ConcurGov
Privacy Impact Assessment

17-July-2019

Version 1.09

Overview

SAP Concur's application, "ConcurGov," is a Web-based, end-to-end travel management system used to plan, authorize, arrange, process, and manage official Federal travel. ConcurGov enables travelers and/or travel arrangers to plan and make reservations (air, rail, lodging, car rental, etc.) online, prepare travel authorizations and vouchers online, produce itineraries, have tickets issued, and store receipts online. In meeting these objectives, ConcurGov collects user data and uses such data in accordance with the GSA E-Gov Travel Services 2.0 (ETS2) Contract, GS-33F-Y0026 awarded to SAP Concur (the "GSA ETS2 Master Contract" or "ETS2"). Only data that is necessary to fulfill travel and expense processing is collected or processed by ConcurGov, and such data is used and transmitted to third parties only in direct support of required activities. In addition, ConcurGov is operated, and designed to safeguard the data it collects, in accordance with the ETS2 Master Contract, which includes requirements to comply with NIST 800-53 Rev. 4 at the Moderate impact level, the PCI-DSS standards, and the Privacy Act, among others.

System Qualification

1. Does your system collect any information in identifiable form (personal data) on the general public? (If "Yes", a System Assessment is required.)
   - No
2. Does your system collect any information in identifiable form (personal data/information) on government employees? (If "Yes", a System Assessment is required.)
   - Yes
3. Has a PIA been done before for the system?
   - Yes. March 28, 2016.

Authorities and Other Requirements

1. What specific legal authorities and/or agreements permit and define the collection of information by the application in question?
   - The GSA ETS2 Master Contract with SAP Concur, GS-33F-Y0026, permits the collection of the information.
2. What Privacy Act System of Records Notice(s) - SORN(s) applies to the information?
   - GSA's Government-wide Contracted Travel Services Program or "E-Travel" SORN (GSA/GOVT-4) covers the systems.
   - In addition, ConcurGov displays the following Privacy Act notice to users at the time of login to ConcurGov:

“********PRIVACY ACT NOTICE**********

This system contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93-579). Any privacy information displayed on the screen or printed must be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary actions, a fine of up to $5,000, or both.

“The information requested in the ConcurGov is collected pursuant to Executive Order 9397 and Chapter 57, Title 5 United States Code. The purpose of the collection is to establish a comprehensive travel services system which enables travel service providers to authorize, issue, and account for travel and travel reimbursements provided to individuals on official Federal Government business. Categories of records in the system records may include: Full name matching the form of ID used for travel; Social Security Number; employee identification number; home, office, agency and emergency contact information; travel and hotel preferences; current passport and/or visa number(s); credit card numbers and related information; bank account information; frequent traveler account information (e.g., frequent flyer account numbers); date of birth; gender; DHS redress and known traveler numbers (numbers DHS assigns to promote resolution with previous watch list alerts and facilitate passenger clearance, respectively); trip information (e.g., destinations, reservation information); travel authorization information; travel claim information; monthly reports from travel agent(s) showing charges to individuals, balances, and other types of account analyses; and other official travel related information.

Routine uses which may be made of the collected information and other financial account information in the system(s) of record entitled "Contracted Travel Services Program GSA/GOVT-4" are: (a) To another Federal agency, Travel Management Center (TMC), online booking engine suppliers and the airlines that are required to support the DHS/TSA Secure Flight program. (b) To a Federal, State, local, or foreign agency responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order, where agencies become aware of a violation or potential violation of civil or criminal law or regulation; (c) To another Federal agency or a court when the Federal Government is party to a judicial proceeding; (d) To a Member of Congress or a congressional staff member in response to an inquiry from that congressional office made at the request of the individual who is the subject of the record; (e) To a Federal agency employee, expert, consultant, or contractor in performing a Federal duty for purposes of authorizing, arranging, and/or claiming reimbursement for official travel, including, but not limited to, traveler profile information; (f) To a credit card company for billing purposes, including collection of past due amounts; (g) To an expert, consultant, or contractor in the performance of a Federal duty to which the information is relevant; (h) To a Federal agency by the contractor in the form of itemized statements or invoices, and reports of all transactions, including refunds and adjustments to enable audits of charges to the Federal Government; (i) To a Federal agency in connection with the hiring or retention of an employee; the issuance of security clearance; the reporting of an investigation; the letting of a contract; or the issuance of a grant, license, or other benefit to the extent that the information is relevant and necessary to a decision; (j) To an authorized appeal or grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee to whom the information pertains; (k) To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), or the Government Accountability Office (GAO) when the information is required for program evaluation purposes; (l) To

