FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

Privacy Threshold Analysis (PTA) and/or Privacy Impact Assessment (PIA)

for

CW Government Travel Inc.

GetThere (SATO Travel)

Date Approved by Chief Privacy Officer (CPO)/Designee: 1/26/2018

SECTION I – OUTSOURCED INFORMATION SERVICE DESCRIPTION

1. Describe the outsourced service and its purpose.

The Federal Deposit Insurance Corporation (FDIC) Division of Finance (DOF) is responsible for providing assistance to FDIC employees at all headquarters, regional and field office sites when making reservations for airline tickets, hotel accommodations, and automobile rentals for official travel. FDIC/DOF has contracted with CW Government Travel, Inc. (CWTSatoTravel or SatoTravel)[1] to assist FDIC employees (travelers) in making official travel arrangements, consistent with FDIC travel policies, cost considerations, and employee preferences. In providing the services required under this contract, SatoTravel has subcontracted with GetThere L.P.[2] to provide FDIC travelers and travel specialists with a secure, self-service online booking engine (OBE) for making reservations (air, rail, lodging, car rental, etc.), preparing travel authorizations and vouchers, producing itineraries, and obtaining tickets and receipts.

In order to access the GetThere OBE, the FDIC employee (traveler) must first enter a user ID and password on the OBE login page. The employee may then establish or modify his/her GetThere user profile consisting of the personal information described in question 2 below.

SECTION II – DATA TYPE, SOURCES, AND USE

2. Describe all information/data that will be collected, used, maintained or generated by the Outsourced Provider (Vendor) as part of the services provided under the contract. If no information/data is involved, select Not Applicable.

GetThere, an authorized subcontractor of SatoTravel, maintains the following personal information about FDIC employees/travelers* in the GetThere system: full name, date of birth, gender, user ID and password, postal address (work and home), email address (work and home), telephone number (work and home), credit card and payment information, travel and accommodation details, passport and visa information (number, issuing country, expiration date), and special travel requests, such as a request for a wheelchair or a special meal. In addition, the GetThere system maintains the traveler's emergency contact information (full name, home address, and home telephone number).

*Note: GetThere maintains data about FDIC employees only. FDIC contractors are not authorized to use the GetThere system to book official travel.

3. Describe the intended purpose and use of the above information/data. If no information/data is involved, select Not Applicable.

---

[1] CWTSatoTravel is an approved provider under the General Services Administration (GSA) E-Gov Travel Services (ETS) program which is focused on assisting the Federal government consolidate online travel booking services and expense management platforms to drive cost savings and efficiencies. ETS-2 is the GSA's second generation travel management program, built on the foundation of ETS. GSA has awarded an ETS Master Contract, as well as ETS-2 Master Contract, to CWTSatoTravel, among other vendors.

[2] GetThere is owned by Sabre. As stipulated in its contract with FDIC, SatoTravel may not engage subcontractors to perform any of its responsibilities without the prior written approval of the FDIC. In addition, as the prime contractor, SatoTravel must ensure that its subcontractors adhere to all of the terms and conditions of the FDIC contract that have flow-down requirements, including but not limited to those related to privacy and security.

GetThere uses the information referenced above to manage employee reservations and issue tickets.

4. What types of personally identifiable information (PII) are (or may be) included in the information specified above?

PII Element	Yes	No
Full Name	☒	☐
Date of Birth	☒	☐
Place of Birth	☐	☒
Social Security Number	☐	☒
Employment Status, History or Information	☒	☐
Mother's Maiden Name	☐	☒
Certificates (e.g., birth, death, naturalization, marriage, etc.)	☐	☒
Medical Information (Medical Records Numbers, Medical Notes, or X-rays)	☐	☒
Home Address	☒	☐
Phone Number(s) (non-work)	☒	☐
Email Address (non-work)	☒	☐
Employee Identification Number (EIN)	☒	☐
Financial Information (e.g., checking account #/PINs/passwords, credit report, etc.)	☒	☐
Driver's License/State Identification Number	☐	☒
Vehicle Identifiers (e.g., license plates)	☐	☒
Legal Documents, Records, or Notes (e.g., divorce decree, criminal records, etc.)	☐	☒
Education Records	☐	☒
Criminal Information	☐	☒
Military Status and/or Records	☐	☒
Investigation Report or Database	☐	☒
Biometric Identifiers (e.g., fingerprint, voiceprint)	☐	☒
Photographic Identifiers (e.g., image, x-ray, video)	☐	☒
Other (Specify: Passport Information, known traveler number, redress number)	☒	☐

