U.S. Department of the Interior
PRIVACY IMPACT ASSESSMENT

Introduction

The Department of the Interior requires PIAs to be conducted and maintained on all IT systems whether already in existence, in development or undergoing modification in order to adequately evaluate risks, ensure the protection of privacy information, and consider privacy implications throughout the information system development life cycle. This PIA form may not be modified and must be completed electronically; hand-written submissions will not be accepted. See the DOI PIA Guide for additional guidance on conducting a PIA or meeting the requirements of the E-Government Act of 2002. See Section 6.0 of the DOI PIA Guide for specific guidance on answering the questions in this form.

NOTE: See Section 7.0 of the DOI PIA Guide for guidance on using the DOI Adapted PIA template to assess third-party websites or applications.

Name of Project: ConcurGov
Bureau/Office: Office of the Secretary
Date: January 13, 2021
Point of Contact:
Name: Vany Kaiser
Title: Departmental Privacy Act Specialist
Email: DOI_Privacy@ios.doi.gov
Phone: (202) 208-1605
Address: 1849 C Street NW, Room 7112, Washington, DC 20240

Section 1. General System Information

A. Is a full PIA required?

☒ Yes, information is collected from or maintained on
- ☐ Members of the general public
- ☐ Federal personnel and/or Federal contractors
- ☐ Volunteers
- ☒ All

☐ No: *Information is NOT collected, maintained, or used that is identifiable to the individual in this system. Only sections 1 and 5 of this form are required to be completed.*

B. What is the purpose of the system?

The ConcurGov system is an end-to-end travel and expense management solution owned by Concur Technologies, which is used by the Federal government to reserve, book, authorize, and manage official travel. ConcurGov is available to Federal government agencies that provide both the Travel and Expense services, and automates the travel and expense management processes for agencies. Concur Technologies has a master contract with the General Services Administration (GSA) that permits the use of the ConcurGov application within the Federal government. Participating agencies create task orders that allow Concur Technologies to provide

the ConcurGov services.

ConcurGov uses a web application portal to communicate with system users and provide access to all travel management services. The web application allows users the ability to facilitate travel booking services; change travel reservations; use travel authorization and vouchering services to document trip approvals; obtain expense reimbursement; and provide accurate accounting of government travel records in compliance with Federal Travel Regulations.

ConcurGov also has a ConcurGov mobile application, which is an on-the-go option for the web version of ConcurGov. The ConcurGov mobile application may only be used by authorized DOI users with a ConcurGov user account. Users are able to capture their travel itineraries and have complete visibility into their bookings and travel expenditures. The mobile application provides access to content from multiple global travel distribution systems, negotiated and published prices, direct flights and web-only fares. Similar to the web version, the mobile application enforces compliance with DOI policies and external regulations.

The Department of the Interior (DOI) Office of Policy and Financial Management (PFM) is the system owner for ConcurGov for DOI. The DOI Business Integration Office (BIO) is responsible for the operations and maintenance of ConcurGov. Each DOI bureau and office is responsible for managing their own bureau/office records for their use of ConcurGov.

C. What is the legal authority?

31 U.S.C. 3511, 3512 and 3523; 5 U.S.C. Chapter 57; and implementing Federal Travel Regulations (41 CFR 300-304)

D. Why is this PIA being completed or modified?

☐ New Information System
☐ New Electronic Collection
☒ Existing Information System under Periodic Review
☐ Merging of Systems
☐ Significantly Modified Information System
☐ Conversion from Paper to Electronic Records
☐ Retiring or Decommissioning a System
☐ Other: *Describe*

E. Is this information system registered in CSAM?

☒ Yes: *Enter the UII Code and the System Security Plan (SSP) Name*

010-000000220; ConcurGov System Security and Privacy Plan

☐ No

F. List all minor applications or subsystems that are hosted on this system and covered under this privacy impact assessment.

Subsystem Name	Purpose	Contains PII *(Yes/No)*	Describe *If Yes, provide a description.*
None	None	No	N/A

G. Does this information system or electronic collection require a published Privacy Act System of Records Notice (SORN)?

☒ Yes: *List Privacy Act SORN Identifier(s)*

GSA has published a government-wide SORN, GSA/GOVT-4, Contracted Travel Services Program, 74 FR 26700 (June 3, 2009), which applies to Federal agency travel service records. Some records related to payment of travel expenses to employees maintained in DOI records may be covered under DOI-88, Travel Management: FBMS, 73 FR 43769 (July 28, 2008), SORNs. These SORNs may be viewed on the DOI SORN website at https://www.doi.gov/privacy/sorn.

