United States Environmental Protection Agency

PRIVACY IMPACT ASSESSMENT

(Rev. 2/2020 - All Previous Editions Obsolete)

Please submit your responses to your Liaison Privacy Official.
All entries must be Times New Roman, 12pt, and start on the next line.
If you need further assistance, contact your LPO. A listing of the LPOs can be found here:
https://usepa.sharepoint.com/:w:/r/sites/oei_Community/OISP/Privacy/LPODoc/LPO Roster.docx

System Name: Concur		**Behalf of the System Owner: Andrew Battin**	
Preparer: Andrew Lam		**Office: OCFO/OTS**	
Date: 4.11.24		**Phone: 202.564.2925**	
Reason for Submittal:			
New: ☒	Revised ☐	Annual Review: ☐	Rescindment: ☐
System Lifecycle Stage(s):			
Definition ☐	Development/Acquisition ☐	Implementation ☐	
Operation & Maintenance ☒	Rescindment/Decommissioned ☐		
Note: New and Existing Systems require a PIA annually, when there is a significant modification to the system or where privacy risk has increased to the system. For examples of significant modifications, see OMB Circular A-130, Appendix 1, Section (c) (1) (a-f). **The PIA must describe the risk associated with that action. For assistance in applying privacy risk see OMB Circular No. A-123, Section VII (A) (pgs. 44-45).**			

Provide a general description/overview and purpose of the system:

Concur Cloud Public Sector CCPS is SAP Concur's end-to-end travel and expense management software as a service (SaaS) solution for United States federal agencies. CCPS includes a web application portal to

communicate with system users and provide access to all services. The web application gives users the ability to facilitate travel booking services, change travel reservations, and authorize travel. From vouchering services to documenting trip approvals and expense reimbursements, the web application provides accurate accounting to government systems in compliance with the Federal Travel Regulation (FTR), Joint Travel Regulations (JTR), and Joint Federal Travel Regulations (JFTR). Users access CCPS using standard web browsers via a URL or using SAP Concur mobile applications for supported mobile devices (i.e., smartphones, tablets, and computer platforms). The CCPS solution provides the following features for its customers:

- Travel process and travel management expertise
- Web-based reservation booking services
- Travel workflow creation with protected user roles
- Travel agency support
- Travel planning and cost estimating
- Travel creation and approval workflow
- Filing, processing, and workflow approval of travel claims
- Interface with agency financial systems
- Reporting and data exchange

Section 1.0 Authorities and Other Requirements

1.1 What specific legal authorities and/or Executive Order(s) permit and define the collection of information by the system in question?

APPLICABLE LAWS AND REGULATIONS include 31 U.S.C. 3511, 3512, and 3523; 5 U.S.C. Chapter 57; and implementing Federal Travel Regulations (41 CFR Chapters 300–304).

1.2 Has a system security plan been completed for the information system(s) supporting the system? Does the system have or will the system be issued an Authorization-to-Operate? When does the ATO expire?

Yes. It does not have an ATO, but it has an ATU, which will expire on January 17, 2027.

1.3 If the information is covered by the Paperwork Reduction Act (PRA), provide the OMB Control number and the agency number for the collection. If there are multiple forms, include a list in an appendix.

No, the information is not covered by the Paperwork Reduction Act; No ICR is required.

1.4 Will the data be maintained or stored in a Cloud? If so, is the Cloud Service Provider (CSP) FedRAMP approved? What type of service

(PaaS, IaaS, SaaS, etc.) will the CSP provide?

Yes, Concur is FedRAMP-approved. It is a SaaS.

Section 2.0 Characterization of the Information

The following questions are intended to define the scope of the information requested and/or collected, as well as reasons for its collection.

2.1 Identify the information the system collects, uses, disseminates, or maintains (e.g., data elements, including name, address, DOB, SSN).

Name, email address, EIN, TA Number or Document number, passport number, date of birth, home address.

2.2 What are the sources of the information and how is the information collected for the system?

The information is collected directly from travelers using EPA Traveler ID Form (Form 2635-4).