5. If Social Security Number (SSN) is checked in question 4, please answer the following:

a) Explain the business purpose requiring the collection of SSNs: N/A

b) Provide the legal authority which permits the collection of SSNs. N/A

c) Identify whether the SSN is masked or otherwise truncated as part of the outsourced service: N/A

6a. Please provide an estimate of the number of records maintained by the vendor for this contract that contain PII:

Estimated Number of Records Containing PII				
0 ☐	1-500 ☐	501-1,000 ☐	1,001 – 2,500 ☐	2,501 – 5,000 ☐
5,001 – 7,500 ☐	7,501 – 10,000 ☒	10,001 – 50,000 ☐	50,001 – 100,000 ☐	over 100,000 ☐

6b. If "0" was answered for 6a, please explain[3]: N/A

7. What are the sources of data (both PII *and* non-PII) for the outsourced service/project? How is the data derived?

Data Source[4] (List all sources that the Outsourced Provider collects, obtains or receives data from, as part of the services provided under the contract.)	**Type of Data Provided by Source & How It is Derived** (Describe the type of PII and non-PII data provided by each source. If PII is included in the data, list the specific PII elements, and explain how the PII is derived.)	**Does Data Include PII?**
FDIC Employees (Travelers) and FDIC/DOF or GetThere Travel Specialists	In order to access the GetThere OBE, the FDIC employee (traveler) first enters a user ID and password on the OBE login page. The employee may then establish or modify his/her GetThere user profile consisting of the personal information described in question 2. The employee also may add emergency contact information (full name, home address, and home telephone number) to his/her profile. Once the FDIC employee has established a user profile, authorized FDIC/DOF Travel Specialists may make edits or corrections to the profile as necessary. CWTSATO Travel Specialists may also make changes to the employee's profile, but only at the employee's direct request.	☒ Yes ☐ No
FDIC's Corporate Human Resources Information System (CHRIS)	The GetThere OBE system imports via Secure File Transfer Protocol (SFTP) the following PII from CHRIS for the purpose of creating profiles for employees: full name, EIN, home and office address, and office email address. On a biweekly basis, CHRIS also automatically securely transfers (via SFTP) a file to update active employee travel profile information (e.g., address change, separation from FDIC, etc.). If the employee separates from FDIC, the GetThere system automatically deletes his/her profile.	☒ Yes ☐ No

8. How will FDIC and/or the Outsourced Service Provider retrieve data or records as part of the outsourced service or project? Can data be retrieved using a personal identifier (e.g., name, address, SSN, EIN, or other unique identifier)?

The FDIC employee (traveler), authorized FDIC or CWTSatoTravel Specialists, and the GetThere OBE System Administrators may retrieve data using personal identifiers, such as the employee's name and EIN. The various data elements can be retrieved in the same manner in which they are input, i.e., via secure Internet connection, system login, and password.

9. In the Federal Register, under which Privacy Act Systems of Record Notice (SORN) does this system operate? Provide number and name.

---

[3] If the vendor has not received work to date for this contract and "0" is checked in 6a, please explain approximately how many records may be maintained by the vendor if they are awarded work under this contract in the future. Additionally, the Division responsible for this vendor must update this PIA to reflect the accurate number of records containing PII that the vendor maintains if this changes in the future.

[4] Examples of potential data sources include, but are not limited to: internal (FDIC) or external (non-FDIC) systems, websites, individual members of the public (e.g., customers, borrowers, etc.), FDIC employees, FDIC contractors, credit bureaus, commercial entities, public records, government agencies, etc.

General Services Administration SORN GSA/GOVT-4, *Contracted Travel Services Program* (74 FR 26700) and FDIC SORN 30-64-0012, *Financial Information Management Records* (80 FR 66996).

