U.S. DEPARTMENT OF AGRICULTURE

PRIVACY IMPACT ASSESSMENT

VERSION 1.4

OFFICE OF THE CHIEF PRIVACY OFFICER

2023

Privacy Impact Assessment

The completion of United States Department of Agriculture (USDA) Privacy Impact Assessments (PIAs) is mandated for any rulemaking, program, system, or practice that collects or uses Personally Identifiable Information (PII) under the authority of the E-government Act of 2002 (44 U.S.C. § 208(b)) and USDA DR 3515-002, PII.

The PIA is designed to identify risk associated with the use of PII by a system, program, project or practice, and to ensure that vital data stewardship issues are addressed for all phases of the System Development Life Cycle (SDLC) of Information Technology (IT) systems. It also ensures that security and privacy protections are built into an IT system during its development cycle. By regularly assessing privacy concerns during the development process, USDA ensures that proponents of a program or technology have taken its potential privacy impact into account from the beginning. The PIA also serves to help identify what level of security risk is associated with a program or technology. In turn, this allows the Department to properly manage the security requirements under the Federal Information Security Management Act (FISMA).

USDA DR 3515-002, Privacy Policy and Compliance for Personally Identifiable Information (PII).

Please note that the E-government Act of 2002 requires that a PIA be made available to the public. In order to comply with this requirement**,** PIAs will be published online for the general public to view. When completing this document please use simple, straight-forward language, avoid overly technical terminology, and write out acronyms the first time you use them to ensure that the document can be read and understood by the general public.

Guidance on how to complete the following PIA Questionnaire is available here.

Privacy Impact Assessment for the USDA IT System/Project:

Front End Associate Chief Financial Officer (ACFO) System Analysis Program (SAP) Concur Cloud for Public Sector (FR ASCCPS)

DAITO

ACFO-Shared Services (SS)

Date PIA submitted for review:

April 8, 2024

Mission Area System/Program Contacts:

	Name	**E-mail**	**Phone Number**
Mission Area Privacy Officer	Michele Washington	Michele.washington@usda.gov	(202) 205-3369
Information System Security Manager	Kenneth McDuffie	Kenneth.Mcduffie@usda.gov	(504) 982-6234
System/Program Manager	Linda Connolly	Linda.Connolly@usda.gov	(504) 226-3430

Abstract

The United States Department of Treasury (Treasury) hosts the System Analysis Program (SAP) Concur. SAP Concur is the world's leading brand for integrated travel, expense, and invoice management. Concur Cloud for Public Sector (CCPS) is a multi-tenant, end-to-end, fully integrated travel, and expense platform, that delivers secure, scalable, and reliable travel and spend management solutions to United States (U.S.) federal, state, local, tribal, and territorial customers, as well as federally funded research and development centers (FFRDCs), U.S. government contractors, and lab entities. CCPS combines the benefits of modern cloud technology, adaptive cybersecurity, and enhances risk management, allowing customers to focus on their mission objectives while reducing risks and IT spending. The SAP Concur ConcurGov E-Gov Travel Service (ETS2) travel system ("ConcurGov") is the application used by USDA for reservations, booking, authorization/obligation, and payment/voucher transactions for USDA mission critical Temporary Duty (TDY) Travel. Users access CCPS by using standard web browsers via a uniform resource locator (URL) or by using SAP Concur mobile applications. This PIA is being created for the front-end, Software-as-a-Service (SaaS) instance of SAP Concur CCPS. Based on the Privacy Threshold Assessment submitted in December 2023, this system does collect Personally Identifiable Information (PII) from USDA employees, and therefore, a PIA is necessary.

The Front End Associate Chief Financial Officer SAP Concur Cloud for Public Sector (FR ASCCPS) is a major mission supportive web-based application.