☐ No

H. Does this information system or electronic collection require an OMB Control Number?

☒ Yes: *Describe*

The bureau/office travel voucher forms and worksheets require an OMB Control Number. Bureaus and offices are working with the Departmental Information Collection Clearance Officer to obtain OMB approval.

☐ No

Section 2. Summary of System Data

A. What PII will be collected? Indicate all that apply.

☒ Name
☒ Gender
☒ Birth Date
☒ Personal Email Address
☒ Home Telephone Number
☒ Credit Card Number
☒ Mailing/Home Address

☒ Other: *Specify the PII collected.*

Personally identifiable information (PII) is limited to the minimum necessary to identify travelers, provide travel services, and process travel claims. ConcurGov contains travel costs, vouchers and related information to process travel claims. DOI users are required to use only their government travel charge card for official travel. Travel charge card numbers are masked when entered into ConcurGov. Date of birth is required for booking flights and are also masked in the system. Social Security numbers are not entered or used in ConcurGov. Personal email address may be provided by travelers to receive itinerary updates. Home telephone numbers may be used by travelers as an alternative contact number.

Individuals with ConcurGov accounts are assigned an FBMS vendor number, which identifies the user and is entered into the ConcurGov user profile. FBMS is DOI's financial management system and the FBMS vendor number is used to provide payment to the user for travel expenses. The FBMS vendor number is also used to validate the user before travel payment is finalized. Without the vendor number, individual payments cannot be processed.

Users must complete the Department-wide ConcurGov Profile Maintenance form to request an account to access ConcurGov. The ConcurGov Profile Maintenance form collects name, username, duty station, and home address, and is submitted to the employee's bureau or office Federal Agency Travel Administrator or Bureau Security Administrator via email to create an account and profile. New user accounts cannot be created in the mobile application, accounts can only be created via the ConcurGov website. After an account is created, users will enter their username and password to access the website and mobile application.

Bureau-specific travel voucher forms or worksheets only collect PII needed to calculate travel claim expenses, such as the traveler name and travel expenses incurred, that are manually entered into ConcurGov.

B. What is the source for the PII collected? Indicate all that apply.

☒ Individual
☐ Federal agency
☐ Tribal agency
☐ Local agency
☒ DOI records
☐ Third party source
☐ State agency
☒ Other: *Describe*

A travel arranger works with Bureaus to create reservations, process documents and complete bureau specific travel voucher forms or worksheets that help claim expenses on behalf of an invitational traveler. An invitational traveler is a non-employee who travels on behalf of DOI where DOI is paying the traveler directly for the travel. This includes volunteers, experts, and many other types of non-employee travelers.

User profiles within FBMS are used for validation purposes and payment of individuals.

C. How will the information be collected? Indicate all that apply.

☒ Paper Format
☒ Email
☐ Face-to-Face Contact
☒ Web site
☒ Fax
☐ Telephone Interview
☒ Information Shared Between Systems
☒ Other: *Describe*

Paper Format – DOI users must submit a ConcurGov Profile Maintenance form to create a user account to log into the SAP ConcurGov website. Once the account is created, users can log into the website and mobile application to set up travel and lodging arrangements for official travel.

ConcurGov mobile application – Authorized DOI users will be able to reserve, book, review an itinerary, approve documents, capture and upload their receipts for travel and purchases using the mobile application.

Fax – Some Bureaus have secure fax machines set up to receive the ConcurGov Profile Maintenance form. The ConcurGov Federal Agency Travel Administrator or Bureau Security Administrator sends the form via email to individuals and then collects the completed form via fax.

Website – The DOI Office of the Chief Information Officer (OCIO), FBMS and SAP Concur established a secure web service connection as the primary connectivity method. Users authenticate via username/password at the perimeter of the ConcurGov network and connect to the DOI network. The ConcurGov website is used to plan, authorize, arrange, process, and manage official Federal travel (air, rail, lodging, car rental, etc.) for authorized users only. Users will manually enter travel data into the ConcurGov Website: https://cge.concursolutions.com/

Email – Users may submit their completed ConcurGov Profile Maintenance Form to their Bureaus via email to have the ConcurGov profile created for travel. Bureau System Administrators will receive the forms only to set up user profiles including a login and a temporary password for user accounts. The DOI Special Interest Group (SIGS) do not receive these forms.

