ConcurGov Privacy Impact Assessment

Privacy Impact Assessment (PIA)

March 8, 2021

POINT *of* CONTACT

Richard Speidel

gsa.privacyact@gsa.gov

Chief Privacy Officer
GSA IT
1800 F Street NW
Washington, DC 20405

Stakeholders

Name of Information System Security Manager (ISSM):

- Arpan Patel

Name of Program Manager/System Owner:

- Rebecca Bond

Signature Page

Signed:

DocuSigned by:
Arpan Patel
8B059AABDAF1477...

Information System Security Manager (ISSM)

DocuSigned by:
Rebecca Bond
A25CBC38B2274C2...

Program Manager/System Owner

DocuSigned by:
Richard Speidel
171D5411183F40A...

Chief Privacy Officer (CPO) - Under the direction of the Senior Agency Official for Privacy (SAOP), the CPO is responsible for evaluating the PIA and ensuring the program manager/system owner has provided complete privacy-related information.

Table of contents

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will GSA verify the information collection, maintenance, use, or dissemination for accuracy and completeness?

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the project? What is the authorization process for access to the project?

6.2 Has GSA completed a system security plan (SSP) for the information system(s) supporting the project?

6.3 How will the system be secured from a physical, technical, and managerial perspective?

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

7.2 What procedures allow individuals to access their information?

7.3 Can individuals amend information about themselves in the system? If so, how?

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the project.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is being used only according to the stated practices in this PIA?

Document purpose

This document contains important details about the ConcurGov information system. To accomplish its mission GSA Privacy Office must, in the course of ConcurGov, collect personally identifiable information (PII) about the people who use such products and services. PII is any information that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.

A. System, Application, or Project Name:

ConcurGov.

B. System, application, or project includes information about:

- ConcurGov is an end-to-end travel management service that is used to plan, authorize, arrange, process, and manage official Federal travel. ConcurGov's end-to-end travel automation consists of fully integrated travel booking and travel management functions, including user profile management, fulfillment, ticketing, ticket tracking, quality control, expense filing, data consolidation, and reporting, with links to enterprise resource providers and financial management systems.
- ConcurGov maintains and uses information in order to meet current and future government travel requirements and needs for the purpose of recording travel information provided by the user to create travel itineraries, reserve any method or mode of travel accommodations, and claim entitlements and allowances prescribed in applicable Federal travel regulations. The purpose of the collection of this information is to establish a comprehensive travel services system that enables travel service providers under contract with the Federal government to authorize, issue, and account for travel and travel reimbursements provided to individuals on official Federal government business. Routine uses of the information are outlined in the Privacy Act notice represented within the Overview of this document.
- ConcurGov doesn't conduct electronic searches, queries, or analyses in an electronic database to discover or locate a predictive pattern or an anomaly.
- User roles and responsibilities are defined from the user interface to the database.

- ConcurGov consists of two key components. The type of PII collected by each component of ConcurGov, the functions that collect it, and the purpose of the collection/how it is used are recorded in Table 1 - PII Mapped to Components.

Table 1 - PII Mapped to Components

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

C. For the categories listed above, how many records are there for each?

There are +5.5 million booking records and +10 million vouchers.

D. System, application, or project includes these data elements:

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

Overview

The purpose of the ConcurGov system is described in the Document Purpose section (above). PII handling and processing is governed by the Privacy Act Notice, which is displayed to users when they log in to ConcurGov:

> **"**********PRIVACY ACT NOTICE**********
>
> This system contains information protected under the provisions of the Privacy Act of 1974 (Public Law 93-579). Any privacy information displayed on the screen or printed must be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary actions, a fine of up to $5,000, or both.
>
> "The information requested in the ConcurGov is collected pursuant to Executive Order 9397 and Chapter 57, Title 5 United States Code. The purpose of the collection is to establish a comprehensive travel services system which enables travel service providers to authorize, issue, and account for travel and travel reimbursements provided to individuals on official Federal Government business. Categories of records in the system records may include: Full name matching the form of ID used for travel; Social Security Number; employee identification number; home, office, agency and emergency contact information; travel and hotel preferences; current passport and/or visa number(s); credit card numbers and related information; bank account information; frequent traveler account information (e.g., frequent flyer account numbers); date of birth; gender; DHS redress and known traveler numbers (numbers DHS assigns to promote resolution with previous watch list alerts and facilitate passenger clearance, respectively); trip information (e.g., destinations, reservation information); travel authorization information; travel claim information; monthly reports from travel agent(s) showing charges to individuals, balances, and other types of account analyses; and other official travel related information.
>
> Routine uses which may be made of the collected information and other financial account information in the system(s) of record entitled "Contracted Travel Services Program GSA/GOVT-4" are: (a) To another Federal agency, Travel Management Center (TMC), online booking engine suppliers and the airlines that are required to support the DHS/TSA Secure Flight program. (b) To a Federal, State, local, or foreign agency responsible for investigating, prosecuting, enforcing, or carrying out a statute, rule, regulation, or order, where agencies become aware of a violation or potential violation of civil or criminal law or regulation; (c) To another Federal agency or a court when the Federal Government is party to a judicial proceeding; (d) To a Member of Congress or a congressional staff member in response to an inquiry from that congressional office made at the request of the individual who is the subject of the record; (e) To a Federal agency employee, expert, consultant, or contractor in performing a Federal duty for purposes of authorizing, arranging, and/or claiming reimbursement for official travel, including, but not limited to, traveler

profile information; (f) To a credit card company for billing purposes, including collection of past due amounts; (g) To an expert, consultant, or contractor in the performance of a Federal duty to which the information is relevant; (h) To a Federal agency by the contractor in the form of itemized statements or invoices, and reports of all transactions, including refunds and adjustments to enable audits of charges to the Federal Government; (i) To a Federal agency in connection with the hiring or retention of an employee; the issuance of security clearance; the reporting of an investigation; the letting of a contract; or the issuance of a grant, license, or other benefit to the extent that the information is relevant and necessary to a decision; (j) To an authorized appeal or grievance examiner, formal complaints examiner, equal employment opportunity investigator, arbitrator, or other duly authorized official engaged in investigation or settlement of a grievance, complaint, or appeal filed by an employee to whom the information pertains; (k) To the Office of Personnel Management (OPM), the Office of Management and Budget (OMB), or the Government Accountability Office (GAO) when the information is required for program evaluation purposes; (l) To officials of labor organizations recognized under 5 U.S.C. Chapter 71 when relevant and necessary to their duties of exclusive representation concerning personnel policies, practices, and matters affecting working conditions; (m) To a travel services provider for billing and refund purposes; (n) To a carrier or an insurer for settlement of an employee claim for loss of or damage to personal property incident to service under 31 U.S.C. § 3721, or to a party involved in a tort claim against the Federal Government resulting from an accident involving a traveler; (o) To a credit reporting agency or credit bureau, as allowed and authorized by law, for the purpose of adding to a credit history file when it has been determined that an individual's account with a creditor with input to the system is delinquent; (p) summary or statistical data from the system with no reference to an identifiable individual may be released publicly; (q) to the National Archives and Records Administration (NARA) for records management purposes; (r) to appropriate agencies, entities, and persons when (1) The Agency suspects or has confirmed that the security or confidentiality of information in the system of records has been compromised; (2) the Agency has determined that as a result of the suspected or confirmed compromise there is a risk of harm to economic or property interests, identity theft or fraud, or harm to the security or integrity of this system or other systems or programs (whether maintained by GSA or another agency or entity) that rely upon the compromised information; and (3) the disclosure made to such agencies, entities, and persons is reasonably necessary to assist in connection with GSA's efforts to respond to the suspected or confirmed compromise and prevent, minimize, or remedy such harm. Information requested is voluntary, however, failure to provide the information may nullify the ability to book online travel reservations."