officials of labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions; (m) To a travel services provider for billing and refund purposes; (n) To a carrier or an insurer for settlement of an employee claim for loss of or damage to personal property incident to service under 31 U.S.C. § 3721, or to a party involved in a tort claim against the Federal Government resulting from an accident involving a traveler; (o) To a credit reporting agency or credit bureau, as allowed and authorized by law, for the purpose of adding to a credit history file when it has been determined that an individual's account with a creditor with input to the system is delinquent; (p) summary or statistical data from the system with no reference to an identifiable individual may be released publicly; (q) to the National Archives and Records Administration (NARA) for records management purposes; (r) to appropriate agencies, entities, and persons when (1) The Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. Information requested is voluntary, however, failure to provide the information may nullify the ability to book online travel reservations."

***************************PRIVACY ACT NOTICE*************************

3. Has a System Security Plan (SSP) been completed for the information system(s) supporting the application?

   - Yes, a System Security Plan (SSP) was last approved by the Government as of June 10, 2016. The SSP is currently being updated.

4. Does a records retention schedule approved by the National Archives and Records Administration (NARA) exist?

   - Yes, 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/, this Master Contract, and IRS regulations as applicable. The applicable schedule is NARA General Records Schedule 01.1/010 (DAA-GRS-2013-0003-0001.
   - The records retention schedule coincides with Government fiscal year—October 1 through the following September 30—for dating and retention of records.
   - The records retention and archiving scheme is documented in SAP Concur's ETS2 Data Management Plan.
   - Controls are in place to prevent the purging of historical records prior to the proper retention period, and permit purging only of those records authorized for disposal by the NARA per 36 CFR 1228 and 1234.

5. 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.

- In accordance with the GSA ETS2 Master Contract, the ConcurGov application verifies the identity of the user and the integrity of electronic content in order to be compliant with the Government Paperwork Elimination Act (GPEA).

Section 2.0 Characterization of the Information

1. Identify the information the application collects, uses, disseminates, or maintains.

   - ConcurGov collects, uses, processes, and maintains data related to official Federal business travel, including information regarding travel planning, authorization, reservations, ticketing, fulfillment, expense reimbursement, and travel management reporting. Types of information include travel profile traveler preferences (including rental car class, seating preferences, ticketing preferences, hotel preferences, travel program affiliations, etc.), expense and financial information travel itinerary, travel vouchers and approvals, among other things. A complete list of the standard data elements maintained by ConcurGov are detailed in the GSA ETS2 Master Contract Section C, Attachment 14.
   - ConcurGov maintains Personally Identifiable Information (PII). The type of PII collected by ConcurGov and the functions that collect it are recorded in Section 3.0, Table 1 - PII Mapped to Components.

2. If the application or system creates new information (for example, a score, analysis, or report) describe how this is done and the purpose of that information.

   - N/A

3. If the application receives information from another system, such as a response to a background check, describe the system from which the information originates, including what information is returned and how it is used.

   - ConcurGov receives information from the Global Distribution System (GDS), which is a system containing information about availability, prices, and related services for airlines, car rental companies, hotel companies, rail companies, and suppliers, and through which reservations can be made and tickets can be issued. The information is received from the GDS through individual Passenger Name Records (PNRs), which allow travel information to populate appropriate travel documents. This information is used to ensure complete information is available to the traveler and approvers for appropriate review, as well as Government-required reporting.
   - Enterprise Application Integration (EAI) is used with agency systems to exchange authorization and voucher document information, and provide document status updates for authorization and vouchers through the agency's financial systems.
   - SAP Concur also receives data from SmartPay2 and SmartPay3 vendors in order to capture credit card transactional data to assist in credit card reconciliation reporting.

4. What are the sources of the information and how is the information collected for the application?

   - Data is submitted into ConcurGov by agency travelers, agency administrators, agency approvers, or agency travel arrangers, in accordance with agency policy and permissions. Traveler profile information may be uploaded by mass import into ConcurGov at the request of the agency.
   - SAP Concur works with each customer agency to establish appropriate user roles with correct

permissions and then assigns the correct user roles through a profile data import for each Federal employee who will have access to the ConcurGov. Federal Agency Travel Administrators (FATAs) with defined access maintain the user profiles after implementation.

