Travel Agent Services (561510)
Statement of Work (SOW)

Refresh 23

Contents

1 INTRODUCTION

Effective on December 18[1], 2024, Refresh 23 of the Multiple Award Schedule (MAS) Travel Agent Services Schedule 561510, requires Contractors on this schedule will be required to meet the following requirements as defined in this Statement of Work (SOW). The information below specifies which Sections are applicable to all Contractors on this schedule and which Sections are applicable to Contractors supporting agencies that will be using the ETSNext Technology MSP.

The document has been structured in the following format.

- **Sections 2 through 7**, *Scope, Period of Performance, Type of Contract, Place of Performance, Pricing Schedule - Management Service Fee, and Deliverables* are related to the schedule itself and applicable to **All Contractors**.
    - Section 7 Deliverables is broken down into *Deliverables for All Contractors* and *Security Deliverables for Contractors supporting the ETSNext* Technology Managed Service Provider (MSP)
- **Sections 8 through 17**, *Definitions, Description of Work, Scope & Complexity, General Requirements, Commercial Security Standards, Protection of Individual Privacy, Personnel Security, Service Level Agreements, TMC Implementation & Transition In & Out Services* are requirements that applicable to All Contractors on the Schedule.
- **Section 18,** *ETSNext Requirements* are **applicable only to Contractors supporting agencies using the ETSNext Technology MSP** including agencies required to use the ETSNext Technology MSP according to the Federal Travel Regulation (FTR) and agencies that are not required to but use the ETSNext Technology MSP either through their own agreement with the ETSNext Shared Service Program Management Office (PMO) or those supported by the Federal Agency Cross Service Providers. The Cross Service Providers are:
    - Department of Transportation (DOT), Federal Aviation Administration (FAA), Enterprise Service Center (ESC)
    - Department of the Interior (DOI), Interior Business Center (IBC)
    - Department of Transportation (DOT), Fiscal Service (FS), Administrative Resource Center (ARC)
- **Sections 19 through 27**, *City Pair Program, Fly America Act, Open Skies Agreements, Lodging, Rail & Amtrak, Ground Transportation, GSA SmartPay Support, Reports, and Explanatory Codes* are Laws, Policies and Regulations, related to Federal travel and are applicable to **All Contractors** on the Schedule.
- **Section 28** Standard Services to be Priced for the ETSNext Technology MSP, DOD, and Other Users of 561510 are the services to be priced and added to a ***Contractor's Terms and Conditions and Price Lists*** **for Contractors supporting agencies using the ETSNext Technology MSP** including agencies required to use the ETSNext Technology MSP according to the Federal Travel Regulation (FTR) and agencies that are not required to but use the ETSNext Technology MSP either through their own agreement with the ETSNext Shared Service Program Management Office (PMO) or those supported by the Federal Agency Cross Service Providers. The Cross Service Providers are:
    - Department of Transportation (DOT), Federal Aviation Administration (FAA), Enterprise Service Center (ESC)
    - Department of the Interior (DOI), Interior Business Center (IBC)

[1] Or when Refresh 23 is published by the Multiple Award Schedule Program Management Office

  - Department of Transportation (DOT), Fiscal Service (FS), Administrative Resource Center (ARC)

The Standardized Services may be used by others authorized users of the schedule in the future.

- The **Appendices**, A - Schedules and Task Order Information, B - Lodging Report, C - GSA Programs and Government Travel Programs, and D - Security Guidance provide additional information and/or guidance on items that may be useful or beneficial to the Contractors on the Schedule. These Appendices do not change the requirements in this SOW or in ordering agency Task Orders.
- **Attachment 1 – Data Elements & FedRamp** provides a set of:
  - Data Elements to be captured and transferred:
    - Data elements may be transferred to GSA, the ordering agency, and the ETSNext Technology Managed Service Provider (MSP)
- **Attachment 2 – Travel User Guide v8** is the instruction manual for the GSA Report Tool for Regulatory Reporting

2 SCOPE

The Travel Management Company (TMC), hereafter referred to as the Contractor, provides commercial services for the provision of travel agent services which includes, but is not limited to travel arrangements, reservations, ticketing and fulfillment (transactions), including traveler support, for air, rail, lodging, and rental car. The contractor may also provide ancillary services, which may include, but is not limited to business services, delivery services, destination services, frequent traveler and loyalty programs support, invoicing, Centrally Billed Account (CBA) reconciliation, profile management, quality assurance & control, and standard travel management reporting.

If the Contractor is submitting new services and pricing, and requires a new eMod, please refer to the Modifications and mass modifications page. For contract support items such as delivery fees, emergency or after hour services, VIP TMC services, etc., please refer to the Price Proposal Template (PPT) for SIN Ancillary.

The Service Contract Labor Standards (SCLS) applies to Schedule Item Number (SIN) 561510 and each individual Task Order (TO) must have an applicable wage determination in accordance with the SCLS.

3 PERIOD OF PERFORMANCE (POP)

The Period of Performance (POP) of Task Orders (TO), under this schedule, will be established in each specific TO.

4 TYPE OF CONTRACT

The contract type will be established in each specific TO.

5 PLACE OF PERFORMANCE

The place of performance of TOs will be specified in each specific TO.

However, it will primarily be at the Contractor's location. An agency may request on-site meetings, as necessary, following the agency accepted Transition Microsoft Project Plan (MPP) or similar project planning software. For certain agencies, e.g. Department of State, the place of performance may be at multiple and/or different locations and could include subcontractor locations Outside the Continental United States (OCONUS).

If requested at the ordering agency TO Level, the Contractor shall supply staffing at on-site locations in Government-owned facilities.

6 PRICING SCHEDULE

6.1 INDUSTRIAL FUNDING FEE (IFF)

On December 31, 2019, as defined in Refresh 24, the Industrial Funding Fee (IFF) for Transaction B (Lodging and/or Car Rental Reservations) was changed from $1.50 to 0.75% of sales. The IFF for Transaction A (Air and/or Rail Ticket with or without Lodging and/or Car Rental Reservations) remains at $3.10.

All reportable sales for Transaction B shall be reported under SIN **Ancillary**. Transaction A shall continue to be reported under SIN **561510**.

6.2 MANAGEMENT SERVICE FEE (Optional)

For services proposed at the task order level, under the Contractor's GSA MAS 561510 *Travel Agent Services*, the Contractor may propose an alternate pricing approach. When proposing an alternate pricing approach, based on other than a per transaction or unit (labor hour category) model, e.g., management service fee, the Contractor, shall:

1. When required at the task order level, the Contractor shall submit a fully burdened Management Service Fee (MSF) and Point of Sale (POS) unit prices (ticketing and fulfillment / transaction fees) that are based on, and do not exceed, their awarded GSA Multiple Award Schedule (MAS) 561510 Travel Agent Services, pricing for the base and option periods of performance. Prospective offerors do not have to have an actual MSF on their MAS price lists. Rather, prospective Offerors may use any combination of the products/services currently awarded in their GSA MAS SINS, to develop the MSF and POS prices for the base and option periods. The Offeror must clearly identify which of their MAS product/service offerings corresponds to the proposed MSF and POS pricing within their price quote and provide a description explaining the compilation of products/services included in the MSF, how the MSF will be assessed, the associated costs for those services on a fixed periodic payment basis (monthly, quarterly, yearly, etc.), and the frequency of payment. Include information on the benefits of using the proposed alternate pricing model.
2. For purposes of this Schedule, Offerors shall include and report an **Industrial Funding Fee (IFF) of 0.75%** (.0075) in its proposed MSF (value of the contract) and/or POS unit prices (transaction fee) for all products and services offered, **excluding Transaction A CLINs** (reservations that include air/rail). The Contractor shall meet fluctuations in the estimated volume at the Firm Fixed Prices (FFPs) as established in the awarded agency TO. Such surges or any other fluctuations in the quantities in the transactions ordered are not considered a change and the contractor shall not be entitled to any adjustment in price.
3. Please note that the **Industrial Funding Fee (IFF)** is $3.10 for each instance involving an airline/rail transaction (i.e., **Transaction A**). If an alternative pricing model is offered and incorporates airline/rail transactions (i.e., **Transaction** A), these transactions and a IFF (i.e., $3.10 per airline/rail transaction) shall be reported under SIN 561510.
    a. In other words, a proposal based on other than per transaction model (e.g. Management Service Fee or another alternative pricing model) must keep track of and report each **Transaction A** for IFF purposes, provide this information to the ordering agency, and reported in accordance with the GSAM 552.238-80, Industrial Funding Fee and Sales Reporting.

7 DELIVERABLES

The following deliverables are required to be submitted to GSA.