Overview

The Associate Chief Financial Officer for Shared Services, Financial Management Services (ACFO-SS/FMS) is the organization responsible for the security, operation, and maintenance of the FR ASCCPS application. The FR ASCCPS infrastructure is hosted by SAP Concur residing on the CCPS, a FedRAMP approved Cloud provider.

FR ASCCPS is a cloud-based, front-end system. The system categorization is Moderate. USDA's eAuthentication (eAUTH) solution serves as the centralized authentication service for USDA employees to access USDA Web Services, including access to the FR ASCCPS application.

Section 1.0 Authorities and Other Requirements

The following questions are intended to identify all statutory and regulatory authority for operating the project, including the authority for collection, what System of Records Notice (SORN) applies, if an Authority to Operate (ATO) has been completed and if there is Paperwork Reduction Act coverage.

1.1. What legal authorities and/or agreements permit the collection of information by the project or system?

Title 5 United States Code (USC) Chapter 57: Travel, Transportation, and Subsistence permits the collection of information by CCPS. Additional laws and regulations include the Federal Information Security Management Act (FISMA), Office of Management and Budget (OMB) circulars, Public Law (PL), USC, and Homeland Security Presidential Directives (HSPD). The following table was extracted from Attachment 4 – FedRAMP SAP Concur, Concur Cloud for Public Sector PIA, Version 1.1, October 11, 2023.

Applicable Laws and Regulations

Identification Number	Title	Date	Link
44 USC 31	NI Title 44 Public Printing and Documents; Chapter 31 Records Management by Federal Agencies ST SP 800-122, Appendix D	January 2012	44 USC 31
5 USC 552a	Title 5 Government Organization and Employees; Chapter 5 Administrative Procedure; Section 552a Records maintained on individuals (Privacy Act of 1974 as amended)	January 2014	5 USC 552A
HSPD-12	Homeland Security Presidential Directive 12, Policy for a Common Identification Standard for Federal Employees and Contractors [HSPD-12], August 27, 2004	August 2004	HSPD-12
HSPD-7	Homeland Security Presidential Directive-7, Critical Infrastructure Identification, Prioritization, and Protection [HSPD-7], December 17, 2003	December 2003	HSPD-7
OMB Circular A-123	Management's Responsibility for Internal Control Revised	December 2004	OMB A-123
OMB Circular A-130	Managing Information as a Strategic Resource	July 2016	OMB A-130

Identification Number	Title	Date	Link
OMB M-01-05	Guidance on Inter-Public Sector Customer Sharing of Personal Data – Protecting Personal Privacy	December 2000	OMB M 01-05
OMB M-04-04	E-Authentication Guidance for Federal Agencies	December 2003	OMB M 04-04
OMB M-06-16	Protection of Sensitive Public Sector Customer Information	June 2006	OMB M-06-16
PL 99-474	Computer Fraud and Abuse Act, 18 USC 1030	October 1986	PL 99-474
PL 104-231	Electronic Freedom of Information Act as Amended in 2002 [PL 104-231, 5 USC 552], October 2, 1996	October 1996	PL 104-231
PL 107-347	E-Government Act of 2002 - Federal Information Security Modernization Act (FISMA) of 2014	December 2014	FISMA 2014

Applicable Standards and Guidance

Identification Number	Source	Title	Date	Link
NIST SP 800-53	National Institute of Standards and Technology	Security and Privacy Controls for Federal Information Systems and Organizations, Revision 5	December 2020	SP 800-53
NIST SP 800-122	National Institute of Standards and Technology	NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	April 2010	SP 800-122
NIST SP 800-144	National Institute of Standards and Technology	Guidelines on Security and Privacy in Public Cloud Computing	December 2011	SP 800-144
NARA 2010-05	National Archives NARA Bulletin 2010-05	Guidance on Managing Records in Cloud Computing Environments (NARA Bulletin)	September 2010	NARA 2020-05

