National Aeronautics and Space Administration

Privacy Impact Assessment (PIA)

PIA Entry Name: NASA E-Gov Travel Services Records

Enterprise Applications Management Office

NASA Point of Contact: Melissa Huzar

Phone Number: 256.961.9686

E-mail: melissa.a.huzar@nasa.gov

PURPOSE OF THE PRIVACY IMPACT ASSESSMENT

The National Aeronautics and Space Administration (NASA) Privacy Impact Assessment (PIA) documents and describes the personally identifiable information (PII) NASA collects and the purpose(s) for which it collects that information; how it uses the PII internally; whether it shares the PII with external entities, and the purposes for such sharing; whether individuals have the ability to consent to specific uses or sharing of PII and how to exercise any such consent; how individuals may obtain access to the PII; and how the PII will be protected. NASA publishes its PIAs, as well as its System of Records Notices (SORNs), on the NASA public-facing website, which describes NASA's activities that impact privacy, the authority for collecting personally identifiable information (PII), and the procedures to access and have PII amended or corrected if necessary.

Reviewing Official: Stayce Hoult, Chief Privacy Officer

System Overview:

NASA utilizes SAP Concur Government Edition (CGE)-E-Gov Travel Services 2 (ETS2), which Is a government-wide, web-based, end-to-end travel management service that has consolidated and automated travel management. The result will be an end-to-end travel service on the desktop of every NASA traveler, for processing their voucher, as well as, supporting all phases of travel from planning, authorizations and reservations. The ETS2 provides an automated end-to-end travel system facilitating further stabilization that complies with OMB mandates and Federal Travel Regulations, provides Federal travel processes, on-line reservations, and travel management expertise. It integrates to NASA's Financial, Human Capital, and Identity, Credential, and Access Management (ICAM) systems. It supports mobile platforms for mobile devices allowing creation of reservations, approvals, as well as electronic receipting. It filters listing of available expenses ensuring only agency policy-compliant expenses are chosen. It provides the capability to support NASA's current business processes and provides enhanced reporting capabilities.

Privacy / Authorities and Other Requirements	
List all legal authorities and/or agreements that permit the collection of privacy information by the project. Explain how these authorities permit the project and the collection of privacy information. If the project collects Social Security numbers, also identify the specific statutory authority allowing it.	NASA utilizes SAP Concur provided by General Services Administration (GSA). Authorities include the following: GS-33F-Y0026 and 5 USC Ch. 57: TRAVEL, TRANSPORTATION, AND SUBSISTENCE.
The records in the system are covered by an existing published System of Records Notice (SORN).	Existing SORN applicable
The SORN Name and Number.	GSA/GOVT-4 NASA 10 Core Finanacial Management Records (CFMR)

Privacy Act of 1974 / Uses of the Information	
Records on individuals are or will be routinely retrieved from the system by using individual's name or other unique identifier (e.g., personal account number, UUPIC, SSN, etc. is used to locate information about an individual in the application/website/information system/paper record).	Yes

Paperwork Reduction Act / Characterization of the Information	
The record/application/website/information system collects information in a standard way (via forms, surveys, questionnaires, etc.) from 10 or more persons (e.g., members of the public and NASA contractors, and grantees).	No

Paperwork Reduction Act / Authorities and Other Requirements	
There is an OMB Control Number.	No
The OMB Control Number.	

Privacy / Characterization of the Information	
Information is collected on the following:	NASA Contractors Government Employees Members of the public (excluding contractors and partners)
Collection contains the following:	Name Date of birth Miscellaneous identification numbers (accounts, permits, etc.) Passport number Work phone number Work cell phone number Personal cell phone number UUPIC Agency User ID (AUID) Work e-mail address Personal e-mail address School e-mail address Home mailing address Financial account information Work Mailing Address Home Phone Number
The collection is the minimum necessary to accomplish the purpose of the collection.	Yes
Discuss the intra-Departmental sharing of information. Identify and list the name(s) of any components or directorates within the Department with which the information is shared.	NASA employee PII is only shared with authorized personnel within that organization who have access to PII data for the purpose of creating user accounts, managing travel services, authorizations, vouchers and expense reimbursements, and ensuring compliance with Federal and travel agency reporting requirements.