This completes the PTA.

- Do not complete the rest of the form, if the service provider is not processing or maintaining sensitive PII. This is the case, if you checked:
  - NOT APPLICABLE for question 3 and NO for all items in question 4; OR
  - Only Full Name in question 4.

- Continue completing the remainder of the form, i.e., Sections III thru VI in their entirety (questions 10 through 18), if the service provider is processing or maintaining sensitive PII. This is the case, if you checked:
  - YES for Social Security Number (SSN) in question 4; OR
  - YES for SSN or for Full Name in addition to one or more boxes in question 4.

- If you have questions or are unsure about whether or not you should complete the remainder of this form, please contact your Division ISM or the Privacy Program Office (privacy@fdic.gov).

SECTION III – DATA ACCESS AND SHARING

10. In the table below, specify the systems/applications and parties (FDIC and non-FDIC) that will access or receive PII data as part of the outsourced service/project.

PII Will Be Accessed By and/or Provided To:	Yes	No	If Yes, Explain How and Why the PII Will Be Accessed/Shared
10a. FDIC Outsourced Service Provider (OSP) Staff; OSP Subcontractors; and/or OSP Systems	☒	☐	OSP Staff and Subcontractors: CWTSatoTravel must provide a sufficient number of trained and experienced agents and other personnel and equipment necessary to assure the highest quality of service is provided at all times. CWTSatoTravel shall make confirmed reservations (domestic and international) for all modes of transportation, lodging, and rental vehicles. CWTSatoTravel shall confirm all reservations for official travel within one hour through an emailed itinerary. As noted previously, CWTSatoTravel subcontracts with GetThere to provide the OBE and manage online travel services on behalf of the FDIC. In this capacity, authorized GetThere Travel Specialists have the ability to view and update FDIC traveler profile data, which includes the PII specified in question 7, for purposes of establishing an employee profile and making or updating travel reservations on behalf of the employee. OSP Subcontractor System: The GetThere OBE system maintains the FDIC employee personal information specified in question 7 for the purposes of allowing FDIC employees to book and manage their travel reservations. The GetThere system also receives information directly from the FDIC, as specified in question 7, on a bi-weekly basis for updating, adding and deleting employee profiles.
10b. FDIC Personnel and/or FDIC Systems/ Applications	☒	☐	FDIC employees may access their own GetThere profiles and reservation data at any time. Only FDIC employees may use GetThere for booking government-approved travel and accommodations; FDIC contractors cannot use the system. This information includes some or all of the PII identified in questions 4 and 7. Authorized FDIC Travel Specialists within DOF have the ability to view and update FDIC traveler profiles in order to fulfill the business needs of managing employee records, such as removing separated employees' profile records from the active roles in GetThere. In addition, as stipulated in its contract with FDIC, CWTSatoTravel provides monthly management reports, some of which contain PII about FDIC travelers, to the FDIC Oversight Manager (OM)/Travel Specialist based on reservation data. These reports are provided via secure email to the FDIC Travel Specialist from the CWTSatoTravel Program Manager, US Military & Government Markets, and are stored on FDIC servers. In addition, the contractor makes all data available to the OM through CWTSato's Program Management