2.3 Does the system use information from commercial sources or publicly available data? If so, explain why and how this information is used.

No.

2.4 Discuss how accuracy of the data is ensured.

Cincinnati Finance staff ensures the data provided on the form is correct and enters it into the system.

2.5 Privacy Impact Analysis: Related to Characterization of the Information

Discuss the privacy risks identified for the specific data elements and for each risk explain how it was mitigated. Specific risks may be inherent in the sources or methods of collection, or the quality or quantity of information included.

Privacy Risk:

There is risk associated with Concur because it processes both PII and SPII collected from EPA-associated travelers. There is risk that privacy information provided by the travel requestor might also be inaccurate.

Mitigation:

We deploy privacy controls on Concur from NIST SP 800-53 privacy control catalogue to protect PII and SPII. We mitigate risk associated with inaccurate information provided by travelers using input validation. Cincinnati Finance staff review the provided information thoroughly, validate for discrepancies, and request the requestor to make necessary corrections.

Section 3.0 Access and Data Retention by the System

The following questions are intended to outline the access controls for the system and how long the system retains the information after the initial collection.

3.1 Do the systems have access control levels within the system to prevent authorized users from accessing information they don't have a need to know? If so, what control levels have been put in place? If no controls are in place why have they been omitted?

Yes, the system does have role-based access controls. Through the use of multiple roles, each user is limited in what actions they can take and what information they can see while a payment is processed.

3.2 In what policy/procedure are the access controls identified in 3.1, documented?

Access control policies are documented in Directive No CIO 2150-P-01.3. Cincinnati Finance Center also maintains Standard Operating Procedures (SOPs) that define what actions each role can complete.

3.3 Are there other components with assigned roles and responsibilities within the system?

Yes, the Concur system incorporates role-based access controls that limit the users' rights by what information they need to review or activities they need to perform. The user's role is identified by the employee's supervisor and approved by regional/national system administrators, followed by the Concur system Security Administrator. There are no other users other than the authorized users.

3.4 Who (internal and external parties) will have access to the data/information in the system? If contractors, are the appropriate Federal Acquisition Regulation (FAR) clauses included in the contract?

OTS staff (Contractor(s)), Cincinnati Finance Center (EPA Employee(s)). FAR clause 52.224-1 (Privacy Act Notification); 52.224-2 (Design, Development operation of records) are included in GSA contracts.

3.5 Explain how long and for what reasons the information is retained. Does the system have an EPA Records Control Schedule? If so, provide the schedule number.

Records are maintained for 6 years and 3 months after final payment. They are deleted when no longer needed. Yes, it has financial records schedule EPA Records Schedule 1005.

3.6 Privacy Impact Analysis: Related to Retention

Discuss the risks associated with the length of time data is retained. How were those risks mitigated? The schedule should align the stated purpose and mission of the system.

Privacy Risk:

The data stored in Concur are retained in the system for longer than specified in the Record Retention Schedule.

Mitigation:

In order to address the risk of over-retention in Concur, records are reviewed annually after collection and maintained for up to 6 years and 3 months after final payment and then deleted.

Section 4.0 Information Sharing

The following questions are intended to describe the scope of the system information sharing external to the Agency. External sharing encompasses sharing with other federal, state and local government, and third-party private sector entities.

4.1 Is information shared outside of EPA as part of the normal agency operations? If so, identify the organization(s), how the information is accessed and how it is to be used, and any agreements that apply.

Yes, ticketing records have to go to a travel management company, BCD Travel. They use the profile information to issue tickets. BCD is a subcontractor to Concur and has a direct agreement with Concur.

4.2 Describe how the external sharing is compatible with the original purposes of the collection.

The original purpose of Concur was to book travel and make payments for travel expenses.

4.3 How does the system review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within EPA and outside?

MOUs and ISAs are reviewed by the Primary Information Office (PISO) with the approval of the Senior Information Official (SIO) and the Chief Information Officer (CIO).