1.2 Has Authorization and Accreditation (A&A) been completed for the system?

1. *The Security Plan Status,* ***Complete***
2. *The Security Plan Status Date,* ***1/9/2024***
3. *The Authorization Status, In progress*
4. *The Authorization Date, In progress*
5. *The Authorization Termination Date,* ***N/A***
6. *The Risk Review Completion Date,* ***1/9/2024***
7. *The FIPS 199 classification of the system (LOW/****MODERATE****/HIGH).* ***11/28/2023***

1.3. What System of Records Notice(s) (SORN(s)) apply to the information?

Government Services Agency (GSA)/GOVT-4 - Contracted Travel Services Program (E-TRAVEL), GSA/GOVT-3 SORN, Travel Charge Card Program

1.4. Is the collection of information covered by the Paperwork Reduction Act?

Yes.

Section 2.0 Characterization of the Information

2.1. What information is collected, used, disseminated, or maintained in the system/program?

Please check any information listed below that your system collects, uses, disseminates, creates, or maintains. If additional sensitive PII is collected, used, disseminated, created, or maintained, please list those in the text box below:

Identifying Numbers					
☐	Social Security number			☒	Truncated or Partial Social Security number
☐	Driver's License Number			☐	License Plate Number
☐	Registration Number			☐	File/Case ID Number
☐	Student ID Number			☐	Federal Student Aid Number
☒	Passport number			☐	Alien Registration Number
☐	DOD ID Number			☐	DOD Benefits Number
☒	Employee Identification Number			☐	Professional License Number
☐	Taxpayer Identification Number			☐	Business Taxpayer Identification Number (sole proprietor)
☒	Credit/Debit Card Number			☐	Business Credit Card Number (sole proprietor)
☐	Vehicle Identification Number			☐	Business Vehicle Identification Number (sole proprietor)
☐	Personal Bank Account Number			☐	Business Bank Account Number (sole proprietor)
☐	Personal Device Identifiers or Serial Numbers			☐	Business device identifiers or serial numbers (sole proprietor)
☒	Personal Mobile Number			☐	Business Mobile Number (sole proprietor)
☐	Health Plan Beneficiary Number				
Biographical Information					
☒	Name (including nicknames)	☒	Gender	☐	Business Mailing Address (sole proprietor)
☒	Date of Birth (MM/DD/YY)	☐	Ethnicity	☐	Business Phone or Fax Number (sole proprietor)
☒	Country of Birth	☐	City or County of Birth	☐	Group/Organization Membership
☐	Citizenship	☐	Immigration Status	☐	Religion/Religious Preference
☒	Home Address	☒	Zip Code	☒	Home Phone or Fax Number
☒	Spouse Information	☐	Sexual Orientation	☐	Children Information
☐	Marital Status	☐	Military Service Information	☐	Mother's Maiden Name
☐	Race	☐	Nationality	☐	Global Positioning System (GPS)/Location Data
☒	Personal e-mail address	☒	Business e-mail address	☐	Personal Financial Information (including loan information)
☒	Employment Information	☒	Alias (username/screenname)	☐	Business Financial Information (including loan information)
☐	Education Information	☐	Resume or curriculum vitae	☐	Professional/personal references
Biometrics/Distinguishing Features/Characteristics					
☐	Fingerprints	☐	Palm prints	☐	Vascular scans
☐	Retina/Iris Scans	☐	Dental Profile	☐	Scars, marks, tattoos
☐	Hair Color	☐	Eye Color	☐	Height

☐	Video recording	☐	Photos	☐	Voice/ Audio Recording
☐	DNA Sample or Profile	☒	Signatures	☐	Weight
Medical/Emergency Information					
☐	Medical/Health Information	☐	Mental Health Information	☐	Disability Information
☐	Workers' Compensation Information	☐	Patient ID Number	☒	Emergency Contact Information
Device Information					
☐	Device settings or preferences (e.g., security level, sharing options, ringtones)	☐	Cell tower records (e.g., logs, user location, time, etc.)	☐	Network communications data
Specific Information/File Types					
☐	Personnel Files	☐	Law Enforcement Information	☐	Credit History Information
☐	Health Information	☐	Academic/Professional Background Information	☐	Civil/Criminal History Information/Police Record
☐	Case files	☐	Security Clearance/Background Check	☐	Taxpayer Information/Tax Return Information