			Center (PMC), a secure web-based reporting application. All CWTSatoTravel reports are used for the management of Corporate travel to ensure compliance with federal regulations. The data that populates these reports is retrieved through the Sabre Global Distribution System (GDS) by CWTSatoTravel. Following are examples of reports containing PII that may be provided to the FDIC OM. • International Reservation Report/International Travel Report: Provides details on each traveler with reservation for international travel that has occurred or is scheduled to occur during the reporting period. The report includes traveler name, division/office, record locator, begin and end dates of travel, itinerary, airfare, and class of service. The purpose of the report is to ensure FDIC employee and Board member international travel complies with applicable Federal travel laws, regulations and policies; specifically, the Fly America Act, 49 USC Section 40118, requires employees, consultants, contractors and any other persons traveling for the federal government outside the United States via commercial air to travel by U.S. flag air carriers. • Refund Report: Provides details on all refunded air and rail tickets for each traveler, including, but not limited to, traveler name, name of airline, ticket number, the date the ticket was issued, ticket routing, last four digits of the credit card, air/rail fare, refund amount, date refund was processed/submitted to airline/Amtrak, and date refund receipt was provided to traveler. The purpose of the report is to provide details on credits received from the vendor for cancelled or changed travel arrangements for reconciliation and research purposes. • Premium Class Travel Report: Provides details on travelers with reservations that include segments booked in premium classes of service (business and first class). The report includes traveler name, division/office, dates of travel, itinerary, fare basis, total fare paid, invoice date and whether the entire trip was booked in premium class or if there was a combination of premium and coach class segments booked. The report also includes information required by the General Services Administration (GSA) for reporting annual premium class travel.[5] . This report provides a means of ensuring premium travel is appropriate and in accordance with GSA and FDIC travel requirements. • Hotel Booking Report: Provides details on each traveler's booked hotels, including, but not limited to, traveler name, division/office, region, hotel name, city and state, rate booked and number of nights booked,

[5] FDIC employees are required to submit and receive approval of FDIC Form 2500/06A, Premium Class Travel Authorization, before making travel arrangements.

			the GSA lodging per diem in that particular location, and the variance (expressed as a percentage) of the rate booked as compared to the GSA lodging per diem. This report is used for analysis of travel rates to ensure employee lodging rates are comparable when using non-GSA lodging. • Car Rental Report: Provides details on each traveler's booked cars, including, but not limited to, name of traveler, division/office, region, name of rental car company, type of rate booked (i.e. government), rate booked, number of days rented, pick up/drop off cities, and car size. This report is used to ensure compliance with Federal and FDIC travel policies. . Centrally Billed Government Travel Account Reconciliation Report: Provides details on all charges made to the FDIC's centrally billed Government Travel Accounts, including, but not limited to, passenger name, FDIC accounting data, routing booked, airfare booked, and fare basis. The purpose of this report is to reconcile expenses charged directly to the FDIC instead of an individual employee. • Traveler Location Report: In the event of a domestic or international disaster, the vendor must provide FDIC with a report showing the name, FDIC division/office, and name and address of hotel of all FDIC travelers in the affected area at the time of the disaster. This report can be used to track and locate employees in event of a disaster.
10c. Individual Members of the Public (e.g., bidders, investors, borrowers, customers, etc.)	☐	☒	*Not applicable.*
10d. Other Non-FDIC Entities/ Parties and/or Non-FDIC Systems/Applications	☒	☐	Third-Party Travel Providers: GetThere may need to share the following types of personal data with various third-party travel suppliers (such as airlines, hotels, train companies, rental car companies, online booking tool companies and safety and security tracking providers, as well as computer reservation systems) within the traveler's home country or in another country where the traveler may be traveling for the purposes of booking transportation and lodging: full name, date of birth, home address, phone number(s) (non-work), email address (non-work), financial information, passport information, known traveler number, and redress number. This data is shared through the Sabre Global Distribution System (GDS) and is encrypted during the automated exchange process. The third-party supplier stores the information in their internal databases for use in reservations, inventory, or property management. If the agents must call a third-party supplier to make reservations, then the exchange of information takes place over the phone. Payment/Credit Card Providers: GetThere may share the following types of personal data with credit card companies and other third parties for the purpose of making payments related to travel reservations: full name, home address, phone

			number(s) (non-work), email address, and financial information. Payment information is shared through the GDS (encrypted during exchange process) or direct phone calls.
10e. Federal, State, and/or Local Agencies	☒	☐	GetThere shares the following types of personal data about travelers with the U.S. Department of Homeland Security Transportation Services Administration (TSA): full name, date of birth, home address, phone number(s) (non-work), email address (non-work), financial information, passport information, known traveler number, and redress number. TSA requires this information for purposes of watch list matching, under the authority of 49 U.S.C. Section 114, and the Intelligence Reform and Terrorism Prevention Act of 2004. If the traveler does not provide this information requested by TSA within the GetThere OBE, they may be subject to additional screening to denied transport or authorization to enter a sterile area. TSA may share this information with law enforcement or intelligence agencies or others under its published system of records notice.[6]
10f. Other	☐	☒	*Not applicable.*

11. If data will be provided to, shared with, or maintained by non-FDIC entities (such as government agencies, contractors, or Outsourced Information Service Providers), have any of the following agreements been issued?