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

For additional information, please see GSA's Government-wide Contracted Travel Services Program or "E-Travel" SORN (GSA/GOVT-4).

SECTION 1.0 PURPOSE OF COLLECTION

1.1 What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?

- The GSA ETS2 Master Contract with SAP Concur, GS-33F-Y0026, permits the collection of the information.

1.2 Is the information searchable by a personal identifier, for example a name or Social Security Number? If so, what System of Records Notice(s) apply/applies to the information?

- Yes, information is searchable by a personal identifier by users with appropriate and authorized permissions.
- GSA's Government-wide Contracted Travel Services Program or "E-Travel" SORN (GSA/GOVT-4) covers the systems.
- PII handling and processing is governed by the Privacy Act Notice (shown above in the Overview section).

1.3 Has an Information Collection Request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)? If yes, provide the relevant names, OMB control numbers, and expiration dates.

N//A.

1.4 Has a records retention schedule been approved by the National Archives and Records Administration (NARA)? Explain how long and for what reason the information is retained.

- 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.

SECTION 2.0 OPENNESS AND TRANSPARENCY

2.1 Will individuals be given notice before the collection, maintenance, use or dissemination of personal information about themselves? If not, please explain.

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

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

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

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

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

Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed, or stored in this system by law enforcement and authorized officials. Use of this system constitutes consent to such monitoring.

SECTION 3.0 DATA MINIMIZATION

3.1 Why is the collection and use of the PII necessary to the system, application, or project?

- ConcurGov collects, uses, processes, and maintains data related to official Federal business travel, including information regarding travel planning, authorization, reservations, ticketing, fulfillment, expense reimbursement, and travel management reporting. Types of information include travel profile traveler preferences (including rental car class, seating preferences, ticketing preferences, hotel preferences, travel program affiliations, and so forth), expense and financial information travel itinerary, and travel vouchers and approvals, among other things. A complete list of the standard data elements maintained by ConcurGov is in the GSA ETS2 Master Contract Section C, Attachment 14.

- ConcurGov maintains Personally Identifiable Information (PII). The type of PII collected by ConcurGov and the functions that collect it are recorded in Section 3.0, Table 1 - PII Mapped to Components.

3.2 Will the system, application, or project create or aggregate new data about the individual? If so, how will this data be maintained and used?

N/A.

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?

- The system is designed to implement security and privacy controls at the FISMA Moderate security categorization level. The ETS2 contract specifies certain data fields that meet the definition of PII under the ETS2 Master Contract. SAP Concur has implemented encryption of data at rest and in transit for these fields throughout the ConcurGov system. System and application logs are collected and monitored.
- Procedural controls are implemented by agencies to ensure that data is appropriately protected. Application of these local policies and procedures minimize that risk that users at a site can read, copy, alter, or steal printed or electronic information for which they are not authorized, and require that only authorized users pick up, receive, or deliver input and output information and media. 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.
- Warning individuals with appropriate access about the misuse of data is accomplished through agency policy. In addition, technology controls, such as auditing, reveal the misuse of data in a timely manner.
- Federal Agency Travel Administrators (FATAs) grant access controls on a need-to-know basis. These controls are periodically reviewed and updated. Logs are audited for inappropriate or unauthorized activity.
- Charge card numbers stored in the profiles are encrypted and cannot be viewed in ConcurGov.

3.4 Will the system monitor the public, GSA employees, or contractors?

- The system does not monitor members of the public
- The system does collect information in identifiable form (personal data/information) on government employees.

3.5 What kinds of report(s) can be produced on individuals?

- Each user/data subject has the right to ask for their personal information maintained in ConcurGov from the Customer/Controller Admin (who is designated by each agency customer and assigned by SAP Concur in coordination with such agency customer). Users may request the information within their profiles and/or corrections to this information from their agencies. In response to such request, SAP Concur will coordinate with the agency to provide a report to the users/data subject detailing his/her personal information maintained in ConcurGov.