4.4 Does the agreement place limitations on re-dissemination?

Yes. The use of data between interconnecting systems is covered in the MOU/ISA.

4.5 Privacy Impact Analysis: Related to Information Sharing

Discuss the privacy risks associated with the sharing of information outside of the agency. How were those risks mitigated?

Privacy Risk:

Information shared outside of the agency may be compromised if handled inappropriately.

Mitigation:

MOU between EPA and outside agencies describe the PII within the information system, the purposes for its distribution and how the data should be protected. To mitigate the risk of information being shared inappropriately, EPA users must undergo privacy awareness training to ensure that they understand EPA privacy responsibilities and procedures.

Section 5.0 Auditing and Accountability

The following questions are intended to describe technical and policy-based safeguards and security measures.

5.1 How does the system ensure that the information is used as stated in Section 6.1?

As documented in Concur System Security Plan (SSP), OCFO utilizes the Risk Management Framework strategy and process to comply with privacy protection requirements and minimize the privacy risk to individuals. Concur is subject to annual third-party security assessments conducted by FAA. Concur team members perform regular reviews of login auditing to monitor access. The Office of Inspector General's (OIG) has responsibility for monitoring and auditing privacy controls and internal privacy policies on a continuous basis to ensure effective implementation of this procedure.

Additionally, the agency Privacy Office conducts annual reviews to evaluate the PII data collected and inquires whether PII data is still required. OCFO responds to these annual FIS data calls that are used to determine if the collection of PII is relevant and necessary to accomplish the mission. In response to the FIS data call, the OCFO re-evaluates the information collected and validates the need for that information.

Individuals who have access to Concur agree to use the system strictly for travel purposes by accepting the Rules of Behavior when logging on. All users are subject to security controls and access is based roles in the system. They all have at least a basic North American Industry Classification System (NACIS) background screening. All EPA personnel with access to sensitive data are required to undergo a higher level of background screening sponsored by EPA. All passwords automatically expire after 30 days of non-use.

5.2 Describe what privacy training is provided to users either generally or specifically relevant to the system/collection.

EPA personnel and contractors are required to complete a mandatory Information Security and Privacy Awareness and Training course on an annual basis. The training course instructs personnel on security and privacy objectives, how to handle PII and how to secure information using approved techniques such as encryption. Concur users also take the annual CUI training.

5.3 Privacy Impact Analysis: Related to Auditing and Accountability

Privacy Risk:

There is risk related to auditing and accountability in terms of changes to the configuration of the system. There is a likelihood that annual audits of systems (FIS) produce inaccurate results that exposes Concur and PII processed to threats. There is also risk that logging records contain PII, and that access logging could fail in relation electronic records.

Mitigation:

We deploy controls mentioned in 5.1 above. The Concur system incorporates least privilege access controls that limit the users' rights by what information they need to review or activities they need to perform. Concur user's role is identified by the employee's supervisor and approved by regional/national system administrators, followed by the Concur system Security Administrator. The Agency Privacy Office conducts a review (Privacy Impact Analysis) to evaluate the PII data collected and reviews whether certain data are still required. OCFO responds to the annual FIS data to confirm that we are only collecting PII relevant and necessary to accomplish the mission. Data call responses are validated by SO and LPOs based on a baseline. Data is only collected and retained for the specific purpose. Only authorized OCFO administrators can effect changes to the configuration of the system. There is risk related to auditing and accountability in terms of changes to the configuration of the system. There is a likelihood that annual audits of systems (FIS) produce inaccurate results that exposes Concur and PII processed to threats. There is also risk that logging records contain PII, and that access logging could fail in relation electronic records.

Section 6.0 Uses of the Information

The following questions require a clear description of the system's use of information.

6.1 Describe how and why the system uses the information.

Concur uses the information to book travel and make payments for travel.

6.2 How is the system designed to retrieve information by the user? Will it be retrieved by personal identifier? Yes_X_ No___. If yes, what identifier(s) will be used. *(A personal identifier is a name, social security number or other identifying symbol assigned to an individual, i.e., any identifier unique to an individual. Or any identifier that can be linked or is linkable to an individual.*)

TA Number, and Voucher Number, email address, traveler name, employee ID number.