D. What is the intended use of the PII collected?

The primary purpose for collecting PII is to create accounts in the ConcurGov system to manage travel authorization services and payment of claims to individuals for official Federal government business in support of the DOI's mission or business needs. ConcurGov helps DOI identify travelers, provide travel services, and process travel claims. An individual's PII is

collected during the DOI employee onboarding process, and the minimum required is used to establish employee accounts in ConcurGov for the purpose of managing official travel. All DOI users are assigned a vendor number in lieu of their Social Security number in ConcurGov, which is used to process travel payment through FBMS.

E. With whom will the PII be shared, both within DOI and outside DOI? Indicate all that apply.

☒ Within the Bureau/Office: *Describe the bureau/office and how the data will be used.*

Bureau employee PII is only shared with authorized personnel within that bureau/office 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.

DOI Office of Financial Management (PFM) Office has administrative access to ConcurGov and The Reporting tool Cognos. PFM builds reports used to support Freedom of Information Act (FOIA) requests and reporting to GSA, and management data calls, which may include PII data if required.

☐ Other Bureaus/Offices: *Describe the bureau/office and how the data will be used.*

☒ Other Federal Agencies: *Describe the federal agency and how the data will be used.*

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 DOI 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 or DOI-88 SORNs, which may be viewed at https://www.doi.gov/privacy/sorn.

☒ Tribal, State or Local Agencies: *Describe the Tribal, state or local agencies and how the data will be used.*

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 or contractor, or the issuance of a security clearance, license, contract, grant or other benefit. See GSA/GOVT-4 or DOI-88 SORNs for authorized routine uses of information: https://www.doi.gov/privacy/sorn.

☒ Contractor: *Describe the contractor and how the data will be used.*

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 or DOI-88 SORNs for authorized routine uses of information: https://www.doi.gov/privacy/sorn.

☒ Other Third Party Sources: *Describe the third party source and how the data will be used.*

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; online booking engine suppliers and the airlines that support the Department of Homeland Security/Transportation Security Administration (DHS/TSA) Secure Flight program to conduct pre-flight comparisons of airline passenger information; and other organizations as permitted under the routine uses identified in GSA/GOVT-4 or DOI-88 SORNs, which may be viewed at https://www.doi.gov/privacy/sorn.

F. Do individuals have the opportunity to decline to provide information or to consent to the specific uses of their PII?

☒ Yes: *Describe the method by which individuals can decline to provide information or how individuals consent to specific uses.*

ConcurGov allows individuals the option to consent to or decline the collection of personal information. Both the Profile Maintenance form and the system provide a Privacy Act statement informing users of the purpose and uses of their information. Employees who do not provide information at the time they establish their travel arrangements in ConcurGov will need to provide the required information to TMC. There are two TMC Duluth travel centers that are utilized by all bureaus and offices within the continental US, and El Sol is used for travelers with duty stations outside the continental US (AK, HI, US Virgin Islands, etc.). Name, date of birth, and gender information are required to issue airline tickets. Employees may refuse to provide information necessary to make travel arrangements, however, they will not be able to complete authorization and booking for official government travel.

☐ No: *State the reason why individuals cannot object or why individuals cannot give or withhold their consent. If no travel information not required if flying information is required for Airline.*

G. What information is provided to an individual when asked to provide PII data? Indicate all that apply.

☒ Privacy Act Statement: *Describe each applicable format.*

Individuals requesting ConcurGov accounts must submit a DOI ConcurGov Profile Maintenance form. The ConcurGov account request form includes a Privacy Act Statement.

A GSA ConcurGov Privacy Act Notice is posted at the ConcurGov login and mobile application. The Privacy Act Notice provides detailed information on the authority and purpose of collecting PII, how PII is used and with whom the PII is shared, the applicable routine uses under the GSA/GOVT-4 SORN, and the voluntary nature of the collection, as well as impacts for not providing information.

☒ Privacy Notice: *Describe each applicable format.*

Notice is provided through the publication of this PIA, and the GSA/GOVT-4 and DOI-88 SORNs, which may be viewed at DOI Privacy Program SORN website at https://www.doi.gov/privacy/sorn. GSA conducted a PIA for ConcurGov, which may be viewed at https://www.gsa.gov/cdnstatic/E-Gov%20Travel-Concur%20Government%20Edition_PIA_July2019.pdf

☒ Other: *Describe each applicable format.*

A Warning Banner is also displayed on the ConcurGov website and mobile application where employees log in: https://cge.concursolutions.com. Upon login, individuals are notified that their use of ConcurGov may be monitored.