3.6 Will the data included in any report(s) be de-identified? If so, what process(es) will be used to aggregate or de-identify the data?

The SAP Concur CPO develops privacy policies and manages the SAP Concur privacy program. SAP Concur documents processes to ensure the appropriate aggregation, redaction, and/or de-identification of PII before disclosure.

The SAP Concur CPO is responsible for limiting the risk to PII to the minimum elements necessary by aggregating, redacting, or otherwise de-identifying PII before disclosure.

The organization:

a. Retains each collection of personally identifiable information (PII) for at least one year to fulfill the purpose(s) identified in the notice or as required by law.

b. Disposes of, destroys, erases, and/or anonymizes the PII, regardless of the method of storage, in accordance with the NARA-approved record retention schedule and in a manner that prevents loss, theft, misuse, or unauthorized access; and

c. Uses techniques and methods in accordance with GSA IT Security Policy CIO 2100.1L to ensure secure deletion or destruction of PII (including originals, copies, and archived records).

Sarbanes-Oxley SAP Concur requires that information be classified on the SAP Concur Data Retention Standard. The purpose of the SAP Concur Data Retention Standard is to establish policy that states the minimum and maximum periods of time that internal records will be maintained in accordance with the GSA Authority. Authority to modify the SAP Concur Data Retention Standard resides with the SAP Concur CPO and is approved by the SAP Concur Policy Review Board. The Concur Data Retention Standard is reviewed at least once per calendar year.

SECTION 4.0 LIMITS ON USING AND SHARING INFORMATION

4.1 Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?

- Yes

4.2 Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations? If so, how will GSA share the information?

- Unless otherwise authorized by a customer, SAP Concur does not disclose data to unauthorized third parties.
- The Master Contract calls for data generated by and/or stored in the system to be transmitted to GSA or third-party vendors designated by GSA, including the Travel Management Information Service (MIS).

4.3 Is the information collected directly from the individual or is it taken from another source? If so, what is the other source(s)?

- The organization describes the purpose(s) for which personally identifiable information (PII) is collected, used, maintained, and shared in its privacy notices. The only agency that provides PII into the system is the client agency, and the stated purpose is part of the system notification settings displayed before entering any personal data.

4.4 Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA? If so, who and how? Is a formal agreement(s) in place?

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

SECTION 5.0 DATA QUALITY AND INTEGRITY

5.1 How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?

- The customer and its users are responsible for ensuring the accuracy of data submitted within the ConcurGov system. SAP Concur personnel alter customer information only when requested by authorized personnel from the customer via customer support case, implementation project, or special project request, which is documented for tracking purposes. ConcurGov is designed such that it can prevent the entry of invalid government travel charge card information (for example, charge card number) within ConcurGov. ConcurGov performs data validation at the time of entry, which prevents inaccurate information from being entered and saved in error. The GDS validates traveler's names with their frequent traveler information to prevent

errors. If there is a problem, users are notified via application error that they need to resolve the issue before being able to book travel.

SECTION 6.0 SECURITY

6.1 Who or what will have access to the data in the system, application, or project? What is the authorization process to gain access?

- Data is submitted to ConcurGov by agency travelers, agency administrators, agency approvers, or agency travel arrangers, in accordance with agency policy and permissions. Traveler profile information can be uploaded by mass import into ConcurGov at the request of the agency.
- SAP Concur works with each customer agency to establish appropriate user roles with correct permissions and then assigns the correct user roles through a profile data import for each Federal employee who will have access to ConcurGov. Federal Agency Travel Administrators (FATAs) with defined access maintain the user profiles after implementation.
- Federal agency business systems interface with ConcurGov for proper recording of authorizations and vouchers. Data is exchanged between systems and is documented in an Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU). The agency business systems do not have direct access to ConcurGov databases.