6.3 What type of evaluation has been conducted on the probable or potential effect of the privacy of individuals whose information is maintained in the system of records?

[The goal here is to look at the data collected, how you plan to use it, and to ensure that you have limited the access to the people who have a need to know in the performance of their official duties. What controls have you erected around the data, so that privacy is not invaded? ex. administrative control, physical control, technical control.]

A standard operating procedure (SOP) has been developed to enforce the sole use and purpose of travel. Individuals who have access to this system agree to use the system strictly for travel.

All users are subject to security controls and access based on roles in the system. They all have at least a basic North American Industry Classification System (NACIS) background screening and agree to Rules of Behavior.

6.4 Privacy Impact Analysis: Related to the Uses of Information

Describe any types of controls that may be in place to ensure that information is handled in accordance with the uses described above.

Privacy Risk:

Users mishandle Concur PII.

Mitigation:

To reduce the likelihood of mishandling PII in Concur, privacy awareness training is provided to ensure that personnel understand privacy responsibilities and procedures. EPA personnel and contractors are required to complete an Information Security Awareness and Training course on an annual basis. Individuals who have system access must have a security background check. Concur only grants access to users based on the principle of least privilege, which provides user sufficient access to perform their jobs, no higher than necessary to accomplish their organizational missions/business functions.

***If no SORN is required, STOP HERE.**

The NPP will determine if a SORN is required. If so, additional sections will be required.

Section 7.0 Notice

The following questions seek information about the system's notice to the individual about the information collected, the right to consent to uses of information, and the right to decline to provide information.

7.1 How does the system provide individuals notice prior to the collection of information? If notice is not provided, explain why not.

The system does provide individuals notice prior to the collection of information. The system has a government-wide SORN, GSA/GOVT-4. National Privacy Program (NPP) publishes all final privacy documents on agency's Privacy internet and intranet sites.

7.2 What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the collection or sharing of their information?

Users have provided the privacy act statement at the logging stage but cannot decline to provide PII information if they want to travel.

7.3 Privacy Impact Analysis: Related to Notice

Discuss how the notice provided corresponds to the purpose of the project and the stated uses. Discuss how the notice given for the initial collection is consistent with the stated use(s) of the information. Describe how the project has mitigated the risks associated with potentially insufficient notice and opportunity to decline or consent.

Privacy Risk:

Notices may not provide enough information for users to understand the full uses of their information.

Mitigation:

There is a notification procedure outlined in the government-wide SORN, GSA/GOVT-4. There is a Systems Warning Notice presented to the Concur users each time they access Concur. There is a Privacy Act Statement presented when users log in.

Section 8.0 Redress

The following questions seek information about processes in place for individuals to seek redress which may include access to records about themselves, ensuring the accuracy of the information collected about them, and/or filing complaints.

8.1 What are the procedures that allow individuals to access their information?

Individuals seeking access to information about themselves in this system of records are required to provide adequate identification (e.g., driver's license, military identification card, employee badge, or identification card). Additional identity verification procedures may be required, as warranted. Requests must meet the requirements of EPA regulations that implement the Privacy Act of 1974, at 40 CFR part 16.

8.2 What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?

Privacy Act Request Procedure. Complete EPA Privacy Act procedures are described in EPA's Privacy Act regulations at 40 CFR part 16. Requests for correction or amendment must identify the record to be changed and the corrective action sought.

8.3 Privacy Impact Analysis: Related to Redress

Discuss what, if any, redress program the project provides beyond the access and correction afforded under the Privacy Act and FOIA.

Privacy Risk:

Individuals' records could be provided to the incorrect requestor.

Mitigation:

EPA's Privacy Act request process ensures the requestor is identity proofed and authenticated to support Privacy Act and/or FOIA requests. The EPA procedure applies only to records the EPA may maintains on that individual, a minor or their legal ward.