☐ None

H. How will the data be retrieved? List the identifiers that will be used to retrieve information (e.g., name, case number, etc.).

DOI travelers can retrieve their own information manually by accessing the ConcurGov. DOI Administrators may access PII only if their role is assigned and permission is granted to access PII data. PII data stored in ConcurGov is masked and only certain roles and groups are granted access to the PII. Only assigned roles of Administrator and Arranger can use personal identifiers to retrieve bureau data in ConcurGov. The following personal identifiers can be used to retrieve data in the ConcurGov system:

- Employee First and Last Name
- Vendor Number (Traveler ID)
- Official Email Address
- User Login ID

For the ConcurGov mobile application, users can only retrieve basic travel information (itinerary, car rentals, authorizations, etc.). Users will not be able to retrieve any sensitive PII using the mobile application. This information can only be accessed using the ConcurGov website using their username and password.

I. Will reports be produced on individuals?

☒ Yes: *What will be the use of these reports? Who will have access to them?*

Reports generated from ConcurGov will be used to monitor the integrity of information within the GSA Electronic Travel System (ETS2), as well as the health of DOI's overall travel program. This includes reports to monitor user profiles and role assignments for accuracy and compliance with DOI profile creation standards and security policies. Expense reports are used to monitor spending, compliance with Department and Federal regulations and policies, and to identify and monitor trends. Reports can also be generated to see how funds are being used to prevent fraud, waste and abuse, but the details of the travel charge card transaction are not stored in ConcurGov.

Reports may also be used for DOI expense payment policies and research purposes (e.g., travel charge cards). Bureau administrators can pull reports to check individuals' travel locations. Travelers do not have access to generate reports. They only have access to view their own profile in ConcurGov. Only personnel with an assigned reporting role can generate reports.

☐ No

Section 3. Attributes of System Data

A. How will data collected from sources other than DOI records be verified for accuracy?

Individuals who submit ConcurGov Profile Maintenance forms to establish an account are responsible for the accuracy of the data they provide. Forms will be reviewed and approved by each traveler's manager to ensure accuracy and appropriate approvals. Data integrity checks will be performed by DOI Special Interest Groups (SIGs). As incoming and outgoing data is processed through the ConcurGov website, checks are conducted on non PII information. DOI SIGs do not have access to view PII data, but may have access to PII listed on the Profile Maintenance Form or provided by an employee to help with their travel arrangements. The ConcurGov system will conduct data integrity checks to ensure data accuracy. User data that conforms to the business rule and integrity checks will be processed. Non-conforming data entered by users will be posted to a suspense file for examination and resubmission upon correction.

In a few cases, travel charge card use and travel information are provided by third party vendors such as airlines and car rental companies. Travel arrangements completed in ConcurGov are provided to the third party vendors electronically. The PII about users included in the data

submitted by these vendors is presumed to be correct; any such PII is initially supplied directly by the employee to the third party vendor, so the data is deemed to be accurate.

B. How will data be checked for completeness?

Individuals submitting ConcurGov Profile Maintenance forms or submitting travel requests in ConcurGov are responsible for the completeness and accuracy of the data provided. In addition, bureaus and offices will be responsible for the management of their forms and ensuring data is complete for the travel reservation and authorization process. During creation of an employee's profile, the ConcurGov system will highlight any missing information. If the data is not entered during the creation of the individual profile, the profile for the traveler cannot be created. Bureau administrators will check to verify the information is complete, and will contact the travel arrangers to complete the setup of the account if there is any missing information. The travel arrangers will contact the employee via phone or email.

C. What procedures are taken to ensure the data is current? Identify the process or name the document (e.g., data models).

Data collected is from the employee users, bureaus, and offices. Employees are responsible for providing updated, current information to process travel arrangements, authorizations and vouchers. Supervisors are responsible for checking accuracy of travel authorizations and vouchers before approving them.

D. What are the retention periods for data in the system? Identify the associated records retention schedule for the records in this system.

ConcurGov data is covered under Departmental and bureau/office records schedules, or General Records Schedule (GRS) approved by the National Archives and Records Administration (NARA) for each type of record or form based on the subject or function and records series.