- Federal agency business systems interface with ConcurGov for proper recording of authorizations and vouchers. Data is exchanged between systems and is documented in an Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU). The agency business systems do not have direct access to ConcurGov databases.

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

   - Yes, ConcurGov receives information from the Global Distribution System (GDS), which is a system containing information about availability, prices, and related services for airlines, car rental companies, hotel companies, rail companies, and suppliers, and through which reservations can be made and tickets can be issued. The information is received from the GDS through individual Passenger Name Records (PNRs), which allow travel information to populate appropriate travel documents. This information is used to ensure that complete information is available to the traveler and approvers for appropriate review, as well as Government-required reporting. ConcurGov receives rail schedule and pricing information directly from Amtrak, and flight information directly from Southwest, where reservations are made and tickets are issued. SAP Concur also receives data from SmartPay2 and SmartPay3 vendors in order to capture credit card transactional data to assist in credit card reconciliation reporting.

6. Discuss how accuracy of the data is ensured.

   - The customer and its users are responsible for ensuring the accuracy of data submitted within the ConcurGov system. SAP Concur personnel will only alter customer information when requested by authorized personnel from the customer via customer support case, implementation project, or special project request, which is documented for tracking purposes. ConcurGov is designed such that it can prevent the entry of invalid government travel charge card information (e.g., charge card number) within ConcurGov. ConcurGov performs data validation at the time of entry, which prevents inaccurate information from being entered and saved in error. The GDS will validate traveler's names with their frequent traveler information to prevent errors and if there is a problem, users will be notified via application error that they will need to resolve before being able to book travel.

7. Privacy Impact Analysis: Related to Characterization of the Information

   Privacy Risk:

   - Implementation and management of procedural controls not completed correctly or completely.
   - Failure to provide appropriate notifications in the event of unauthorized access or use of data.
   - Failure to implement and properly manage access controls to the data.

   Mitigation:

   - The system is designed to implement security and privacy controls at the FISMA Moderate

security categorization level. The ETS2 contract specifies certain data fields that meet the definition of PII under the ETS2 Master Contract. SAP Concur has implemented encryption of data at rest and in transit for these fields throughout the ConcurGov system. System and application logs are collected and monitored.

- Procedural controls are implemented by agencies to ensure that data is appropriately protected commensurate with its sensitivity. Application of these local policies and procedures will minimize that risk that users at a site can read, copy, alter, or steal printed or electronic information for which they are not authorized, and will require that only authorized user's pick up, receive, or deliver input and output information and media. Warning banners are displayed at login to ConcurGov to all users to warn them that ConcurGov is For Official Use Only and that it contains information covered in the Privacy Act of 1974. These warning banners must be acknowledged by the user prior to the user logging in to ConcurGov. The warning banners advise users of their obligations to protect the application and data it contains in accordance with Federal policy.
- Warning individuals with appropriate access about the misuse of data will be accomplished through agency policy. In addition, there are technology controls, such as auditing, in place that will reveal the misuse of data in a timely manner.
- Federal Agency Travel Administrators (FATAs) grant access controls on a need-to-know basis. These are periodically reviewed and updated. Logs are audited for inappropriate or unauthorized activity.
- Charge card numbers that are stored in the profiles are encrypted and cannot be viewed in ConcurGov.

Section 3.0 Uses of the Information

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

1. Describe how and why the application uses the information:
    - ConcurGov is an end-to-end travel management service that is used to plan, authorize, arrange, process, and manage official Federal travel. ConcurGov's end-to-end travel automation consists of fully integrated travel booking and travel management functions, including user profile management, fulfillment, ticketing, ticket tracking, quality control, expense filing, data consolidation and reporting, with links to enterprise resource providers and financial management systems.
    - ConcurGov maintains and uses information in order to meet current and future government travel requirements and needs for the purpose of recording travel information provided by the user to create travel itineraries, reserve any method or mode of travel accommodations, and claim entitlements and allowances prescribed in applicable Federal travel regulations. The purpose of the collection of this information is to establish a comprehensive travel services system that enables travel service providers under contract with the Federal government to authorize, issue, and account for travel and travel reimbursements provided to individuals on official Federal government business. Routine uses of the information are outlined in the Privacy Act notice represented within this document.
    - ConcurGov consists of two key components. The type of PII collected by each component of

ConcurGov, the functions that collect it, and the purpose of the collection/how it will used are recorded in Table 1 - PII Mapped to Components.