Data Protection and/or Sharing Agreements	Yes	No
FDIC Confidentiality Agreement (Corporation)	☒	☐
FDIC Confidentiality Agreement (Individual)	☒	☐
Non-Disclosure Agreement (NDA)	☐	☒
Memoranda of Understanding (MOU)	☐	☒
Information Sharing Agreements (ISA)	☐	☒
Authentication Risk Assessment	☐	☒
Other Applicable Agreement(s) (*Specify*: _____)	☐	☒

If you answered NO to any item above, please provide additional information if available: CWTSatoTravel was mandated for use by government agencies by GSA, which produces and maintains the security artifacts.

[6] For more information or to view the TSA system of records notice and the privacy impact assessment, visit www.tsa.gov.

SECTION IV – NOTICE AND CONSENT

12. Do individuals have the opportunity to decline to provide information or to consent to particular uses of their information (other than required or authorized uses)?

☐ No. Individuals do not have the opportunity to "opt out" of providing their data and/or consenting to particular uses of their information.

☒ Yes. Individuals have the opportunity to decline to provide their personal data or to consent to particular uses of their information.

FDIC employees have the opportunity to opt out of providing PII, as FDIC does not require employees to use of the online booking system in order to book FDIC travel. Employees may book FDIC travel on their own and then seek reimbursement from the Corporation later. However, employees who elect to use the online booking system cannot opt out of providing PII, as this information is necessary to book and manage reservations.

13. If PII is being collected via a public-facing website and/or application as part of this outsourced service, has the Outsourced Information Service Provider posted any of the following types of privacy policies or Privacy Act notices?

☐ No
☒ Yes
- ☐ Link to FDIC Privacy Policy
- ☒ FDIC Privacy Act Statement
- ☒ Contractor Privacy Policy or Statement
- ☐ No Privacy Policy has been posted

☐ Not applicable

SECTION V – DATA SECURITY AND ACCURACY

14. Please assert what administrative procedures and technical safeguards are in place to protect sensitive PII data in the Outsourced Information Service Provider's care.

☒ The vendor has gone through the security review required by the FDIC's Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical, and administrative security measures to safeguard FDIC-provided PII and other sensitive data. If it has gone through the Methodology, has it been approved? ☐ NO ☒ YES

☒ The FDIC conducts background investigations (BIs) on key CW Government Travel Inc. and subcontractor personnel prior to their beginning work on the contract.

☒ CW Government Travel Inc. and its subcontractors are subject to periodic compliance reviews by FDIC. Per the contract, scheduled and unannounced inspections and assessments of the Outsourced Service Provider's facilities, personnel, hardware, software and its security and privacy practices by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. General Accountability Office (GAO). These inspections may be conducted either by phone, electronically or in-person, on both a pre-award basis

and throughout the term of the contract or task order, to ensure and verify compliance with FDIC IT security and privacy requirements.

☒ Other (Explain any other administrative and/or technical safeguards in place to protect PII data in the Outsourced Information Service Provider's care.) ***Attach the Contract Clause Verification Checklist to the back of this form*.**

CW Government Travel Inc. assumes the risk for ensuring appropriate security controls are maintained in support of E2 Solutions Operational status. They ensure protection for the application OBE and the information contained therein. E2 Solutions complies with all pertinent requirements of Federal law and policy.

15. What are the procedure(s) for ensuring that the information maintained is accurate, complete and up-to-date?

☒ Data is collected directly from individual FDIC employees and FDIC Travel Specialists. As such, the FDIC and CW Government Travel Inc. rely on the individuals and the FDIC/DOF Travel Specialists to provide accurate data.

☐ The vendor/contractor works with FDIC to verify the integrity of the data [before, in conjunction with, and/or after] inputting it into the system or using it to support the project.