Table 1 - Deliverables

Name	Content	Frequency	Report Period	Due Date	Delivered To:
All Contractors					
Industrial Funding Fee (IFF) & Sales Reporting	Report of Transaction A and all other Product and Services Sold except for Debit Memos	Quarterly	January 1 and March 31	April 30	https://vsc.gsa.gov/vsc/ tmcstrategy@gsa.gov
Industrial Funding Fee (IFF) & Sales Reporting	Report of Transaction A and all other Product and Services Sold except for Debit Memos	Quarterly	April 1 and June 30	July 30	https://vsc.gsa.gov/vsc/ tmcstrategy@gsa.gov
Industrial Funding Fee (IFF) & Sales Reporting	Report of Transaction A and all other Product and Services Sold except for Debit Memos	Quarterly	July 1 and September 30	October 30	https://vsc.gsa.gov/vsc/ tmcstrategy@gsa.gov
Industrial Funding Fee (IFF) & Sales Reporting	Report of Transaction A and all other Product and Services Sold except for Debit Memos	Quarterly	October 1 and December 31	January 31	https://vsc.gsa.gov/vsc/ tmcstrategy@gsa.gov
Task Orders	Task Orders awarded under this schedule and all modifications	Not Applicable	Not Applicable	Five (5) Business Days after Execution	onthego@gsa.gov tmcstrategy@gsa.gov
Annual Total Travel Report	See Table 2 Annual Total Travel Report	Yearly	October 1 through September 30	15th Calendar Day after the end of the fiscal year.	tmcstrategy@gsa.gov
Agency CPP Travel Report	See Table 3 Monthly Agency / CPP Travel Report	Monthly	Previous Month	15th Calendar Day after the end of the month	tmcstrategy@gsa.gov

Name	Content	Frequency	Report Period	Due Date	Delivered To:
CPP Audit Report	See Table 4 CPP Audit Report Monthly	Monthly	Previous Month	15th Calendar Day after the end of the month	tmcstrategy@gsa.gov
Lodging Report	List of hotel related data elements per Table 5 Lodging Report Monthly	Monthly	Previous Month	15th Calendar Day after the end of the month	lodging@gsa.gov
Standard Call Center Metrics (Supporting Customer Service Key Performance Indicators (KPIs))	See Table 5, Item 24	Monthly	Previous Month	15th Calendar Day after the end of the Month	tmcstrategy@gsa.gov
Security Deliverables for Contractors Supporting Agencies Using the ETSNext Technology MSP					
CUI Nonfederal System Security and Privacy Plan (SSPP) Template	Documents the controls to meet the standards as identified in the current and future versions of NIST 800-171. Refer to *Appendix A* of Guide for details.	Initial submission six (6) months after award and then Yearly. Also prior to a significant change to the nonfederal system's security posture.	Not Applicable	Two months prior to completion of the government fiscal year, ending on September 30. Due date is the last workday of July.	Secure portal provided by government or vendor due to CUI
Plan of Action and Milestones (POA&M)	Also referred to as a corrective action plan, is the authoritative agency management tool for documenting the remediation actions of system risk. Refer to *Appendix A* and *Section 2.5 Phase 5 Monitor* of Guide for details.	Initial submission NLT 30 calendar days after award and then Quarterly. Also prior to a significant change to the nonfederal system's security posture.	Previous Quarter	One month prior to the completion of each quarter in the government fiscal year, ending on September 30. Due dates are the last workday of each month listed below: Q1 – November Q2 – February Q3 – May Q4 – August	Secure portal provided by government or vendor due to CUI

Name	Content	Frequency	Report Period	Due Date	Delivered To:
Security Assessment Report (SAR)	A Security Assessment Report is a document that demonstrates that an agency has performed due diligence in testing security controls. Refer to *Appendix A* of Guide for details.	Initial submission and then every three (3) years. Also prior to a significant change to the nonfederal system's security posture.	Not Applicable	Two (2) months prior to the completion of the government fiscal year, ending on September 30. Due date is the last workday of July.	Secure portal provided by government or vendor due to CUI
Vulnerability Scanning Reports	A vulnerability scan report is a document generated by a vulnerability scanner that identifies potential security risks in an organization's systems and applications. Refer to *Appendix A* and *Section 2.5 Phase 5 Monitor* of Guide for details.	Quarterly. Also prior to a significant change to the nonfederal system's security posture.	Previous Quarter	One month prior to the completion of each quarter in the government fiscal year, ending on September 30. Due dates are the last workday of each month listed below: Q1 – November Q2 – February Q3 – May Q4 – August	Secure portal provided by government or vendor due to CUI
Privacy Threat Assessment (PTA)	A PTA is the means for analyzing whether an IT system collects, maintains, or uses PII for identifying appropriate privacy protection measures. The PTA questionnaire is also used to identify other potential categories of Controlled Unclassified Information (CUI). Refer to *Appendix A* of Guide for details.	Annually. Also prior to a significant change to the nonfederal system's security posture.	Not Applicable	Two months prior to completion of the government fiscal year, ending on September 30. Due date is the last workday of July.	Secure portal provided by government or vendor due to CUI
Privacy Impact Assessment (PIA)	A Privacy Impact Assessment, or PIA, is an analysis of how	Annually. Also prior to a significant	Not Applicable	Two months prior to completion of the government	Secure portal provided by government or vendor due to CUI

Name	Content	Frequency	Report Period	Due Date	Delivered To:
	personally identifiable information is collected, used, shared, and maintained. Refer to *Appendix A* of Guide for details.	change to the nonfederal system's security posture.		fiscal year, ending on September 30. Due date is the last workday of July.	
Penetration Test	A test methodology in which assessors, typically working under specific constraints, attempt to circumvent or defeat the security features of a system. Refer to *Appendix A* and *Section 2.5 Phase 5 Monitor* of Guide for details.	Annually. Also prior to a significant change to the nonfederal system's security posture.	Not Applicable	Two months prior to completion of the government fiscal year, ending on September 30. Due date is the last workday of July.	Secure portal provided by government or vendor due to CUI
CUI Nonfederal System Architecture Briefing	The briefing should be appropriate for an hour discussion with the agency. Vendors are encouraged to provide supplemental / supporting documents (e.g., authorization boundary diagram, data flow diagrams, console screenshots) to augment the detail provided in the slide briefing. A briefing slide template with instructions will be provided.	Initial submission. Also prior to a significant change to the nonfederal system's security posture.	Not Applicable	30 days after contract award. For proposed significant changes, as earliest as possible to solicit GSA input.	Secure portal provided by government or vendor due to CUI. Slide deck submitted. Provide presentation/briefing
CUI Nonfederal Memorandum of Record for Use Template	Memo authorizing use of vendor system for agency use based on approval of authorization	Annually. Also prior to a significant change to the	Not Applicable	Issued upon approval of the initial authorization package.	Secure portal provided by government or vendor due to CUI

Name	Content	Frequency	Report Period	Due Date	Delivered To:
	package (refer to above deliverables.)	nonfederal system's security posture.		Subsequently, prior to the anniversary of the last authorization.	
Optional Documentation Security Deliverables for Contractors Supporting Agencies Using the ETSNext Technology MSP					
CUI Nonfederal Vendor Kickoff Overview Slides	CUI nonfederal security and privacy engagement overview provided by agency security team.	Optional - upon initial vendor engagement	Not Applicable	Optional	Attend agency presentation
CUI Nonfederal System Work Breakdown Structure (WBS)	WBS template provided by agency where timelines and responsibilities are defined for CUI Nonfederal NIST SP 800-171 process.	Optional - upon initial vendor engagement	Not Applicable	Optional - recommend completing within 30 days of contract award	Secure portal provided by government or vendor due to CUI
Example Security/Privacy Control Statements	Provide examples of control statements that will be used in the SSPP	Optional - if vendor wants feedback before completing SSPP	Not Applicable	Optional - at the start of SSPP preparation	Secure portal provided by government or vendor due to CUI

8 DEFINITIONS

Abandoned Call: An abandoned call is a call, or other type of contact, made to a call / contact center that is ended while a person is on hold and before any conversation occurs.

Accommodated Travel Management Company (ATMC): Under the E-Gov Travel Services (ETS) 2 program, an Accommodated TMC is a TMC that is under contract directly with the agency, usually through the MAS. The ATMC works closely with the ETS contractor to supply a full range of travel services as described herein and within the customer agency task order.

Airline Reporting Corporation (ARC): An airline-owned company serving the travel industry with financial services, data products and services, ticket distribution, and settlement in the United States, Puerto Rico, and the U.S. Virgin Islands.

Application Programming Interface: APIs are mechanisms that enable two software components to communicate with each other using a set of definitions and protocols. For example, the weather bureau's software system holds daily weather data. The weather app on your phone "talks" to this system via APIs and shows you daily weather updates on your phone.