2.2. What are the sources of the information in the system/program?

USDA employees provide the information listed in the table above when setting up their individual profiles in the travel system by completing USDA Concur-Government Edition Access Request Form (OCFO-FPD-2017).

2.2.1. How is the information collected?

A Level 2, E-authentication identification (ID) is required for access to the system. Access is requested via the USDA Concur-Government Edition Access Request Form (OCFO-FPD-2017). The Lead Federal Agency Travel Administrator (LFATA) and/or Federal Agency Travel Administrator (FATA) adds, modifies, and/or disables the profile.

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

Yes. This information is used to book all mission critical Temporary Duty Travel (TDY), which includes airline, train, hotel, and rental car reservation information.

2.4. How will the information be checked for accuracy? How often will it be checked?

Authorization and Voucher data are validated for Travel Policy by employing Audit checks before the Authorization and Voucher are transmitted to the Financial Management Modernization Initiative (FMMI) for budget and accounting validation. ConcurGov has implemented a multilayered defense strategy as a protection against unauthorized modifications. ConcurGov requests that the individual's authorized representative validate PII during the collection process. The authorized representative checks for, and corrects as necessary, any inaccurate or outdated PII used by its programs or systems per submission and annually.

2.5. Does the system/program use third-party websites?

Yes

2.5.1. What is the purpose of the use of third-party websites?

Third party websites are used to obtain supplemental travel information to assist in performing Government travel (state tax exemption forms, GSA Travel information, per diem, and meals and incidental expenses (MI&E)).

2.5.1.1. What PII will be made available to the agency through the use of third-party websites?

Employee profile information (name, contact information, etc.) is sent to third-party websites to secure reservations for hotel, airlines, and rental car. Options for these travel details are made available to the agency through the use of third-party sites.

2.6. PRIVACY IMPACT ANALYSIS: Related to Characterization of the Information.

Follow the format below:

Possible risks:

- Unauthorized disclosure and access to user information
- Audit and compliance issues
- Data breaches and cyber attacks
- Potential legal and regulatory consequences

Mitigation: These risks are mitigated by applying the following controls:

- Encryption – All client/server communications are encrypted through Transport Layer Security.

- Controlled access – USDA eAuthentication limits ConcurGov access to authorized users only. In addition, authorized users must be defined to the ConcurGov application.
- Timeout for remote access – ConcurGov sessions are cancelled by the application server after a specified idle period.
- Access controls including role-based account management and implementation of separation of duties and least privilege is enforced through the use of profiles and roles.

Section 3.0 Uses of the Information

The following questions are intended to clearly delineate the use of information and the accuracy of the data being used.

3.1. Describe why and how the information collected, used, disseminated and/or maintained will support the program's business purpose?

The information collected is used for reservation, booking, authorization/obligation, and payment/voucher transactions for USDA mission critical TDY Travel.

3.2. Does the system/project/program use technology to conduct electronic searches, queries, or analysis in an electronic database to discover or locate a predictive pattern or anomaly? If so, state how USDA plans to use such results.

Yes. Travelers can set up preferences within their profiles that are retained for future reference. The system analyzes and uses the data to create a predictive pattern for preferred airline seating, rental car companies, hotel details, etc.