☐ As necessary, an [authorized user or administrator] of the [System/Project Name] checks the data for completeness by reviewing the information, verifying whether or not certain documents or data is missing, and as feasible, updating this data when required.

☒ Other (*Please explain*.)

The traveler is responsible for verifying the accuracy of all traveler profile data and reservation data they enter into GetThere (OBE). The online system will automatically check profile data for completeness, prompting the individual to enter additional data when required fields are not completed.

The traveler will check reservation data for completeness. The online booking engine will prompt the individual entering reservations, but the automated system will not know whether a traveler requires a hotel room or not; it will not know whether a rental car is required, etc. It is ultimately the traveler's responsibility to assure that reservations are complete and accurate.

Authorized FDIC/DOF and GetThere Travel Specialists have the ability to verify and update accounts as needed.

16. In terms of assuring proper use of the data, please assert whether the following statements are true for the Outsourced Information Service Provider.

☒ Within FDIC, the CWTSatoTravel Program Manager/Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager (ISM) are collectively responsible for assuring proper use of the data. In addition, it is every FDIC user's responsibility to abide by FDIC data protection rules which are outlined in the FDIC's Information Security and Privacy Awareness training course which all employees take annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

☒ Additionally, the Outsourced Information Service Provider is responsible for assuring proper use of the data. Policies and procedures have been established to delineate this responsibility, and the vendor has designated the CIO/E-Gov Travel Systems to have overall accountability for ensuring the proper handling of data by GetThere personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. Access to certain data may be limited, depending on the nature and type of data

The E-Gov Solutions CIO has responsibility for assuring the access controls are in place within the GetThere system through continuous monitoring activities. GetThere is a core component of E2 Solutions which is not inside the accredited boundary. CW Government Travel Inc. assumes the risk for ensuring appropriate security controls are maintained in support of E2 Solutions operational status.

All user sessions between the FDIC user's workstation and GetThere web server are encrypted using a FIPS-compliant encrypted connection. The individual users are logically separated within the GetThere OBE. System login, passwords, and a FIPS-compliant encrypted connection are in place to protect the data and prevent unauthorized access. Security controls are in place to restrict the data to only those users with a "need-to-know." To initiate any travel process, travelers access the online system via the Internet and login using user ID and password. With a valid login, the system presents travelers with a menu for managing travel profiles and reservations.

System security banners are displayed to users upon logging in, warning them that the E2 Solutions system contains information covered by the Privacy Act and advising them of their obligations to protect the system and data it contains in accordance with Federal law and policy. These warning banners must be acknowledged by the user prior to being granted system access.

☒ The Outsourced Provider must comply with the Incident Response and Incident Monitoring contractual requirement.

☐ None of the above. *(Explain why no FDIC staff or Outsourced Information Service Provider personnel have been designated responsibility for assuring proper use of the data.)*

SECTION VI – DATA RETENTION AND DISPOSAL

17. Where will the Outsourced Service Provider store or maintain the PII data identified in question 4? Describe both electronic and physical storage repositories, as applicable.

The employee PII data will be used, processed, and then stored in the GetThere servers.

18. Specify the period of time that data is retained by the Outsourced Service Provider and the specific procedures for disposing of or returning the data at the end of the retention period or contract, whichever is first.

GetThere data exists only in electronic form. The vendor, including its subcontractor, will permanently delete the data at the end of the prescribed records retention period as specified below. When user accounts are deleted from the active database, their respective trips/data are

also deleted from the active database; however, this information will be stored in the archival files for the periods specified below.

Data will be stored in the archival files for six (6) years and three (3) months after being deleted from the active database, in accordance with National Archives and Records Administration (NARA) General Records Schedule 9 for Travel and Transportation Records and General Records Schedule 20 for Electronic Records. NARA guidelines regarding records disposition are also followed. As specified in its contract with FDIC, the vendor shall prevent the purging of historical records prior to the proper retention period, and permit purging only of those records authorized for disposal by NARA per 36 CFR 1228 and 1234.

Further, the vendor's contract with FDIC stipulates that the vendor must provide FDIC online access to detailed transaction information for a minimum period of 36 months, and permit access to archived detailed transaction information for a period of 6 years and 3 months.