Table 1 - PII Mapped to Components

Components	Does this function collect or store PII? (Yes/No)	Type of PII	Reason for Collection of PII	Safeguards
SAP Concur Travel (Travel) – reference GSA Master Contract Section C Attachment 14	Yes	Traveler Information	ConcurGov system access; booking travel/trips	In place in accordance with the ETS2 contract
Travel Authorization and Voucher (TAVS) (Expense) – reference GSA Master Contract Section C Attachment 14	Yes	Traveler expense Information	Travel expense payment and reimbursement	In place in accordance with the ETS2 contract

2. Does the application use technology to conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly? If so, state how GSA plans to use such results.

   - No

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

   - User roles are defined from the user interface to the database.

4. Privacy Impact Analysis: Related to the Uses of Information

   Privacy Risk:

   - Unauthorized usage of or access to data stored within ConcurGov application.

   Mitigation:

   - ConcurGov is configured with appropriate safeguards and controls designed to limit access and use of the data stored therein.
   - Mobile device support for ConcurGov is designed to manage data in accordance to NIST 800-122 and 800-124.

Section 4.0 Notice

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

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

   ConcurGov displays the following notices in accordance with the GSA ETS2 Master Contract:

   - The Privacy Act Notice, set forth in Section 1.2 above, is displayed to the user before login.
   - The following Federal information system warning at the time of login:

   ****************WARNING***************

   This is a U.S. Federal Government information system that is "FOR OFFICIAL USE ONLY."

   Unauthorized access is a violation of U.S. Law and may result in criminal or administrative penalties. Users shall not access other users' or system files without proper authority. Absence of access controls IS NOT authorization for access! Information systems and equipment related to the E-Gov Travel Service are intended for communication, transmission, processing, and storage of U.S. Government information. These systems and equipment are subject to monitoring by law enforcement and authorized officials. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by law enforcement and authorized officials. Use of this system constitutes consent to such monitoring.

2. What opportunities are available for individuals to consent to uses, decline to provide information, or opt out of the application?

   - The Federal Information System Warning set forth in Section 4.1 above specifies that use of ConcurGov constitutes a user's consent to such monitoring. The Privacy Act notice advises of the uses for the information collected and notes that "Information requested is voluntary; however, failure to provide the information may nullify the ability to book online travel reservations."

3. Privacy Impact Analysis: Related to Notice

   Privacy Risk:

   - Failure to maintain a clear and concise understanding of the use of the personal data, how it is processed and stored through the notification of policy to all users.

   Mitigation:

   - The appropriate banners (including the Privacy Act Notice and Federal information system warning) appear in their entirety at the login page to ConcurGov: https://cge.concursolutions.com/

Section 5.0 Data Retention by the Application

The following questions are intended to outline how long the application retains the information after the initial collection.

1. Explain how long and for what reason the information is retained.
    - SAP Concur retains information in accordance with the contractual requirements within the ETS2 contract as per the NARA guidelines, as documented in SAP Concur's Data Management Plan, a contract deliverable that may be made available for viewing by the GSA PMO .

Section 6.0 Information Sharing

The following questions are intended to describe the scope of the application information sharing external to the agency. External sharing encompasses sharing with other Federal, State and Local government and private sector entities.

1. Is information shared outside of GSA as part of the normal agency operations? If so, identify the organization(s) and how the information is accessed and how it is to be used.
    - Unless otherwise authorized by a customer, SAP Concur does not disclose data to unauthorized third parties.
    - The Master Contract calls for data generated by and/or stored in the system to be transmitted to GSA or third-party vendors designated by GSA, including the Travel Management Information Service (MIS).

2. Describe how the external sharing noted in 6.1 is compatible with the SORN noted in Section 1.2.
    - The information described above is provided to a contractor for accumulating reporting data in accordance with the Privacy Act Notification.

3. Does the application place limitations on re-dissemination?
    - No

4. Describe how the application maintains a record of any disclosures outside of the Agency.
    - SAP Concur maintains records and processes to appropriately identify any unauthorized disclosures should one occur and will handle such unauthorized disclosure by directly working with affected agency customers and the GSA PMO ISSO as outlined in the ETS2 Incident Response Plan.