3.3. PRIVACY IMPACT ANALYSIS: Related to uses of the information.

Follow the format below:

Privacy Risk:

Possible risks associated with the PII accessible through this system is:

- Unauthorized disclosure and access to user information
- Audit and compliance issues
- Data breaches and cyber attacks
- Potential legal and regulatory consequences

Mitigation: These risks are mitigated by applying the following controls:

- Encryption – All client/server communications are encrypted through Transport Layer Security.
- Controlled access – USDA eAuthentication limits ConcurGov access to authorized users only. In addition, authorized users must be defined to the ConcurGov application.
- Timeout for remote access – ConcurGov sessions are cancelled by the application server after a specified idle period.
- Access controls including role-based account management and implementation of separation of duties and least privilege is enforced through the use of profiles and roles.

Section 4.0 Notice

The following questions are directed at providing notice to the individual of the scope of information collected, the right to consent to uses of the information, and the right to decline to provide information.

4.1. How does the project/program/system provide notice to individuals prior to collection?
ConcurGov displays the following The Privacy Act Notice, before users 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.

Users that need additional information on the system warning above can reach out to their Mission Area FATA for further details on how their information is used once they access the system. The FATA's contact information is provided to users as a part of the Government Charge Card registration process. Users cannot travel without accessing the system.

4.2. What options are available for individuals to consent, decline, or opt out of the project?
The Federal Information System Warning specifies that use of ConcurGov constitutes a user's consent to such monitoring. Information requested is voluntary; however, failure to provide the information may nullify the ability to book online travel reservations. If users want to consent to the system, they can click the "I Agree" button following the warning banner. Alternatively, if users elect to decline or opt out, regardless of reason, they can click the "Cancel" button following the warning banner and therefore, will not gain access to the system.

4.3. PRIVACY IMPACT ANALYSIS: Related to Notice

Follow the format below:

Privacy Risks:

- Users may have challenges understanding the system access requirements and how their information will be used.

Mitigation: These risks are mitigated by applying the following controls:

- As a part of the Government's Charge Card registration process, users are given a designated FATA (Travel Point of Contact) to provide comprehensive guidance for accessing the system. Users can email or call the FATA as needed.

Section 5.0 Data Retention

The following questions are intended to outline how long information will be retained after the initial collection.

5.1. What information is retained and for how long?

User information is retained in compliance with National Archives and Records Administration (NARA) retention guidelines for financial management data. Bill related data is retained for a minimum of six full years.

5.2. Has the retention schedule been approved by the USDA records office and the National Archives and Records Administration (NARA)? If so, please indicate the name of the records retention schedule.

General Records Schedule (GRS) for USDA Travel and supporting documents.

5.3. PRIVACY IMPACT ANALYSIS: Related to retention of information.

Follow the format below:

Privacy Risk:

- Longer period of data retention can impose the risk of data being stolen, loss of data integrity and confidentiality.

Mitigation: These risks are mitigated by applying the following controls:

- Users are required to undergo USDA Records Management training in AgLearn annually. Course completion includes Records Management, Records Management Responsibilities, and Acknowledgment. Information is protected by access rules. Users who need access to the data must be granted access by an authorized individual and will apply the appropriate access rules to the user's ID.
- Encryption – All client/server communications are encrypted through Transport Layer Security.
- Masking of PII data.
- Controlled access – USDA eAuthentication limits SAP ConcurGov access to authorized users only. In addition, authorized users must be defined to the SAP ConcurGov application.
- Timeout for remote access – SAP Concur sessions are cancelled by the application server after a specified idle period.
- System audit logs – The hosting provider captures and retains all logon and logoff actions and selected additional actions such as changes to user profiles.

Section 6.0 Information Sharing

The following questions are intended to define the content, scope, and authority for information sharing.

6.1. With which internal organizations and/or systems is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

This system is used Enterprise-wide. Authorization and Voucher data are validated for Travel Policy by employing Audit checks before the Authorization and Voucher are transmitted to the Financial Management Modernization Initiative (FMMI) for budget and accounting validation. Authorized USDA agency users access the ConcurGov system the same way as ACFO-FMS internal users. Limitations are applied through the assignment of restrictive roles. Data leaving the system/application is secured with Transport Layer Security (TLS) 1.2 encryption authentication schemas.