API stands for Application Programming Interface. In the context of APIs, the word Application refers to any software with a distinct function. Interface can be thought of as a contract of service between two applications. This contract defines how the two communicate with each other using requests and responses. Their API documentation has information on how developers are to structure those requests and responses.[2]

Auto-cancellation: The cancellation of an un-ticketed City Pair Program reservation prior to its scheduled departure. An un-ticketed coach class City Program reservation (i.e., YCA and _CA) will auto-cancel 48 hours prior to the scheduled departure date and time. This only applies to reservations booked 72 hours or more before the scheduled departure. Reservations made less than 72 hours prior to the scheduled departure time may be exempt and may require ticketing six (6) hours before the scheduled departure at the carrier's discretion.

An un-ticketed business class or premium economy class City Pair Program reservation (i.e., _CP and _CB, respectively) will auto-cancel seven (7) calendar days prior to the scheduled departure date and time. This only applies to reservations booked eight (8) calendar days or more before the scheduled departure. Reservations made seven (7) calendar days or less prior to the scheduled departure time may be exempt and may require ticketing six (6) hours before the scheduled departure at the carrier's discretion. There are no fees or penalties associated with auto-cancellation of a reservation or rebooking a reservation that was subjected to auto-cancellation.

Average speed of answer (ASA): Refers to the time it takes for calls to be answered from the instant a customer is placed in a queue to the moment an agent answers the call. This doesn't include the time spent routing a customer to the appropriate queue, or time spent interacting with an interactive voice response system. ASA does include the time spent while the phone is ringing for agents.

Billing and Settlement Plan (BSP): A service provided by the International Air Transport Association (IATA). BSP is a system designed to facilitate and simplify the selling, reporting and remitting procedures of IATA Accredited Passenger Sales Agents, as well as improve financial control and cash flow for BSP Airlines.

[2] What is an API from Amazon Web Services.

Centrally Billed Account (CBA): A travel card/account set up by the GSA SmartPay® contractor at the request of the agency/organization. These may be card, cardless, or virtual accounts. Payments are made directly to the GSA SmartPay® contractor by the agency or organization.

Churning: The excessive changing, rebooking, and canceling of the same itinerary, usually in the same Passenger Name Record (PNR) but may be accounted for with multiple PNRs, to hold the reservation. To avoid and prevent churning when doing cost estimates, it is best practice to price the segment then cancel the segment if it's determined the TMC or Traveler won't be purchasing the segment.

City Pair Program (CPP): GSA's procurement program for air passenger transportation services. A GSA SmartPay® affiliated card, including the Individually Billed Account (IBA), Centrally Billed Account (CBA), card, Tax Advantage Card, or a Government Transportation Request (GTR) are the only forms of payment acceptable under the City Pair Program for official travel.

Common Carrier (Carrier): Types of common carrier authorized – airline, train, ship, bus, or other transit system. The basic requirements for using common carrier transportation fall into three categories: a.) Using contract carriers, when available and if a government agency is a mandatory user of GSA's CPP. b.) Using coach class (economy) service, unless other than coach class is authorized. c.) Mandatory use of U.S. Flag Carrier (or ship) service for air or ship passenger transportation.

Contract Fare: The Federal Government awarded airfares as it pertains to the CPP Contract or other contract fares negotiated by the Federal Government. CPP Contract fares include Unrestricted (YCA), Capacity Controlled (_CA), Contract Business (_CB), and Contract Premium Economy (_CP) fares.

Continental United States (CONUS): Within the forty-eight (48) contiguous States and the District of Columbia.

Core Hours (Continental United States (CONUS)): Monday through Friday, 7:00 a.m. through 10:00 p.m., U.S. Eastern time, without supplementary costs to the Government.

Core Hours OCONUS: Core Hours OCONUS will be defined at the agency TO level.

Cost Constructed Travel: As defined in the Foreign Affairs Manual (FAM)Travel based on a cost comparison between the cost of official (i.e., direct) travel and the cost of personal (i.e., indirect) travel. When cost constructing travel, the traveler can only claim the cost of the fare(s) the U.S. Government would have paid to the contract and/or common carrier or the cost of the commercial fare(s) the traveler actually paid to common carriers, whichever is less.

Any deviation from the most economical, direct usually traveled route for personal reasons requires a cost construct, including:

- Different origin or destination
- Different routing (requests to stop in a different city en route)
- Different carrier
- Different mode of transportation
- Different class of service (i.e., premium economy, business, first)[3]

Constructive cost, as defined by the **Federal Travel Regulation (FTR)**[4], is the sum of travel and transportation expenses the employee would reasonably have incurred for round-trip travel between

[3] Definition from FAM 511.3
[4] From the FTR 301-70.506 (b)

the official station and the alternate location plus per diem calculated for the appropriate en route travel time. The calculation will necessarily involve assumptions. Examples of related expenses that could be considered constructive costs include, but are not limited to, taxi and TNC fares, baggage fees, rental car costs, tolls, ferry fees, and parking charges.

This service may be offered if personal cost construct services do not impede the official travel service levels under the contract.

Debit Memo: Any written or electronically transmitted request, from a carrier (airline) to a TMC, for payment of any obligation arising under the ARC *Agent Reporting Agreement*, including penalties and fees charged including, but not limited to inaccurate reporting, prohibited booking practices, and ticketing in violation of applicable fare and tariff rules. Failure to pay a Debit Memo sent to it by a carrier may result in termination by the carrier of its appointment of the TMC as its agent, and withdrawal of its airline identification plate, effectively preventing the TMC from any further ticketing of reservations on the carrier.

Circumstances that may cause a federal agency to receive a request to pay for a debit memo, due to traveler behavior, may include:

- Churning
- Duplicate Booking (Traveler Made)
- Other Traveler behaviors, e.g., back-to-back ticketing, unused flight legs to obtain a lower fare.

Circumstances that cause a TMC to receive a debit memo, that are not the responsibility of the agency, may include:

- Churning
- Commission recalls from refunds.
- Duplicate Booking (TMC Made)
- Incorrect faring
- Incorrect refund calculation

Defense Travel Management Office (DTMO): Serves as the single focal point for commercial travel within DoD with central oversight for travel programs, travel policy and implementation, travel card program management, customer support and training, functional oversight of the Defense Travel System (DTS). For additional information, please visit https://www.travel.dod.mil/About/.

DoD Preferred®: Is managed by the Defense Travel Management Office (DTMO) under section 642 of the FY21 National Defense Authorization Act, which provides DoD the authority to direct travelers to utilize specific types of lodging. DoD focuses primarily on a high level of quality for the program and participating hotels to ensure Duty of Care for DoD travelers. The program strategically sources commercial lodging properties that are required to meet specific quality, safety, and security requirements, and provide traveler conveniences and amenities at a rate that is a minimum of 10% below per diem. The number of properties selected for the program is determined by the estimated amount of lodging needed by DoD for DoD Personnel in an area. For additional information, please visit https://www.travel.dod.mil/Programs/Lodging/DoD-Preferred-Commercial-Lodging/Become-a-DoD-Preferred-Hotel/, which provides more information on the program.

Defense Travel System (DTS): DoD's current fully integrated, automated, end-to-end travel management system that enables DoD travelers to create authorizations (TDY travel orders), prepare reservations,

receive approvals, generate travel vouchers, and receive a split reimbursement between their bank accounts and the Government Travel Charge Card (GTCC) vendor. This solution may be replaced in the future as part of the DTMO's Defense Travel Modernization (DTM).

Dual Fares: In certain markets, there are two awarded CPP fares, including an unrestricted fare (YCA), and a capacity-controlled fare (_CA) with the number of seats available for this fare as the only restriction. Use of either fare satisfies the requirement to use the contract carrier. The blank before CA (_CA) refers to an alpha character variable that may be applied by various airlines.

Duplicate Booking: Other reservations (bookings – e.g., air, rail, lodging, or rental car) that cannot logically be used by the traveler, which are similar or identical to another reservation for the same traveler contained in one or more PNR(s). Duplicate bookings (e.g., air, rail, lodging, rental car) are subject to cancellation without notice by the affected supplier, Global Distribution System (GDS), or TMC and can result in additional penalties and charges, in the form of Debit Memos, to the TMC by the affected carrier that may then become a financial obligation to the Federal agency or the traveler. See **Debit Memo**.

