infrastructure Certificates*
- *Denial of Service*
- *Network Disconnect*
- *Session Authenticity*
- *Protection of Information at Rest*

***Technical Controls are provided by both PBGC and the CSP*

Administrative Controls - All PBGC users are required to complete privacy training annually. Administrative controls employed to secure the PII in the system include:

- *Periodic Security Audits*
- *Regular Monitoring of User's Activities*
- *Annual Security, Privacy, and Records Management Refresher Training*
- *Backups Secured Offsite*
- *Encryption of Backups containing sensitive data*
- *Role-Based Training*
- *Least Privilege Access - The Financial Operations Department documents its access procedures in the 6.0 System Access and Production Support document.*

Mandatory on-boarding training for security, privacy, and Records management personnel

16. Please discuss additional training for users, other than the PBGC mandatory annual training, for protecting information in the system.

Besides PBGC mandatory training (Information Security & Privacy Awareness, Privacy Literacy, Insider Threat, and Rules of Behavior), CFS users are offered additional on the job training and other privacy refreshers by the Learning and Development Division via FedTalent Learning Management.

17. Does the System leverage the Enterprise Access Controls?

☒ Yes
☐ No

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

☒ Yes
☐ No

19. Discuss the process in place for retention and destruction of PII. Cite the applicable retention schedule(s).

PBGC retains and destroys PII in accordance with the National Archives and Records Administration (NARA) records and the PBGC Simplified Records Schedule outlined in the FOD File Plan Dashboard – "Break file at the end of each fiscal year or case closure (latest documented use). Destroy or delete after 7 years."

2.3 Privacy Office Review

Name of Reviewer	Loretta Dennison
Date Reviewed	5/15/2026
Expiration Date	5/15/2027
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