SAP Concur controls and protects session authenticity at the Transport Layer. The CCPS employs the following solutions to protect authenticity of communication sessions and communications leveraging:

- Multifactor authentication
- Transmission Control Protocol (TCP) transport layer
- Network Access Control Lists (NACLs)
- Akamai Domain Name System Security Extensions (DNSSEC)
- Akamai Site Shield
- Virtual Private Network (VPN)

Connection traffic flows through the Akamai content delivery network (CDN) leveraging the web application firewall feature, into the FortiGate edge firewall. Web connections are secured using TLS

1.2 with 128-bit encryption or higher.

In order to protect against session hijacking, the CCPS environment employs an Akamai web application firewall (WAF) feature that prevents man in the middle attacks, including session hijacking. Akamai Site Shield provides internal validation that the traffic is indeed coming from Akamai (through the firewall) and not from a third-party malicious actor.

6.2. PRIVACY IMPACT ANALYSIS: Related to internal sharing and disclosure.

Follow the format below:

Privacy Risks:

- Unauthorized disclosure and access to user information

Mitigation: These risks are mitigated by applying the following controls:

- Controlled access – USDA eAuthentication limits ConcurGov access to authorized users only. Limitations are applied through the assignment of restrictive roles.
- Access controls including role-based account management and implementation of separation of duties and least privilege is enforced through the use of profiles and roles.

6.3. With which external organizations (outside USDA) is information shared/received/transmitted? What information is shared/received/transmitted, and for what purpose? How is the information transmitted?

Information Shared/Received/Transmitted with ConcurGov, preferred transportation facilities, and preferred lodging facilities is as follows:

- First name, last name, contact information, preferences
- Lodging preferences
- Transportation preferences (Rental car, airlines, etc)
- Travel itinerary

This information is shared for the purpose of processing authorizations/obligations travel related vouchers.

6.4. PRIVACY IMPACT ANALYSIS: Related to external sharing and disclosure.

Follow the format below:

Privacy Risk:

- Unauthorized disclosure and access to user information
- Data breaches and cyber attacks

Mitigation: These risks are mitigated by applying the following controls:

- Controlled access – USDA eAuthentication limits ConcurGov access to authorized users only. Limitations are applied through the assignment of restrictive roles.
- Access controls including role-based account management and implementation of separation of duties and least privilege is enforced through the use of profiles and roles.
- Encryption – All client/server communications are encrypted through Transport Layer Security.

Section 7.0 Redress

The following questions are directed at an individual's ability to ensure the accuracy of the information collected about him or her.

7.1. What are the procedures that allow individuals to gain access to their information?

Travelers have access within ConcurGov via a Profile selection button to view and update their information as needed. Users have the ability to access and update their information at any time.

7.2. What are the procedures for correcting inaccurate or erroneous information?

Travelers may update their information directly within ConcurGov. The traveler's assigned Mission Area FATA may also update inaccurate or erroneous information at the request of the traveler via email. ACFO-FMS FATAs use discretion when determining if personally identifiable information is to be corrected or deleted based on the scope of requests, the changes sought, the impact of the changes, and laws, regulations, and policies.

7.3. How are individuals notified of the procedures for correcting their information?

When travelers access the system for the first time they are required to review and/or update their information. Travelers may also update their information within ConcurGov at any time as there is a profile button for selection in ConcurGov. In addition, the Traveler may request assistance from their Agency FATA listed in the USDA Travel Point of Contact List. This list can be found on the USDA GCC SharePoint Site. The Agency FATAs are the main vehicle for communication.

7.4. If no formal redress is provided, what alternatives are available to the individual?

N/A

7.5. PRIVACY IMPACT ANALYSIS: Related to Redress.

Follow the format below:

Privacy Risks:

- The FATA may decline the requested changes from the traveler based on the scope of requests, the changes sought, the impact of the changes, and laws, regulations, and policies.