Travel Records: Departmental Records Schedules (DRS) 1.3 0011, Long-term Financial and Acquisition Management. These records have a temporary disposition and includes official government travel records with all supporting documents including travel orders and vouchers. Records are cut-off at the end of the fiscal year in which travel occurred and destroyed 7 years after the end of fiscal year in which the travel was done.

Information Technology Records: DRS 1.4 0013, System Maintenance and Use Records. These records have a temporary disposition. Records are cut-off when obsolete and destroyed no later than 3 years after cut-off.

Traveler profiles are deactivated when a user leaves the agency. Traveler profile data is maintained for the life of the profile, and will be retained for the life of the system or longer to meet agency needs, whichever is later.

E. What are the procedures for disposition of the data at the end of the retention period? Where are the procedures documented?

ConcurGov retains all records in accordance with the DRS records schedules identified above. Traveler and user profiles are deactivated when the user leaves the agency. Traveler profile data is maintained for the life of the profile, and will be retained for the life of the system or longer to meet agency needs, whichever is later.

Hard copy material will be disposed of by shredding or pulping, and records contained on electronic media will be degaussed or securely overwritten or turned in for destruction in accordance with NARA guidelines, 36 CFR 1228 and 1234.

F. Briefly describe privacy risks and how information handling practices at each stage of the "information lifecycle" (i.e., collection, use, retention, processing, disclosure and destruction) affect individual privacy.

There is a privacy risk associated with ConcurGov related to the collection, use, transfer, maintenance, and sharing of PII. A significant amount of PII is submitted by employees via form, website, and email. There is a privacy risk due to the sensitivity of PII data contained on the ConcurGov Profile Maintenance forms and ConcurGov, which may be inappropriately accessed or misused by DOI or ConcurGov personnel. In order to receive authorization to access PII data, DOI requires all its employees and service providers to take security, privacy awareness, and role-based training annually to ensure security and privacy compliance in accordance with Federal law and policy, and DOI information assurance and privacy policy. In addition, all users will be required to consent to the ConcurGov Rules of Behavior. To protect individual privacy, all DOI users are assigned a vendor number in lieu of their SSN in ConcurGov.

ConcurGov has undergone a formal Assessment and Authorization for issuance of an authority to operate in accordance with FISMA, and has been rated as a moderate system requiring strict security and privacy controls to protect the confidentiality, integrity, and availability of data in the system.

The use of DOI Information Systems is conducted in accordance with the appropriate DOI Security and Privacy Control Standards policy. An audit trail of activity will be maintained sufficient to reconstruct security relevant events. The BIO follows the least privilege security principle, such that only the least amount of access is given to a user to complete their required activity. ConcurGov can generate both usage and access reports that can be monitored by system administrators. All access is controlled by authentication methods to validate the authorized user and TMC has access to PII data for a limited time period.

Security and privacy controls are implemented and in compliance with the Privacy Act, Federal Information Security Modernization Act of 2014 (FISMA), OMB Circular A-130, *Managing Information as a Strategic Resource*, OMB Circular A-123, *Management's Responsibility for Internal Control*, and National Institute of Standards and Technology (NIST) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*. Access to the

ConcurGov website requires users to login with username and password to authenticate before access is granted. System access is granted to authorized personnel on a need to know basis. Different levels of access are assigned dependent on the role of the user. Unique user identification and authentication, passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels are assigned. In addition, network security configurations are built into the architecture of the system and fully implemented in accordance with NIST guidelines and Departmental policies. ConcurGov has multiple layers of security that protect content at the object level and can be applied to a user, a group of users, or set as a general feature. Some information may be stored in a central repository within the FBMS database. ConcurGov system infrastructure is hosted in a secure environment and the data is encrypted both in-transit and at rest. The ConcurGov website is secured with https connection security to protect information. As a Federal agency contractor, Concur Technologies is subject to all the Federal legal and policy requirements for safeguarding Federal information and is responsible for preventing unauthorized access to the system and protecting the data contained within the system.

For the ConcurGov mobile application, users will login using their ConcurGov account username and password. Once users login all DOI ConcurGov policies and restrictions apply. DOI does not use ConcurGov "Single sign-on (SSO) Company Code Sign In" option. Users can only retrieve basic travel information (itinerary, car rentals, authorizations, etc.) and will not be able to retrieve any sensitive PII using the mobile application. This information can only be accessed using the ConcurGov website with username and password. The ConcurGov mobile application does not store any sensitive data such as travel charge card information on a user's mobile device. DOI does not use Concur Locate and does not track employee geo-location while using ConcurGov mobile application.