Embedded TMC (ETMC): A TMC that is a subcontractor to an E-Gov Travel Service 2 (ETS2) contractor that supplies a full range of TMC services, as described within the ETS2 Master Contract, and as specifically ordered through the customer agency's ETS2 task order. **There will not be embedded TMCs as part of the ETSNext Technology MSP.**

Emergency Travel Service: Emergency travel service (sometimes referred to as "*Last Minute Travel*") provides reservation and ticketing support for travel needs meeting the following criteria: a) the call occurs before or after TO - defined established **Core Hours** and b) the travel will commence within the following 24 hours or C) the need to travel arises over the weekend or during a holiday for travel that will commence over the weekend or on the next business day, and the traveler cannot wait until the next business day to process reservations.

E-Gov Travel Service (ETS, including ETS2, & ETSNext): The E-Gov Travel Service (ETS) is a government-wide, web-based, and world-class travel management service managed by GSA. This streamlined service continually applies commercial best practices to realize travel efficiencies and deliver a transparent, accountable, and sustainable service that yields exceptional customer satisfaction.

> **ETS2:** Is GSA's current contracted web-based service used by the civilian federal agencies for T&E management. ETS2 is a dual award Indefinite Delivery Indefinite Quantity (IDIQ) contract that allows travelers to create authorizations (TDY travel orders), prepare reservations, receive approvals, generate travel vouchers, and receive a split reimbursement between their bank accounts and the GSA SmartPay® vendor. ETS2 expires on June 3, 2027.
>
> **ETSNext:** E-Gov Travel Service Next Generation (ETSNext) is the third generation of electronic Government travel services (ETS) that will support the missions of Government agencies through an intuitive and streamlined platform that delivers a secure and positive customer experience while mitigating transition costs and risks. GSA's Federal Acquisition Service (FAS) is buying a configurable, commercial T&E Technology Managed Service to be deployed and centrally managed Government-wide. The T&E technology managed service includes planning, authorizing, booking, and vouchering for T&E expenses as well as providing audit and reporting services and ensuring travel is performed in compliance with travel regulations. The ETSNext Technology MSP will also provide security, integration services, data management, support services (e.g., training, helpdesk, etc.), program management, change management, and transition services under a fully managed shared services model. The ETSNext Technology MSP will replace ETS2 when it expires on June 3, 2027. Agencies will begin transitioning to the

ETSNext Technology MSP Shared Service beginning FY 24 or FY 25 and continue to transition through the end of ETS2, on June 3, 2027, with a goal of completing the transition, for all agencies, in February 2027.

Explanatory Codes/Exception Codes: Codified explanatory notations, recorded in the PNR, that document, among other things, reasons for certain airline, hotel or rental car travel options that are selected by the federal traveler, including policy deviations. Also known as reason codes, certain required explanatory codes, for the GSA City Pair Program, are defined for the Schedule and included in the section Explanatory Codes below.

Federal Fiscal Year: October 1 through September 30.

Federal Holiday: United States Federal Government holidays. Information about United States Federal Holidays is located at the following: http://www.opm.gov/Operating_Status_Schedules/fedhol/.

FedRooms®: Provides Federal Travel Regulation (FTR)-compliant hotel rooms at or below per diem with standard amenities for federal government travelers. Agencies should utilize FedRooms® when booking lodging for official duty travel to take advantage of the benefits and protections. For more information visit www.gsa.gov/fedrooms.

Federal Travel Regulation (FTR): Implements statutory requirements and Executive branch policies for travel and relocation for all Title 5 Executive Agency employees. Federal civilian employees and others authorized to travel at the government's expense must follow the policies defined in the FTR. The FTR includes policies on: Temporary duty (TDY) travel allowances, Relocation allowances, Payment of expenses connected with the death of certain employees, and Payment of expenses from a non-federal source.

Federal Information Security Management Act of 2002: This act provides a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets. It also provides effective Government wide management and oversight of the related information security risks, including coordination of information security efforts throughout the civilian, national security, and law enforcement communities. The act also sets minimum controls required to protect Federal Information and information systems. It may be found at: NIST Page on FISMA

Foreign Affairs Manual (FAM): The Foreign Affairs Manual (FAM) and associated Foreign Affairs Handbooks (FAHs) are a single, comprehensive, and authoritative source for the State Department's organizational structures, policies, and procedures that govern the operations of the State Department, the Foreign Service and, when applicable, other federal agencies. Please visit https://fam.state.gov/ for more information.

It is Department of State policy, as authorized by section 901 of the Foreign Service Act (22 U.S.C. 4081) that the Secretary authorize and pay for the official travel and related expenses of members of the Foreign Service and their families, including costs or expenses incurred for:

1. Proceeding to and returning from assigned posts of duty;
2. Authorized or required home leave;
3. Family members to accompany, precede, or follow a member of the Service to a place of temporary duty;
4. Representational travel;
5. Medical travel (other than for routine follow-up care);

6. Rest and recuperation travel;
7. Evacuation travel;
8. Visitation travel;
9. Return remains of member of the Service or of a family member of the Service who dies abroad or while assigned within the United States; and
10. Other travel, as authorized and necessary, to accomplish the Department's mission.

Fulfillment or Fulfillment Services: The manual and automated assisted steps a TMC must take between the time a reservation is made either via an online booking tool (OBT) or with a travel agent, and the transaction is completed, including but not limited to performing policy management, providing quality assurance, completing all PNR documentary requirements, including Form of Payment (FOP) and accounting classification/Line of Accounting (LOA) information, issuing and delivering an electronic ticket with a correct and complete travel itinerary, and performing ARC reporting. These processes support travel reservations made through ETS & DTS. In addition, see the T&E Business Standards TRT.010.040 *Travel Ticketing* Activities and Capabilities for services related to the ETSNext Technology MSP.

Global Distribution System (GDS): The GDS is a technology platform for multi-sourced travel content aggregation and distribution. The GDS enables the TMC to perform searches, view, comparison shopping, book and service airline, hotel accommodations, ground transportation and ancillary services. The platforms may offer a range of additional services including, but not limited to quality control, back-office integration, reservation management, and policy management. GDSs are used by TMCs, OBTs, ETS, & DTS to enable travel reservations, ticketing, fulfillment.

Government Transportation Request (GTR): Optional Form 1169, the Government document used to buy transportation services. GTRs are issued and used only for officially authorized passenger transportation for the account of the United States. GTRs may be used to pay for international air travel. For domestic air travel, GTRs may be used under special circumstances and for travel related expenses. Special domestic circumstances are defined as acts of God, emergency situations, and when buying a domestic ticket in the USA in conjunction with travel that originated overseas.

GSA SmartPay® Program: The Travel and Transportation Reform Act of 1998 (Public Law 105-264) mandates federal government cardholders to use the SmartPay® contractor bank issued travel card (including Individually Billed Accounts (IBA), Centrally Billed Accounts (CBAs), Virtual Cards, etc.) for official government travel expenses following FTR Section 301- 70.704. The GSA SmartPay® travel charge card (Visa or MasterCard branded) shall be used only for authorized official travel.

GSA SmartPay Tax Advantage Travel Card Account: The GSA SmartPay Tax Advantage Travel Card Account is a product offering, under the SmartPay 3 award, which combines an IBA and CBA, providing a means to obtain tax exemption automatically at the point of sale for rental cars and lodging charges in the United States.

GSA Travel Reporting Tool: GSA collects and reports on agency travel data for Premium Class Travel, Senior Federal Travel and Government-wide Travel Reporting Information.

Individually Billed Account (IBA): A Government SmartPay® contractor-issued charge card issued to authorized employees to pay for official travel expenses for which the SmartPay® charge card contractor bills the employee.

Industrial Funding Fee (IFF): The IFF reimburses the General Services Administration for the costs incurred in procuring and managing the FSS and MAS and the CPP. See Price Proposal Template for more information.

International Air Transportation Association (IATA) Number: Number used to identify the travel agent.

Invitational Travel: Authorized travel of individuals either not employed or employed intermittently (under 5 U.S.C. 5703) in the Government service as consultants or experts and paid on a daily when actually employed basis and for individuals serving without pay or at $1 a year when they are acting in a capacity that is directly related to, or in connection with, official activities of the Government. Travel allowances authorized for such persons are the same as those normally authorized for employees in connection with TDY.

Itinerary: An Itinerary is defined as all arrangements and all air, rail, lodging, or rental car reservations (ticketed segments) for a single (one) trip/authorization. This includes making and changing reservations for air, rail, lodging, or rental cars for one or multiple locations and tickets issued per traveler.

In the **Price Proposal Template**, the Unit of Issue "**Per Itinerary**" for **Ancillary Services** requested (e.g., VIP Services, International Rate Desk, etc.), may be charged at the time the service is provided and is not refundable if the travel is subsequently canceled after ticketing.

An added "**Per Itinerary**" fee may be incurred if changes in the trip/authorization require the issuance of a new ticket(s) related to the itinerary.

