Pension Benefit Guaranty Corporation

Information Technology Infrastructure Operations Department (ITIOD)

Concur Gov
Privacy Impact Assessment (PIA)

Last Updated: 09/10/2025

1 PRIVACY POINT OF CONTACT

Name	Catherine Diamante
Title	Information System Security and Privacy Officer (ISSPO)
Phone	202.229.6039
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.

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)*
Concur Gov (bidirectional flow)	*Concur Gov processes travel vouchers and claims for authorized government travel.*	Yes	GSA/GOVT-4	31 U.S.C. §§ 3511, 3512, and 3523; 5 U.S.C. Chapter 57; and 41 Code of Federal Regulations (CFR), Implementing Federal Travel Regulations (FTR) Chapters 300-304	Yes

2.2 The System as a Whole

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

Concur Gov is a Software-as-a-Service (SaaS) cloud solution implemented at PBGC to streamline and modernize official federal travel operations. This secure, web-based platform provides end-to-end travel and expense management tailored for federal agencies, including PBGC.

Concur Gov supports the full lifecycle of official PBGC travel—from planning and authorization to booking, processing, and oversight. With Concur Gov, PBGC travelers and travel arrangers can:

- Plan and book air, rail, lodging, and car rental reservations online in compliance with federal travel regulations
- Prepare and submit travel authorizations and vouchers electronically, reducing manual processing time
- Generate itineraries, issue tickets, and store receipts digitally, enabling greater efficiency, transparency, and audit readiness.

By leveraging Concur Gov, PBGC ensures consistency, accountability, and convenience across all aspects of official travel.

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.

This is an existing system. No changes have occurred since the last review.

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 intended use of PII is to identify the intended traveler/recipient and provide reimbursement to the traveler, as needed. Only information required to complete the process is requested. Concur procedures are reviewed annually. Employees and contractors that are required to travel on behalf of the agency provide their Personally Identifiable Information (PII) which can consist of the following identifiers -name, email, employee ID (CFS Supplier Number) for identification purposes in the submission of a traveler 's request. That information, including banking information, is used to create the traveler's profile in Concur Gov. The employee and contractor's information are maintained in Concur Gov to book travel and for the issuance of reimbursements. Concur Gov procedures are reviewed annually.

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.

The identifiers include Name, Email, or Employee ID (CFS Supplier Number).

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

Approximately 539.

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.

The submission of PII by individuals is mandatory for identification and reimbursement.

10. If your system collects Social Security Numbers:

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

Concur Gov does not collect SSNs.

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

N/A

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.

Concur Gov uses a web application portal to communicate with system users and to provide access to all travel management services. Individuals complete a profile maintenance form to request an account to access Concur Gov. Users provide their information via the web application to facilitate travel booking services. Use of the system constitutes a user's consent to sharing their information with authorized users. Each time a user login into the Concur portal, they accept/agree to the Privacy Act Notice which can be found at https://usg.concursolutions.com/govui.

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.

Within the Concur Gov System Security Plan, PBGC requires that providers of external system services comply with organizational security and privacy requirements. While GSA is not currently offering PT-2, PT-3, PT-4, PT-5, or PT-6 for inheritance, PBGC leverages the GSA/GOVT-4 SORN, legal authorities, purpose, and Privacy Act Statement that GSA provides. As identified in the ISA between SAP Concur, GSA, and PBGC, all parties to this agreement — including Concur, the GSA Federal Acquisition Service E-Gov Travel Services Program

Management Office, and the PBGC's Financial Operations Department–Consolidated Financial Systems (CFS) along with their employees, agents, and any third-party subcontractors, are required to comply with all applicable federal privacy laws and regulations. This includes, but is not limited to, the Privacy Act of 1974 (5 U.S.C. § 552a, as amended) and any binding, government-wide policies governing the collection, maintenance, and use of federal agency data. Compliance must also align with all relevant guidance issued by the Office of Management and Budget (OMB).

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 (including 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.

In accordance with GSA/GOVT-4, circumstances under which personal information may be shared with other entities under federal law, are primarily for travel, law enforcement, security, and administrative purposes. As part of the DHS/TSA Secure Flight program, personal data including date of birth, gender, redress number (optional), and known traveler number (future use) is collected and shared with airlines, Travel Management Centers (TMCs), and online booking systems to verify passengers against government watch lists prior to flights. This ensures compliance with national security measures and enhances aviation safety.

Beyond travel-related sharing, the information may also be disclosed to various government agencies, courts, consultants, contractors, and service providers for purposes such as legal investigations, judicial proceedings, travel reimbursement, billing, audits, personnel decisions, and program evaluations. Disclosures may also occur in cases of suspected data breaches to help contain and address potential harm. Statistical data may be released publicly if it does not identify individuals, and information may also be provided to labor organizations, Members of Congress (upon individual request), and agencies like OPM, GAO, or NARA for operational or regulatory reasons.

14. For the user roles in the system:

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
FT - Federal Traveler	539	David Guarnero	Read, Write and Edit	Weekly review by the Enterprise Identity Management (EIM) team and system administrator.

Role Name	Number of Users in that role	Approver	Access Level (Read, Write, etc.)	Recertification Date
Traveler FTA - Federal Travel Arranger	44	David Guarnero	Read, Write and Edit	Weekly review by the Enterprise Identity Management (EIM) team and system administrator.
FSTA - Federal Supervisory Travel Approver	159	David Guarnero	Read	Weekly review by the Enterprise Identity Management (EIM) team and system administrator.
FATA Level 6 - Federal Agency Travel Administrator	8	David Guarnero	Read, Write and Edit	Weekly review by the Enterprise Identity Management (EIM) team and system administrator.
FATA Level 8 - Federal Agency Travel Administrator	6	David Guarnero	Read, Write and Edit	Weekly review by the Enterprise Identity Management (EIM) team and system administrator.
Grand Total	**756**			

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

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

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

Besides PBGC mandatory training (Cyber Awareness and Rules of Behavior), Concur 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).

Concur Gov records are retained in accordance with the GSA ETS2 Master Contract, which specifies compliance with the records retention requirements established by the NARA, accessible at http://www.archives.gov/about/laws/. General Records Schedule 1.1: Financial Management Reporting Records for Transportation and Travel Requests, Authorization and Vouchers: destroy after six years, but longer retention is authorized if required for business use.

2.3 Privacy Office Review

Name of Reviewer	Loretta Dennison
Date Reviewed	09/10/2025
Expiration Date	09/10/2026
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).

Discuss any conditions on Approval