6.2 Has GSA completed a System Security Plan (SSP) for the information system(s) or application?

- Yes, a System Security Plan (SSP) was last approved by the Government on June 12, 2020: SSP Date: ConcurGov_SSP_V7.8_20200612_Final_Signed.docx, ATO Date: June 12, 2020.

6.3 How will the system or application be secured from a physical, technical, and managerial perspective?

- Data is submitted to ConcurGov by agency travelers, agency administrators, agency approvers, or agency travel arrangers, in accordance with agency policy and permissions. Traveler profile information can be uploaded by mass import into ConcurGov at the request of the agency.
- SAP Concur works with each customer agency to establish appropriate user roles with correct permissions and then assigns the correct user roles through a profile data import for each Federal employee who will have access to ConcurGov. Federal Agency Travel Administrators (FATAs) with defined access maintain the user profiles after implementation.
- Federal agency business systems interface with ConcurGov for proper recording of authorizations and vouchers. Data is exchanged between

systems and is documented in an Interconnection Security Agreement (ISA) and Memorandum of Understanding (MOU). The agency business systems do not have direct access to ConcurGov databases.

- The system is designed to implement security and privacy controls at the FISMA Moderate security categorization level. The ETS2 contract specifies certain data fields that meet the definition of PII under the ETS2 Master Contract. SAP Concur has implemented encryption of data at rest and in transit for these fields throughout the ConcurGov system. System and application logs are collected and monitored.
- Procedural controls are implemented by agencies to ensure that data is appropriately protected. Application of these local policies and procedures minimize that risk that users at a site can read, copy, alter, or steal printed or electronic information for which they are not authorized, and require that only authorized users pick up, receive, or deliver input and output information and media. 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.
- Warning individuals with appropriate access about the misuse of data is accomplished through agency policy. In addition, technology controls, such as auditing, reveal the misuse of data in a timely manner.
- Federal Agency Travel Administrators (FATAs) grant access controls on a need-to-know basis. These controls are periodically reviewed and updated. Logs are audited for inappropriate or unauthorized activity.
- Charge card numbers stored in the profiles are encrypted and cannot be viewed in ConcurGov.

6.4 Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII? If so, what are they?

- SAP Concur maintains records and processes to appropriately identify any unauthorized disclosures (should one occur) and handles such unauthorized disclosure by directly working with affected agency customers and the GSA PMO ISSO, as outlined in the ETS2 Incident Response Plan.

SECTION 7.0 INDIVIDUAL PARTICIPATION

7.1 What opportunities do individuals have to consent or decline to provide information? Can they opt-in or opt-out? If there are no opportunities to consent, decline, opt in, or opt out, please explain.

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

7.2 What procedures allow individuals to access their information?

- Each user/data subject has the right to ask for their personal information maintained in ConcurGov from the Customer/Controller Admin (who is designated by each agency customer and assigned by SAP Concur in coordination with said agency customer). Users can request the information within their profiles and/or corrections to this information from their agencies. In response to such request, SAP Concur coordinates with the agency to provide a report to the users/data subject detailing their personal information maintained in ConcurGov.
- Users with access to the ConcurGov platform also can view and update their personal information in the user interface (UI) via their Traveler Profile.

7.3 Can individuals amend information about themselves? If so, how?

- As outlined in Section 7.1 above, users may request the information within their profiles and/or corrections to this information from their agencies. Users with access can update their personal information within ConcurGov.
- Each customer agency has different processes and procedures for data correction. Agencies can post notifications to end users within ConcurGov and provide direction through configuration settings. When a user makes updates within ConcurGov, they receive a notification confirming the updated information. If the correction is made via a Support request, a written confirmation of the update is sent to the user. ConcurGov provides notifications via email to users to notify them that profile information was changed.

SECTION 8.0 AWARENESS AND TRAINING

8.1 Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

- 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.

SECTION 9.0 ACCOUNTABILITY AND AUDITING

9.1 How does the system owner ensure that the information is used only according to the stated practices in this PIA?

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