Joint Travel Regulation (JTR) The Joint Travel Regulations (JTR) implements policy and law to establish travel and transportation allowances for Uniformed Service members (i.e., Army, Navy, Air Force, Marine Corps, Space Force, **Coast Guard, National Oceanic and Atmospheric Administration Commissioned Corps, and Public Health Service Commissioned Corps**), Department of Defense (DoD) civilian employees, and others traveling at the DoD's expense. Please visit https://www.travel.dod.mil/Policy-Regulations/Joint-Travel-Regulations/ for more information.

Known Traveler Number (KTN): A nine-digit number that serves as the known traveler number for an individual enrolled in the Transportation Security Administration (TSA) Pre-check program.

Long Term Lodging (30 or more lodging nights) - Lodging accommodations for durations of 30 or more nights.

Leave in Conjunction with Official travel (LICWO)/Leisure Travel: Any transaction for which the services of the TMC are used to book leisure travel requested by a traveler concurrent with and/or in addition to authorized official travel.

This service may be offered if personal Leave in Conjunction with Official travel/Leisure travel services do not impede the official travel service levels under the contract.

Lowest Logical Fare: The lowest applicable fares compliant with FTR and/or FAM, contract City Pair Program (CPP) airfare usage, agency policy, and reporting requirements.

Management Service Fee (MSF): MSF method consists of charging a fixed fee per month for full performance of all contract requirements. See Price Proposal Template for more information.

New Distribution Capability (NDC): Is a travel industry-supported program (NDC Program) launched by IATA for the development and market adoption of a new, XML-based data transmission standard (NDC Standard). The NDC Standard enhances the capability of communications between airlines and travel agents and is open to any third party, intermediary, IT provider or non-IATA member, to implement and use.

NDC enables the travel industry to transform the way air products are retailed to corporations, leisure, and business travelers, by addressing the industry's current distribution limitations: product differentiation and time-to-market, access to full and rich air content and finally, transparent shopping experience. For more information visit iata.org.

Non-Emergency After-Hours Service: Calls requesting travel services not meeting the definition of emergency travel services that occur outside core service hours. Examples of non-emergency travel service requests include but are not limited to a) requests for flight schedule information, b) transaction fee questions, c) requests for invoice copy, d) requests to update traveler profiles, e) requests to add loyalty program information to reservation, and f) requests to change seat assignments.

Nonforeign Outside the Continental United States (OCONUS) (NF OCONUS): U.S. Territories that are located outside the 48 Contiguous States – Alaska, Hawaii, Guam & the Northen Mariana Islands, Puerto Rico, and the U.S. Virgin Islands

Occupancy Rate: The percentage of time that agents are occupied, performing call center activities (talking to customers and/or performing after call tasks).

OCONUS: Outside of the forty-eight (48) contiguous United States and the District of Columbia.

Official Travel: Authorized travel and assignment solely in connection with business of the Government. Types of official travel may include Temporary Duty (TDY), Permanent Change of Station (PCS), Permanent Duty Travel (PDT), Recruitment travel, travel by Reserve Component/National Guard members, Leave in Conjunction with Official Travel (LICWO) / Leisure, and Evacuation Travel.

Official travel also includes civilians in connection with official United States Government business, and travel performed under orders at the expense of federal appropriated and non-appropriated funds.

Online Booking Tool (OBT): A web-based solution for making reservations for Air, Rail, Lodging, Rental Car, etc., without the support of a travel agent.

Open or Limited Open Travel Authorization: Written approval to travel on official business for a given period, usually no longer than 1-year. May also be referred to as a "Blanket "or "Open Blanket" authorization.

Passenger Information: Passenger information may include, but is not limited to, Passenger Name Record (PNR) locators, names, gender, passport, dates of service, ticket numbers, carrier/rental car company/hotel name & code, class of service; base fare/tax/total ticket amounts, departure and arrival airport codes by segment, origin and destination markers, explanatory codes, lowest available fares, ticket designator, user-defined ID fields (UDIDs), and car rental rate types.

Contractors must remove all Personally Identifiable Information (PII) from all GSA reports (NOTE: PII must be deleted from GSA reports and from the data transferred to GSA or GSA-designated third parties unless otherwise agreed to in writing by GSA. (See 26 REPORTS for distinction between GSA reports and GSA data transfer).

Passenger Name Record (PNR): A file in a Global Distribution System (GDS) that holds pertinent information relating to a specific reservation / itinerary.

Per Diem Allowance: A daily payment for lodging, meals, and incidental expenses (M&IE) used instead of reimbursement for actual expenses incurred. For more information, please visit https://www.gsa.gov/travel/plan-book/per-diem-rates.

Permanent Change of Station (PCS) / Relocation: The permanent assignment, detail, or transfer of a Service member, civilian employee, or unit to a different Official Station or Permanent Duty Station

(PDS). A PCS / Relocation travel authorization / Order does not direct further assignment to a second new Official Station / PDS or return to the old Official Station / PDS. A PCS / Relocation travel authorization order does not specify the duty as temporary but may authorize Temporary Duty Travel (TDY) travel for House Hunting trips or enroute travel to the new Official Station / PDS.

Personally Identifiable Information (PII): Any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means. For more information, see NIST SP-800-122 *Guide to Protecting the Confidentiality of Personally Identifiable Information*.

Point of Sale (POS): The time and place at which a retail transaction (transaction fee) is charged.

Redress Control Number: A record identifier for people who apply for redress through the Department of Homeland Security (DHS) Travel Redress Inquiry Program (DHS TRIP). DHS TRIP is for travelers who have been repeatedly identified for additional screening and who want to file an inquiry to have erroneous information corrected in DHS systems.

Rental Car Program: The U.S. Government Rental Car Program, from the Defense Management Travel Office (DTMO), offers reduced rates and special benefits when renting cars, passenger vans, or small pick-up trucks through a variety of approved rental car companies. The program is open to federal government employees and service members traveling on official business and is administered through the U.S. Rental Car Agreement #5 For additional information, please visit, https://www.travel.dod.mil/Programs/Rental-Car/.

Reshopping: After the initial booking is made by the traveler, information from the reservation is fed (usually by a TMC queue or API) to a vendor designated by the government to run automated checks and notifications on a regular interval to determine if a lower policy-compliant airfare is available (parameters likely set to only search flights on the same flight or on the same day and at the same time) or if a lower policy-compliant hotel rate is available (parameters likely set to only search same hotel).

Secure Flight: The Intelligence Reform and Terrorism Prevention Act of 2004 requires that the DHS Transportation Security Administration (TSA) conduct preflight comparisons of passengers to Government watch lists. DHS requires travelers to supply gender and date of birth; this information may also include a government passport, known traveler number (KTN), redress number, if applicable, for air and/ or rail reservations.

Service Contract Labor Standards (SCLS): Requires contractors and subcontractors performing services on prime contracts more than $2,500 to pay service employees in various classes no less than the wage rates and fringe benefits found prevailing in the locality, or the rates (including prospective increases) contained in a predecessor contractor's collective bargaining agreement. The Department of Labor issues wage determinations on a contract-by-contract basis in response to specific requests from contracting agencies. These determinations are incorporated into the contract.

For contracts equal to or less than $2,500, contractors must pay the federal minimum wage as provided in Section 6(a)(1) of the Fair Labor Standards Act.

For prime contracts more than $100,000, contractors and subcontractors must also, under the provisions of the Contract Work Hours and Safety Standards Act, as amended, pay laborers and mechanics, including guards and watchmen, at least one and one-half times their regular rate of pay for all hours worked over 40 in a workweek. The overtime provisions of the Fair Labor Standards Act may also apply to SCLS-covered contracts. Additional information can be found at https://www.dol.gov/agencies/whd/government-contracts/service-contracts.

Service Level: A performance metric that measures the quality and efficiency of a call center's customer service. It refers to the percentage of calls answered within a specified time frame, usually expressed as "X% of calls answered within Y seconds."

Service Level Agreement (SLA): A service-level agreement (SLA) is a contract between a service provider and its customers that documents what services the provider will offer and defines the service standards the provider is obligated to meet. A service-level commitment (SLC) is a broader and more generalized form of an SLA.

Special Publication 800-87 (SP 800-87): Provides agency organizational codes used under this schedule for reporting purposes. This standard data element may be used for the interchange of information on federal operations when that information is identified by organization. This publication is available at https://csrc.nist.gov/pubs/sp/800/87/r2/final.

Strategic Meetings Management (SMM): Is a disciplined approach to managing enterprise-wide meeting and event activities, processes, suppliers, and data to achieve measurable business objectives that align with the organization's strategic goals and vision, and deliver value in the form of quantitative savings, risk mitigation, and service quality.