There is a risk that data may be stored for longer than necessary. Records are maintained and disposed of under a NARA approved records schedule. User accounts containing PII that are inactive are disabled by system administrators, however, user created content is maintained as long as it remains active or as deemed necessary by DOI. Information collected and stored within the ConcurGov is maintained, protected, and destroyed in compliance with all applicable Federal laws, Executive Orders, directives, policies, regulations, standards, and operational requirements.

There is a risk users may not have adequate notice of the collection and use of their data. This is mitigated by the notices provided on the ConcurGov website, mobile application, and DOI forms that collect information, and the publication of this PIA, GSA ConcurGov PIA, the GSA/GOVT-4 and DOI-88 SORNs. A detailed Privacy Act Notice and Warning Banner are displayed on the ConcurGov website and mobile application where employees log in: https://cge.concursolutions.com. These notices provide information to individuals on how their PII will be used and shared and how they may seek notification, access, or amendment of their records.

Section 4. PIA Risk Review

A. Is the use of the data both relevant and necessary to the purpose for which the system is being designed?

☒ Yes: *Explanation*

ConcurGov is an enterprise-wide, web-based, end-to-end travel system that is used to plan, authorize, arrange, process, and manage official Federal travel. The required travelers' information is needed to process travel requests, claims, travel reimbursements, and ensure payment is processed and paid to the individual in a timely manner.

☐ No

B. Does this system or electronic collection derive new data or create previously unavailable data about an individual through data aggregation?

☐ Yes: *Explain what risks are introduced by this data aggregation and how these risks will be mitigated.*

☒ No

C. Will the new data be placed in the individual's record?

☐ Yes: *Explanation*
☒ No

D. Can the system make determinations about individuals that would not be possible without the new data?

☐ Yes: *Explanation*
☒ No

E. How will the new data be verified for relevance and accuracy?

Individuals will be required to enter new travel request data each time the users need to travel. Data is verified for relevance and accuracy when inputted. If information is missing, travel requests cannot be processed and completed until the individual inputs the missing data.

F. Are the data or the processes being consolidated?

☐ Yes, data is being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☐ Yes, processes are being consolidated. *Describe the controls that are in place to protect the data from unauthorized access or use.*

☒ No, data or processes are not being consolidated.

G. Who will have access to data in the system or electronic collection? Indicate all that apply.

☒ Users
☒ Contractors
☐ Developers
☒ System Administrator
☒ Other: *Describe*

ConcurGov system administrators and authorized users will have access to the data in ConcurGov. Access to information will be limited to authorized personnel who have a need-to-know to perform their official duties. Individuals who submit travel requests will have access only to the information and data they submit for their own accounts. ConcurGov administrators will have access only to the data obtained through the forms they manage for their organizations. Access to ConcurGov by system administrators, authorized program personnel, and contractors is based on least privileges and role-based access.

TMC has limited access to the travelers' PII information. The TMC only has access to the information when individuals decline to input the sensitive information in their travel request when making reservations for the airlines. The TMC will only have access to the employee name, date of birth, and gender in order to finalize flight information.

H. How is user access to data determined? Will users have access to all data or will access be restricted?

Access level restrictions, authentication, least privileges, and audit logs 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 DOI 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. Access to such

information is dependent on the performance of their official duties and requires a valid username and password. Unique user identification and authentication, such as passwords, least privileges and audit logs are utilized to ensure appropriate permissions and access levels.

I. Are contractors involved with the design and/or development of the system, or will they be involved with the maintenance of the system?

☒ Yes. *Were Privacy Act contract clauses included in their contracts and other regulatory measures addressed?*

Contractors are involved in the design and development of the system and Privacy Act clauses are included in all contractor agreements.

☐ No

J. Is the system using technologies in ways that the DOI has not previously employed (e.g., monitoring software, SmartCards or Caller ID)?

☐ Yes. *Explanation*
☒ No

K. Will this system provide the capability to identify, locate and monitor individuals?

☐ Yes. *Explanation*
☒ No

L. What kinds of information are collected as a function of the monitoring of individuals?

The system is not intended to monitor individuals; however, the system will have the ability to audit the usage activity in the system, including the use by system administrators, Departmental Manager, Bureau/Office Managers, and other resources. Audit information includes reviewable data such as login date and time. In addition, the system will monitor workflow, including monitoring the status of reviews of new and existing travel claims. In the event that review of system workflows reveals that reviews are not being performed in a timely fashion, the matter will be escalated.