Privacy / Uses of the Information	
NASA will use the information in the following ways:	To establish a comprehensive beginning-to-end travel services system containing information to enable travel service providers under contract to the Federal Government to authorize, issue, and account for travel and travel reimbursements provided to individuals on official Federal Government business.
The application/website/information system stores, collects, or maintains Information in Identifiable Form (IIF).	Yes

Consent / Notice	
Does the project provide individuals notice prior to the collection of information?	Yes
If no, explain why individuals are not notified prior to collection of information.	
If yes, describe how the notice provided for the collection of information is adequate to inform those impacted.	Warning banners are displayed at ConcurGov login 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 before the user logs in to ConcurGov. The warning banners advise users of their obligations to protect the application and data it contains in accordance with Federal policy.
Do individuals have opportunities to decline to provide information, or opt out of the project?	Yes
If yes, describe the process. If this is not an option, explain why not.	The agency head or his/her designee may grant an individual case by case exception to required use of your agency's current TMS or to required use of ETS once it is fully deployed within the agency, but only when travel meets one of the following conditions: (1) Such use would result in an unreasonable burden on mission accomplishment (e.g., emergency travel is involved and TMS/ETS is not accessible; the traveler is performing invitational travel; or the traveler has special needs or requires disability accommodations in accordance with part 301–13 of this chapter). (2) Such use would compromise a national security interest. (3) Such use might endanger the traveler's life (e.g., the individual is traveling under the Federal witness protection program, or is a threatened law enforcement/investigative officer traveling under part 301–31 of this chapter). (b) Any exception granted must be consistent with any contractual terms applicable to your current TMS or ETS, once it is fully deployed, and must not cause a breach of contract terms.
Do individuals have opportunities to consent to specific/targeted uses of their information?	Yes
If yes, describe the process. If this is not an option, explain why not	The Federal Information System Warning specifies that use of ConcurGov constitutes a user’s consent to such monitoring.
The IIF is collected	Voluntary
There is a process in place for the following:	
Ensuring consent is obtained from the individuals whose IIF is stored, collected, or maintained.	Yes

Are individuals provided with notice that they have opportunities to consent to uses, decline to provide information, or opt out of the project?	Yes
If yes, describe the process. If no, explain why not.	The Federal Information System Warning 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.
Are individuals notified of the consequences of providing information?	Yes
If yes, describe the process. If no, explain why not.	Warning banners are displayed at ConcurGov login 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 before the user logs in to ConcurGov. The warning banners advise users of their obligations to protect the application and data it contains in accordance with Federal policy.

Data Retention	
Explain how long each type of information is retained. Include a justification for the retention period of each information type and how/why that period is necessary to the mission/project.	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 before the proper retention period, and permit purging only of those records authorized for disposal by the NARA per 36 CFR 1228 and 1234.

Information Sharing	
Is information shared outside of the organization as part of the normal agency operations?	Yes

Identify who the information is shared with, how the information is accessed, and how it is to be used.	Other Federal Agecnies: Disclosures may be made to the Department of the Treasury to process payment of claims or recover debts owed to the government; the General Services Administration to provide reports or records related to transactions, refunds or adjustments, or to enable audits related to travel services and management of the system of records; the State Department pertaining to passports; another Federal agency or a court when the Federal Government is party to a judicial proceeding; to other agencies and entities when it is suspected that the records have been compromised and NASA determines there is a risk of harm to individuals and it is necessary to share information in order to prevent or remedy such harm; and as permitted under the routine uses identified in GSA/GOVT-4. Tribal, State or Local Agencies: Information may be shared with a Tribal, State, local, territorial, 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, or when it is relevant or necessary to the hiring, firing or retention of an employee orcontractor, or the issuance of a security clearance, license, contract, grant or other benefit. See GSA/GOVT-4. Contractor: Information may be shared with contractors, experts or consultants to perform official functions, provide support for travel services or audits, process travel or travel claims, or for billing and refunds. Individuals traveling that decline to provide their PII information when booking a flight will need to contact the Travel Management Center (TMC) to collect the information and forward it to the airline. Employee PII is forwarded to the TMC to book airline tickets. The employee's flight arrangements cannot be completed without the required PII, including name, date of birth, known traveler ID (where applicable), government travel charge card information and gender, which are used to issue tickets and finalize the flight itinerary. See GSA/GOVT-4 Other Third Party Sources: Disclosures may be made to commercial travel services and travel charge card vendors to facilitate travel and travel claims; consumer reporting agencies pertaining to travel card applicants and to facilitate debts owed to the government; TMC to provide employee name, date of birth and gender information to the airlines to finalize flight arrangements for the

	employee traveling; and other organizations as permitted under the routine uses identified in GSA/GOVT-4
Describe how the external sharing noted in the previous question is compatible with the SORN noted in PIA-02.	External sharing noted in previous question aligns with SORNs "Routine Uses of Records Maintained in the System, Including Categories of Users and the Purposes of Such Uses."