5. Privacy Impact Analysis: Related to Information Sharing.

    Privacy Risk:

    - Sharing information could result in release of PII and/or inappropriate use of the information.

    Mitigation:

    - Where data is shared, an Interconnected Service Agreement (ISA) and Memorandum of Understanding (MOU) is in place. The system provides a warning about proper uses of the information and a warning

about unauthorized use/transmission/etc.

Section 7.0 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.

1. What are the procedures that allow individuals to access their information?
   - Each user/data subject has the right to ask for their personal information maintained in ConcurGov from the Customer/Controller Admin (who is designated by each agency customer and assigned by SAP Concur in coordination with such agency customer). Users may request the information within their profiles and/or corrections to this information from their agencies. In response to such request, SAP Concur will coordinate with the agency to provide a report to the users/data subject detailing his/her personal information maintained in ConcurGov.
   - Users with access to the ConcurGov platform also have the ability to view and update their personal information in the user interface (UI) via their Traveler Profile.

2. What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?
   - As outlined in Section 7.1 above, users may request the agency provide the information within their profile and/or correct information. Users with access have the ability to update their personal information within ConcurGov.

3. How does the application notify individuals about the procedures for correcting their information?
   - Each customer agency has different processes and procedures for data correction. Agencies can post notifications to end-users within ConcurGov and provide direction through configuration settings. When a user makes updates within ConcurGov, a user receives a notification confirming the updated information. If the correction is made via a Support request, a written confirmation of the update will be sent to the user. ConcurGov provides notifications via email to users to notify them that profile information was changed.

4. Privacy Impact Analysis: Related to Redress

   Privacy Risk:
   - The inability to access and update personal information maintained in ConcurGov.

   Mitigation:
   - This is mitigated by the controls outlined above in this section.

Section 8.0 Auditing and Accountability

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

1. How does the application ensure that the information is used in accordance with stated practices in this PIA?

   - ConcurGov has designed access controls to protect data in motion and data at rest against intruders and other unauthorized personnel. In addition, detective controls are designed to alert SAP Concur personnel of any unusual or improper activity that could represent attempts to steal or destroy sensitive data maintained in ConcurGov.
   - ConcurGov undergoes audits and validation of controls as required in the ETS2 contract; to include, but are not limited to FISMA, SOC, and internal assessments. SAP Concur will monitor, track and provide corrective activities if needed to resolve any deviations from the requirements outlined in the GSA ETS2 Master Contract.
   - SAP Concur has implemented a control framework that has been founded on the controls required to comply with the Federal Information Security Management Act (FISMA). Security controls maintenance will be managed through internal and external audits of the operating environment to determine if the security controls in the information system continue to be effective.

2. Describe what privacy training is provided to users either generally or specifically relevant to the application.

   - SAP Concur requires that all appropriate SAP Concur employees receive annual security training and other training as required by the ETS2 Master Contract and other applicable requirements. SAP Concur maintains privacy and security awareness training records for its employees that are available to the GSA PMO.

3. What procedures are in place to determine which users may access the information and how does the application determine who has access?

   - Agencies and user roles are added and assigned within ConcurGov. Permission levels for each role will be set by the agency. Each agency may configure ConcurGov so that a user's access to view other users' information is restricted.
   - Agencies may configure ConcurGov to include roles necessary to support business processes. SAP Concur may propose additional roles and use cases that it deems appropriate to provide the most effective model for ConcurGov and ETS2.
   - ConcurGov supports establishment of user accounts with specific permissions and access rights to include the following:
     - The ability for travel arrangers to edit travel preferences and profiles for travelers, as well as access to their travel documents. Travel arrangers will have views that are filtered to show documents that they have arranged.
     - The ability for the customer agency to create multiple tiers of system administrative access
     - Administrative user access as appropriate.
   - ConcurGov provides non-Government travelers who are authorized by a Government sponsor the ability to register within ConcurGov and route their registration to the appropriate Government representative for account approval to support invitational travel. ConcurGov provides a filter for travel arrangers to view documents they have arranged.

- SAP Concur can report account usage of ConcurGov on request to customers so they can review and identify adjustments to accounts.

4. How does the application review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within GSA and outside?

   - ISAs, MOUs, new uses of the information, and organization access to the system are coordinated with GSA in accordance with the ETS2 contract.

E-Gov Travel-Concur Government Edition F