Mitigation: These risks are mitigated by applying the following controls:

• USDA FATAs must adhere to established laws, regulations, and policies in order to ensure continuity and security of the system. The following laws, regulations, and policies are applicable to ensuring continuity and security of the system:

Identification Number	Source	Title	Date	Link
NIST SP 800-53	National Institute of Standards and Technology	Security and Privacy Controls for Federal Information Systems and Organizations, Revision 5	December 2020	SP 800-53
NIST SP 800-122	National Institute of Standards and Technology	NIST SP 800-122, Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)	April 2010	SP 800-122
NIST SP 800-144	National Institute of Standards and Technology	Guidelines on Security and Privacy in Public Cloud Computing	December 2011	SP 800-144
NARA 2010-05	National Archives NARA Bulletin 2010-05	Guidance on Managing Records in Cloud Computing Environments (NARA Bulletin)	September 2010	NARA 2020-05
PL 107-347	E-Government Act of 2002	Federal Information Security Modernization Act (FISMA) of 2014	December 2014	FISMA 2014

Section 8 Auditing and Accountability

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

8.1. How is the information in the system/project/program secured?

• Encryption – All client/server communications are encrypted through Transport Layer Security.

• Masking of PII data.

• Controlled access – USDA eAuthentication limits SAP ConcurGov access to authorized users only. In addition, authorized users must be defined to the SAP ConcurGov application.

• Timeout for remote access – SAP Concur sessions are cancelled by the application server after a specified idle period.

• System audit logs – The hosting provider captures and retains all logon and logoff actions and selected additional actions such as changes to user profiles.

8.2. What procedures are in place to determine which users may access the program or system/project, and are they documented?

Users have access to the information in the system based on job function and the need to know the information. Profiles are set up and Roles are assigned to users to ensure that internal controls and separation of duties are maintained. Sensitive information is restricted from users if there is no valid job-related need for the information to perform the duties of their position.

A USDA Concur - Government Edition Access Request Form is required to establish a user account, report a change in duties, report separation from the agency, and report name or profile changes. For agency personnel the LFATA and/or FATA adds, modifies, and/or disables users profiles.

8.3. How does the program review and approve information sharing requirements?

Memorandums of Understanding (MOU) and Interconnection Service Agreements (ISAs) are reviewed and approved at the SAP Concur Program level. The MOU/ISAs include security and privacy requirements, interface characteristics, controls, and responsibilities for each system. As part of the Risk Management Framework, MOUs and ISAs are reviewed annually or updated immediately when changes are made.

8.4. Describe what privacy training is provided to users either generally or specifically relevant to the program or system/project?

All users including contractors are required to complete Privacy Awareness training and USDA Travel Charge Card Training. Privacy Awareness training in AgLearn helps federal employees follow federal privacy laws and ensure Fair Information Principles, or FIPs, are followed. Additionally, the USDA Travel Card (OCFO-TravelCard-20##) training in AgLearn is a required course that must be taken annually by existing travel charge cardholders. For those new to Federal travel, the course must be completed before the issuance of the travel card. Training includes basic security briefings about awareness training and annual refresher training, rules of behavior, and non-disclosure agreements. All user training is tracked and reported through the AgLearn monthly scorecard. Personnel identified as having system security roles and responsibilities are provided additional specialized training through AgLearn.

Approval Signatures:

_____
Linda Connolly, Deputy Director, Financial Management Services
System Owner
United States Department of Agriculture

_____
Michele Washington
Mission Area Privacy Officer
Departmental Administration Information
Technology Office, DAITO
United States Department of Agriculture

QUANISHA JONES Digitally signed by QUANISHA JONES
Date: 2024.11.01 13:52:06 -04'00'
_____
Office of the Chief Privacy Officer
United States Department of Agriculture