Temporary Duty Travel (TDY): Travel at a place, away from an employee's official duty station, where the employee is authorized to travel.

Transaction: A "*Transaction*" is defined as providing a particular service, in support of a single (one) trip/authorization, e.g., "*Non GDS Air/Rail Surcharge*," "*Leisure Travel*," "*Cost-Constructed Travel*," etc.

In the **Price Proposal Template**, the Unit of Issue "**Per Transaction**" for **Ancillary Services** requested (e.g., "*Non GDS Air/Rail Surcharge*," "*Leisure Travel*," "*Cost-Constructed Travel*," etc.), may be charged at the time the service is provided and is not refundable if the travel is subsequently canceled before or after ticketing.

An added "**Per Transaction**" fee may be incurred if changes in the trip/authorization require additional service(s) related to the itinerary.

Transaction Fee: The fee charged for travel and transportation arrangements for one Itinerary and the associated travel authorization.

> **Transaction A - Air and/or Rail Ticket with or without Lodging and/or Car Rental Reservations:** Transaction A fee applies for all arrangements and reservations related to a single (one) itinerary for which an air or rail ticket is issued (paper or electronic). The fee includes making and changing reservations (air/rail, lodging, and/or car rental) for one or multiple locations. The fee may only be charged at the time of ticket issuance and is not refundable if the travel is subsequently canceled after ticketing. The transaction fee covers tracking of unused tickets and the processing of refunds or credits for unused tickets.
>
> An *added transaction fee* may be incurred if changes in the itinerary require the issuance of a new ticket related to the itinerary. The contractor shall not charge a fee for cancellations made prior to issuance of tickets. Research of travel arrangements, changes to existing arrangements, and air/rail reservations for which air/rail tickets are not generated shall not be considered as a **Transaction A** transaction.
>
> **Transaction B - Lodging and/or Car Rental Reservations Only:** Transaction B fee applies for all arrangements and reservations related to a single (one) itinerary for which an air or rail ticket is NOT issued. The fee includes making and changing lodging and/or car rental arrangements for one or multiple locations when air or rail transportation is not included in the itinerary. Research

of travel arrangements, changes to existing arrangements, and reservations that are canceled prior to the check-in date shall not be considered as a Transaction B transaction. Transaction B fees shall be charged at the point the authorization is approved by the customer agency travel authorizing/approving official or their designee.

NOTE:

1. For a Group Travel Request (Air), a transaction fee can be charged for each traveler in the group.

Following industry standards, if air/rail changes after ticketing require ticket reissuance, an additional transaction fee may be charged, which shall be considered a full service / offline transaction.

Transient Lodging (1-29 lodging nights): Lodging accommodations for durations of twenty-nine (29) or less lodging nights. This may include rooms occupied by those with reservations at FedRooms®, rack, corporate negotiated, package, government, or foreign traveler rates. Also includes rooms booked via third party websites (exception: simultaneous bookings of ten (10) or more rooms which should be defined as a group). Lodging accommodations to include short term and extended stays (typically more than five (5) consecutive nights) for durations of less than 30 lodging nights.

Travel Authorization (TA): Electronic or written approval to travel on official business.

Travel Authorization and Voucher System (TAVS): A term for the end-to-end T&E management solution offered by **ETS2**.

Travel & Expense (T&E) Management Business Standards: Business standards, established and agreed to by agencies, using the Federal Integrated Business Framework (FIBF) enable the government to better coordinate on the decision-making needed to determine what can be adopted and commonly shared. They are an essential first step towards agreement on outcomes, data, and cross-functional end to end processes that will drive economies of scale and leverage the government's buying power. The T&E Business Standards are the basis for the requirements for the ETSNext Technology MSP.

The T&E Business Standards can be found at https://ussm.gsa.gov/fibf-travel/. TMCs, at a minimum, will need to support TRT.010.020 *Travel Reservation Assistance and Processing* and TRT.010.040 *Travel Ticketing*. They will also need to support TRT.010.010 Travel Personnel Profile Set-Up and Maintenance, to ensure that profiles are kept in-sync between the ETSNext Technology MSP T&E Shared Service, including the OBT, and the GDS. See ETSNext Technology MSP and the Travel & Expense Business Standards of this SOW for more information.

Travel Management Company (TMC): A company under contract with an agency to arrange travel services for federal employees on official travel, including tickets and transportation, and reservation of accommodations.

Trip-by-Trip: Written approval to travel on official business on a trip-by-trip basis.

VIP Travel Services: Specialized travel agency services, provided by a TMC, that do not include usual, customary, and ordinary TMC requirements and are performed by specifically designated travel counselors that provide enhanced travel reservation services to designated customer agency personnel. VIP travel services include specific duties and performance standards about responsiveness and unique areas of travel industry knowledge. These services may be offered under SIN Ancillary, *Ancillary Supplies and Services*.

Verbal Authorization / Orders: A verbal authorization, given in advance of travel, and subsequently confirmed in writing, email, etc., giving date of the verbal authorization, and approved by competent authority that will meet the requirement for written authorizations.

Virtual Charge Card: Temporary account numbers that may be used during a limited time, for a limited amount, for a specific vendor or merchant category code (MCC) etc. This may include single-use accounts, "ghost" cards, and smartphone apps to support payment transactions.

YCA Fare: The code used to identify unrestricted coach class contract fares for Government contract carriers. “CA” means “contract award.”

_CA Fare: A three-letter code used to identify capacity-controlled coach class contract fares for Government contract carriers. Such codes shall include the letters “_CA” as the last two characters.

_CB Fare: A three-letter code used to identify capacity-controlled Government contract business class fares.

_CP Fare: A three-letter code used to identify international premium economy class fares.

Non-Government Contract Fares: *Other Government Airfare* (also known as "DG" or "CATZ"). **These are non-contract Government fares** that include discounted Government fares (DG) or Category Z (CATZ) and constructed City Pair fares.

- DISCOUNTED GOVERNMENT FARES (DG Fares): The fare is fully refundable and has similar benefits of the YCA fare. However, discounted government (DG) fares, sometimes referred to as "Me Too" fares, are offered by other **non-contract airlines** to match GSA contract fares. They are NOT part of the CPP.
- CATEGORY Z FARES (CATZ) The Category Z fares are competitive airfares available to Government travelers on official travel. The cost may be the same or less than a GSA contract City Pair fare; however, many airlines are not required to maintain the booking class and can change that class of service; in turn, creating an invalid fare and booking class. Although rare, it is crucial to check the rules before using this government fare. These fares may not be used as a reason to fly non-contract fares based on a lower price.

9 DESCRIPTION OF WORK

The Contractor shall supply professional travel agents and related services to aid the Government and the ETS and DTS contractors in meeting its travel needs for various types of domestic and international travel (e.g., invitational, TDY, open, trip-by-trip). This may include, but is not limited to, the following:

Account Management Services

Airline Reservation Services

ARC & BSP Ticketing Reports

Booking Assistance

Business Services

Car & Truck Rental Services

Centrally Billed Account Reconciliation Services

Credit and Refund Services

Destination Services

DTS & ETS (ETS2 & ETSNext) Interface / Integration Services

Enroute Travel Services

Emergency/Evacuation Related Travel Services

Frequent Traveler / Loyalty Programs

Ground Transportation Services

International Travel Services

Invoicing

Itineraries

Lodging Reservation Services

Medical Travel

Messaging - Travelers

Onsite Travel Agent Support

Outsourced Passport & Visa Services

Preferred Supplier Programs

Profiles

Quality Assurance / Control

Rail Reservation Services

Receipts

Reports / Dashboards

Relocation / Permanent Change of Station (PCS)

Reservations

Routing Support Services

Service Level Agreements

Ticketing and Fulfillment

Travel Technology

Unused Ticket Tracking & Reporting

VIP Travel

Typical tasks may include, but are not limited to:

1. Arrange travel reservations, ticket & fulfill official travel for individuals and groups.
2. Ensure travel services are booked with government contract & agreement holders.
3. Provide travel policy support in support of government contract & agreement holders.
4. Provide reconciliation support for Centrally Billed Accounts.
5. Provide Account Management services, including T&E management reports that include but are not limited to air/rail, car, and hotel data.
6. Provide onsite travel agent services (as defined at the agency TO level).
7. Meet the SLAs as defined as part of this SOW and at the agency TO level.

10 SCOPE

1. Offer a full range of services necessary to satisfy ordering agencies' travel management requirements. The Government is seeking services that the travel industry normally gives to its commercial customers.
2. Be capable of handling multiple agency task orders simultaneously.
3. Be capable of supporting the T&E management solutions available under the ETS program if a TMC is interested in supporting the agencies required to use ETS per FTR 301-50.3.