M. What controls will be used to prevent unauthorized monitoring?

The system is not intended to monitor individuals; however, the system will have the ability to audit the usage activity in the system, including the use by system administrators, Departmental Manager, Bureau/Office Managers, and other resources. Audit information includes reviewable data such as login date and time. In addition, the system will monitor workflow, including monitoring the status of reviews of new and existing travel claims.

Firewalls and network security configurations are also built into the architecture of the system and NIST SP 800-53, *Security and Privacy Controls for Federal Information Systems*, and other DOI policies are fully implemented to prevent unauthorized monitoring. ConcurGov System administrators will review the use of the ConcurGov system and the activities of users to ensure that the system is not improperly used and to prevent unauthorized monitoring or access. BIO bureau System Administrators assigns roles based on the principles of least privilege and performs due diligence toward ensuring that separation of duties is in place.

Only authorized users with valid DOI credentials will be able to access the system. In addition, all users will be required to consent to the ConcurGov Rules of Behavior and complete Information Management Training awareness, Privacy Awareness, Records Management, Section 508 Compliance, and Controlled Unclassified Information (CUI) training before being granted access to the DOI network or any DOI system, and annually thereafter. Authorized users are also required to complete role-based privacy or security training based on their roles and responsibilities.

The ConcurGov website and mobile application users are presented a warning banner stating this is a "U.S Federal Government Information System "FOR OFFICIAL USE ONLY" and are informed that they are subject to monitoring by law enforcement and authorized officials to include all data communicated, transmitted, processed or stored in the system, and that individual use of the system is consent to the monitoring. ConcurGov also provides a Privacy Act Notice "This system contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93-579)".

N. How will the PII be secured?

(1) Physical Controls. Indicate all that apply.

☒ Security Guards
☒ Key Guards
☒ Locked File Cabinets
☒ Secured Facility
☒ Closed Circuit Television
☐ Cipher Locks
☒ Identification Badges
☐ Safes
☐ Combination Locks
☒ Locked Offices
☐ Other. *Describe*

(2) Technical Controls. Indicate all that apply.

☒ Password
☒ Firewall

☒ Encryption
☒ User Identification
☐ Biometrics
☒ Intrusion Detection System (IDS)
☒ Virtual Private Network (VPN)
☒ Public Key Infrastructure (PKI) Certificates
☒ Personal Identity Verification (PIV) Card
☐ Other. *Describe*

(3) Administrative Controls. Indicate all that apply.

☒ Periodic Security Audits
☒ Backups Secured Off-site
☒ Rules of Behavior
☒ Role-Based Training
☒ Regular Monitoring of Users' Security Practices
☒ Methods to Ensure Only Authorized Personnel Have Access to PII
☒ Encryption of Backups Containing Sensitive Data
☒ Mandatory Security, Privacy and Records Management Training
☐ Other. *Describe*

O. Who will be responsible for protecting the privacy rights of the public and employees? This includes officials responsible for addressing Privacy Act complaints and requests for redress or amendment of records.

The Office of Policy and Financial Management is responsible for the oversight and management of security and privacy controls and the protection of agency information processed and stored in ConcurGov. The Information System Owner, Information System Security Officer, and authorized bureau/office system managers are responsible for ensuring adequate safeguards are implemented to protect individual privacy in compliance with Federal laws and policies for the data managed and stored in ConcurGov, and addressing Privacy Act requests and complaints in consultation with the DOI Privacy Officials.

P. Who is responsible for assuring proper use of the data and for reporting the loss, compromise, unauthorized disclosure, or unauthorized access of privacy protected information?

The ConcurGov Information System Owner is responsible for daily operational oversight and management of the system's security and privacy controls, for ensuring to the greatest possible extent that the data is properly managed and that all access to the data has been granted in a secure and auditable manner. The ConcurGov Information System Owner, Information System Security Officer and authorized bureau/office system managers are also responsible for ensuring that any loss, compromise, unauthorized access or disclosure of PII is reported to DOI-CIRC and

DOI privacy officials within 1-hour of discovery in accordance with Federal policy and established DOI procedures, and appropriate remedial activities are taken to mitigate any impact to individuals, in consultation with DOI Privacy Officials.