Redress	
What are the procedures that allow individuals to access their information?	Users must complete a NASA Account Management System (NAMS) request for account access to ConcurGov. Information within the NAMS request includes name, username, duty station, and home address, and is submitted to the employee's supervisor for approval. Once approvals are obtained the account will be provisioned. User can then access their account and information using Concur web address which authenticates using agency userid via LaunchPad.
What procedures are in place to allow the subject individual to correct inaccurate or erroneous information?	Users can make updates to their individual profiles as necessary. If fields are locked for user update, users can submit a Change Request (CRQ) in the NASA Integrated Service Management (NISM) system requesting updates.
How does the project notify individuals about the procedures for correcting their information?	Users typically contact their Central Travel office for assistance with correcting information.. If additional assistance is required, the Center Travel Office will submit a CRQ in NISM. The Concur website includes a banner titled "Important Information" which suggests that if issues exist to first contact the Center travel office but it also provides contact information for Concur and the Travel Management Company as well. There is also a help section that will allow users to submit a help ticket to Concur.

Auditing and Accountability	
How does the project ensure that the information is used in accordance with stated practices in this PIA?	Access level restrictions, authentication, and least privileges are used to ensure users have access only to the data they are authorized to view. ConcurGov system administrators' access to the data is limited to those who have official responsibilities for managing ConcurGov data. Access is further governed by NASA IT security policy, including use of assigned passwords, limited access rules, various firewalls, and other protections put in place to assure the integrity and protection of any personal information. System administrators have access to audit reports on

	various aspects of the system's operating controls, including system functions and user actions. Sensitive data can only be accessed on the secure ConcurGov website. Users will not be able to access any personal or sensitive information via the mobile application. Computer records are protected by a password system that is compliant with NIST standards as specified in NIST SP 800-53, Security and Privacy Controls for Federal Information Systems and Organizations, and NIST SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems. The records contained in this system are safeguarded in accordance with applicable security rules and policies. Access to servers containing records in this system is limited to authorized personnel who have a need-to-know basis.
Describe what privacy training is provided to users either generally or specifically relevant to the project.	Users are required to take annual Cybersecurity and Privacy Awareness Training. 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.
What procedures are in place to determine which users may access the information and how does the project determine who has access?	User access is granted via NAMS request and submitted to ConcurGov by agency travelers, agency administrators, agency approvers, or agency travel arrangers, in accordance with agency policy and permissions. Federal Agency Travel Administrators (FATAs) grant access controls on a need-to-know basis. 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 ConcurGov. Federal Agency Travel Administrators (FATAs) with defined access maintain the user profiles after implementation.
How does the project review and approve information sharing agreements, MOUs, new uses of the information, new access to the system by organizations within the department and outside?	The Agency works with Concur and GSA to make any necessary updates to MOUs & ISAs. Approval is then required from Concur, GSA and Application and Platform Services (APS) Leadership. New access requests to the system within the Agency are submitted through NISM.

Security Controls / Characterization of the Information

Monitor and Response to privacy and/or security incidents policies.	Yes

Security Controls / Auditing and Accountability	
Technical controls (safeguards) are in place to minimize the possibility of unauthorized access, use, or dissemination of the IIF in the application/ website/ information system/ cloud system.	Yes
Access controls.	Yes

Information Sharing Practices / Characterization of Information	
The application/website/information system/cloud systems collects IIF from other resources (e.g., databases, websites).	No
The application/website/information system/cloud system populates data for other resources (e.g., databases, websites, or external agencies, people, or organizations).	No

Accessibility, Redress, Complaints / Characterization of the Information	
There is a process in place for periodic reviews of IIF in the system to ensure data integrity, availability, accuracy, and relevance.	Yes

Web Measurement and Customizing Technology / Characterization of the Information	
The Application/Website/Information System Utilizes Web Measurement and Customization Technology (Cookies/Persistent Tracking).	No

Agency Privacy Manager (APM):

Guerin, Michael D
HARRIS HOULT, STAYCE D
Kostka, Paul A
Midulla, Laura P
Montasser, Ali S
Scholz, Matthew C

APM Review Decision: Concur

APM Review Date: 04/23/2024

Chief Privacy Officer (CPO):

HARRIS HOULT, STAYCE D

CPO Review Decision: Concur

CPO Review Date: 03/03/2025

_____
CPO Digital Signature

NASA Senior Agency Information Security Officer (SAISO):

Witt, Michael

SAISO Review Decision: Concur

SAISO Review Date: 03/14/2025

NASA Senior Agency Official for Privacy (SAOP):

SEATON, JEFFREY M

SAOP Review Decision: Approve

SAOP Review Date: 03/21/2025