11 GENERAL REQUIREMENTS

11.1 Provide travel agent services as negotiated and ordered by agencies and as specified here. The (PRIVACY ACT) and **Service Contract Labor Standards (SCLS)** apply to travel agent services.

11.2 Ensure that DHS TSA Secure Flight Passenger data is captured following standard commercial practices when making reservations on behalf of a traveler. Verify the information is provided, via the OBT (if applicable) when performing Quality Control checks.

11.3 Ensure that its company and staff keep any generally required professional certification, accreditation, license, bond, and proficiency relative to their area of expertise. This includes, but is not limited to, adherence to a code of conduct through the Association of Retail Travel Agents or the American Society of Travel Agents, accreditation by supplier organizations such as Airline Reporting Corporation, compliance with State and local licensing requirements, if any, etc. The Contractor shall keep documentation of such records. The Government will not pay for expenses to meet this requirement.

11.4 Provide dedicated Government support like what is available to commercial clients. Travel agents provided under this SIN SOW should only work on Government accounts.

11.5 Provide a local, toll-free, collect, and teletypewriter (TTY) telephone number for both CONUS and OCONUS customers, as appropriate and available.

11.6 Service content, via the GDS, and have a method to make reservations when the GDS system is not operating or when reservations must be made when an airline or other service provider does not subscribe to a GDS.

11.7 Service content and support reservations utilizing New Distribution Capability (NDC), direct connect, content aggregators, and other content suppliers from transportation carriers and other service providers. Support for NDC, direct

connect, content aggregators, and other content suppliers may be defined in this schedule, the awarded ETSNext Technology MSP contract, in the agency TO, and in the agreement between the TMC, the agency, and the ETSNext Technology Managed Service Provider (MSP).

11.8 Ensure that travelers have access to and are aware of all Government contract fares and Government preferred suppliers, subject to the restrictions noted below in, CITY PAIR PROGRAM (CPP) REQUIREMENTS. Fulfill travel requirements with all Government contracts, agreements, and preferred suppliers as applicable.

11.9 Ensure delivery of services provided follows the Government's travel regulations including the FTR and JTR. This may include, but not be limited to, reservation, booking and fulfillment of contracted fares and rates of travel services with mandatory programs (e.g., Airline City Pair Program), preferred suppliers (e.g., FedRooms® BIC lodging contract solution), DTMO's car rental agreement #5 (and subsequent revisions thereto), and agency-specific policies; and processing credits and refunds for unused, partially used or exchanged tickets. The FTR, JTR, FAM, and other applicable travel regulations, and related agency policies regulate the federal travel process. Ticketing time frames for the CPP will be provided at the agency TO level. Non-contract fares must be issued in accordance with the fare rules.

11.10 Provide a Quality Assurance (QA) / Quality Control Program (QCP), including automated and automation-assisted quality control processes, to ensure reservations, are to the maximum extent possible, booked correctly and documented at the point of sale, without re-contacting the traveler or the need for manual post-call (or post-booking) processing by agents. QCP shall ensure all PNRs are evaluated for accuracy, completeness, policy compliance, etc. To the maximum extent possible, use automated file finishing to minimize or eliminate the need for manual intervention in reservation fulfillment. QCP shall include tracking of unused tickets. This may include adding a Ticket Designator (TD) or other airline-required field e.g. CLID, to assist carriers in identifying all Government transactions in the future.

11.11 If non-contract reservations made by the Contractor are not at the lowest available rate allowed, at the time of ticketing, the Contractor shall refund the difference to the Government.

11.12 Provide prompt reconciliation of centrally billed accounts (CBAs). The Contractor shall reconcile centrally billed accounts within five (5) business days of the receipt of travel card information from the GSA SmartPay® contractor, or within a timeframe mutually agreed upon at the agency TO level. The Contractor

shall deliver to each customer agency a monthly commercial standard Charge Card Reconciliation Report to include sufficient transactional detail as necessary to properly associate charges with tracked expenses authorized by the Government. CBA reconciliation may include, but is not limited to, the matching of charges to travel authorizations, a list of unmatched charges including and the reason they were unable to be matched, e.g., missing travel authorization number, missing CBA number, etc. The format of the report may be negotiated at the agency task order level.

11.13 Service Level Agreements (SLAs) may be proposed at the task order level to the extent the terms of such agreements do not conflict with the terms and conditions of this Schedule (see Order of Precedence of Clause 52.212-4) and can be used in conjunction with Performance Incentives. SLAs may be negotiated with ordering agencies. See SERVICE LEVEL AGREEMENTS (SLA) below for the SLAs required as part of this schedule.

11.14 Provide Government agencies with standard commercial, contract management reports following Section 26 REPORTS and as requested in customer agency task orders. This includes, but is not limited to, pre- and post-trip reporting, travel booking analysis (e.g., air, hotel, car, other), policy compliance reporting, exception reporting, fare basis, top travel destinations/markets/vendors, cba reconciliation reports, unused tickets, class of service (e.g., first class) required by the FTR, JTR, & FAM as applicable.

11.15 Reports should be available by an industry standard reporting solution. The reporting solution should be able to support the “standard” reports referenced below in Section 26 REPORTS and allow for ad hoc report development by agencies for self-service reporting. The reporting solution should support the development and use of dashboards for executive reporting. Reporting should support reporting based upon the agency hierarchy including at a summary level.

11.16 Transfer data, as outlined in Section 26 REPORTS, to GSA monthly. All transfer of data is at no cost to the Government. All data generated under this schedule and associated TOs and stored in contractor’s systems (such as back-office systems), as well as data transferred to GSA is owned by the Government. The Contractor must provide GSA with data, as specified in the MAS, without requiring or seeking authorization at the TO level. TOs do not supersede GSA’s rights to data under this contract.

11.17 Provide ordering agencies and/or GSA with ad hoc reports within 15 days of request or at regular intervals as defined at the agency TO level. If an ad hoc report will take more than 15 days, the contractor must provide the estimated

delivery date within five (5) business days. All reports are owned by the Government.

11.18 **Unused Tickets**: The Contractor shall redeem unused or partially used tickets (both e-tickets and paper tickets) issued by the Contractor on behalf of the ordering agency. This includes, but is not limited to:

11.18.1 Identifying unused tickets.

11.18.2 Provide nonrefundable unused ticket information to the ETS (ETS2, ETSNext), or DTS contractor for application during the online booking process (notification via the OBT, if available, will be managed in coordination with the ETSNext Technology MSP.)

11.18.3 Notifying travelers of all unused tickets available for reuse during the booking process.

11.18.4 Notifying travelers of expiring tickets 90 days prior to expiration (notification via the OBT, if available, will be managed in coordination with the ETSNext Technology MSP.)

11.18.5 Support and aid with name changes for unused tickets, as allowed by the carrier.

11.18.6 Completing necessary forms for a refund and sending the claim to the carrier within 15 days of the last segment date or five (5) business days following notification by the agency to cancel and refund the ticket.

11.18.7 Receipt of, accounting, and reconciliation of the refund.

11.18.8 Reporting of such activity.

11.19 **Reshopping**: The Contractor shall, if asked by GSA and the ETSNext Technology MSP, support, and queue reservation data to a GSA and the ETSNext Technology MSP approved Reshopping vendor at no added cost to the government.

11.19.1 The Contractor shall support the rebooking and reticketing of reservations based upon the Reshopping vendor's recommendations and the policy rules set forth by the Government.

11.19.2 If the Reshopping services recommends that a reservation, air, or hotel, be rebooked and reticketed the Contractor shall charge the appropriate Transaction A or Transaction B fee.

11.19.3 If Reshopping is not offered by GSA and the ETSNext Technology MSP, the TMC may offer Reshopping as a service on the schedule.

11.20 **Leave in Conjunction with Official Travel (LICWO) / Leisure Travel**: The Contractor may offer services to plan and book LICWO / leisure (personal) travel conducted in conjunction with official travel provided:

11.20.1 Leisure travel services are provided **at no cost to the Government**, including any costs for development, maintenance, operation, customer support, etc. The Contractor shall not advertise, solicit, or sell any leisure travel services.

11.20.2 The Contractor shall provide a separate Contract Item Number (CLIN) for LICWO / leisure services and may not charge the government specific CLINs for providing support for leisure travel.

11.20.3 **Travelers are responsible for any costs that exceed the official portion of the trip.** The contractor shall not charge the Government for any leisure only reservations or services.

11.20.4 Travelers cannot book City-Pair or other Government-negotiated fares (which are not authorized for personal use) for leisure travel.

11.20.5 A method for direct payment by the traveler must be provided for personal travel. Travelers may book FedRooms® lodging rates for leisure travel only if the hotel decides to offer their FedRooms rates to federal employees, on leisure travel, as part of the annual FedRooms Request for Proposal (RFP) for hotel sourcing.

11.20.6 Collection of amounts due and any refunds for these personal travel legs are to be arranged directly between the Contractor and the traveler and collected prior to releasing the ticket. The Contractor will clearly document the cost and routings of personal portions of combined trips on all itinerary/invoices and provide reports on such trips as requested by the Government. The Contractor will ensure that arranging personal travel does not interfere with arranging Official Travel.

11.20.7 Any exchanges or refunds that result in a credit for the official part of travel, because of ticket changes, must be returned to the Government.

11.20.8 This service may be offered if personal Leisure Travel services do not impede the official travel service levels under the contract.

11.21 **Cost-Constructed Travel**: If requested at the ordering agency TO level, the Contractor may offer Cost-Constructed Travel as a service.

11.21.1 The fee is charged for all cost-constructed itineraries that are completed within three quotes. It is charged per itinerary (not per person) so, for example, a family of five with the same itinerary would be charged one fee.

11.21.2 It is payable at the time a cost constructed itinerary is ticketed. If a cost construct itinerary is changed and requires a new ticket, a new cost construct fee per itinerary is charged.

11.21.3 If there is an itinerary which requires more than three quotes, an added fee will be charged for EACH additional quote after the initial three.

11.21.4 The TMC must document in the PNR to show that the traveler has agreed to the cost-constructed itinerary, fare, and has provided a means of payment for the added fees. The TMC will provide a copy of the authorized itinerary, fare calculation, as well as the cost-constructed itinerary and fare.

11.21.5 This service may be offered if personal Cost Construct services do not impede the official travel service levels under the contract.

11.22 **Account Management Support**: The Contractor shall:

11.22.1 Be proactive in implementing and streamlining travel management operations and initiatives and be proactive in communication with the Agency.

11.22.2 Be a strategic partner and provide forward thinking recommendations on improvement opportunities by including new technologies, operational models, and a go-forward optimization strategy across the full travel management program.

11.22.3 Provide Global, Regional and Local account management (as applicable) with a high level of service to all travelers and arrangers, as well as the Travel Manager(s), while keeping the agency current with industry enhancements/developments.

11.22.4 Identify strategic opportunities to enhance and grow the program while maintaining or lowering costs.

11.22.5 Provide quarterly and annual business reviews, and technology reviews at least twice a year.

11.22.6 Ad hoc reviews of any deficiency in services must be addressed at once and a corrective action plan submitted within five (5) business days. Once reviewed and approved by the Government, the Contractor shall implement the corrective action plan within two (2) business days or other timeline agreed upon by both parties."

11.22.7 The Contractor shall ensure that any change brought about by technological advances is effectuated in a smooth, seamless manner, with minimal disruption to the travel program. The Contractor shall coordinate any technological transition with the ordering agency Contracting Officer (CO) and the Contracting Officer's Representative (COR) at least 90 calendar days prior to transition.

11.22.8 Given the rapid pace of technology advancement, new services and capabilities are expected to appear during performance under this SIN SOW. As commercial T&E services evolve, the Government requires that the Contractor consider these new services and capabilities for continuous improvement.

12 COMMERCIAL SECURITY STANDARDS:

12.1 **Minimum Commercial Standards**: To be on the Travel Agent Services Schedule, 561510, all Contractors shall meet the minimum commercial standards as described below. In addition, TMCs will need to comply with the federal security standards, as required by the ordering agency, at the TO level. For security requirements in support of ETSNext, please see Section 18.4 FEDERAL SECURITY STANDARDS FOR the ETSNext Technology MSP.

12.1.1 The Contractor shall apply commercially accepted security risk management standards, processes, and frameworks that achieve the intent and goals of Government Assessment and Authorization (A&A) requirements. This would be

carried out using a commercially accepted or a combination of commercially accepted frameworks that can be mapped back to and achieve the same desired security outcomes found under FISMA, NIST, OMB, and GSA Policy, as appropriate.

12.1.2 The Contractor shall set up, implement, maintain, and comply with information security policies, processes and procedures that meet or exceed the standards and controls set forth in the current and future versions of **ISO/IEC 27001:2013 and ISO/IEC 27002:2013**.

12.1.2.1 If the Contractor already meets the NIST SP 800-171, SP 800-53, or FedRamp, and has an Authority to Operate (ATO), Authority to Use (ATU), or a Memorandum for the Record (MFR) (or similar document) there is no need for the Contractor to provide proof of meeting the ISO/IEC standards or a Third-Party Assessment showing that they meet the ISO 27001 controls.

12.1.2.2 In lieu of the ISO standards, the Government agrees to accept certification of Contractor's compliance with the standards and controls set forth within SSAE 18 (SOC 2 Type II) as a viable mitigating control when approved by the Government's appropriate security Authorizing Official.

12.1.3 The Contractor shall support the current and future versions of the **Payment Card Industry (PCI) Digital Security Standards (DSS) version 4.0** published in March of 2022, which is hereby incorporated by reference and may be updated over the course of performance. For additional information, please visit https://www.pcisecuritystandards.org/ or https://www.pcisecuritystandards.org/document_library/?category=pcidss.

12.1.4 Upon Government's written request, the Contractor shall provide certification of its compliance with such standards by an independent third-party reasonably acceptable to the Government only to the extent that such certification is available to the Contractor.

12.1.5 Establish proper administrative, technical, and physical safeguards to protect all non-public Government data to ensure the confidentiality, integrity, and availability of Government data. All Contractor personnel with access to or responsibility for non-public Government data under this contract shall follow all security directives and instructions.

12.2 Access Controls

12.2.1 Contractor will develop, monitor, maintain and implement logical and appropriate security controls, at its expense, for regulating access to its network, operating systems, applications, databases, network devices and other devices or systems on which Government data is stored or processed, including: assigning users and devices the minimum access rights required to perform required functions; updating access rights based on personnel or system changes; reviewing users' access rights at an appropriate frequency (at least annually, or more frequently if a user's role/access needs change) based on the risk to the application or system; designing appropriate acceptable-use policies and requiring users to agree to them; controlling privileged access; and modifying or disabling access (e.g., user accounts

and passwords) to systems, services and applications/software immediately upon an applicable individual's transfer, role change or termination date.

12.2.2 Contractor will maintain a password management program/policy in accordance with NIST SP 800-63B and/or agency specific requirements for customer user accounts and Contractor employee/sub-contractor user accounts.

12.2.3 If any Government Data resides on Contractor's systems or Contractor has access to Government's network or systems, Contractor shall implement multifactor authentication access controls for all remote access (including for privileged access) to prohibit unauthorized access to Contractor's systems and Government's Data.

12.2.4 On an annual basis, at a minimum, Contractor will perform an access certification for its users and their access to its information systems, services, and applications/software. Contractor will enforce segregation of duties within its operations related to any of Contractor's information systems and/or use of/access to Government Data so that no one individual can modify, initiate, or create changes to Contractor's information systems or Government Data without appropriate oversight, authorization, or detection. Where such segregation of duties is not practicable, demonstrable compensating controls must be implemented by Contractor.

12.3 Penetration and Vulnerability Testing:

12.3.1 Contractor's security program shall have an application and network penetration and vulnerability assessment process that includes and addresses, at a minimum, the following components:

12.3.2 Threat modeling (i.e., known vulnerabilities in hardware or software, in the system or application, and in required network services).

12.3.3 Penetration testing conducted at least annually.

12.3.4 Vulnerability scanning at least weekly.

12.3.5 Application custom code security testing prior to each release.

12.3.6 Assessment of the potential exploits and impacts.

12.3.7 Safeguard analysis such as code revisions, patches, fixes, configuration changes and compensation or other controls.

12.3.8 Remediation of found vulnerabilities according to their assigned threat rating.

12.3.9 Contractor shall perform a penetration and vulnerability assessment prior to production use (e.g., the "go live" date), following this paragraph, with respect to all new or significantly changed applications that are either Internet-facing applications or internal applications that handle Government Data.

12.3.10 Contractor shall provide GSA and the ordering agency with reports, on a quarterly basis, unless otherwise mutually agreed upon with the GSA CO summarizing any material failures or issues (including Critical and High-risk findings) that have been found by the penetration and vulnerability assessments along with the status for implementing any corrective action plans intended to remediate any identified failures or issues.

12.3.11 Upon reasonable request by GSA and the ordering agency, the Contractor shall also provide the evidence (or attestation) of remediation of any applicable failure or issue.

12.3.12 Contractor shall implement proper practices, procedures and vulnerability scanning tools to assess and monitor Contractor's systems, networks, hosts, applications, databases, containers, and associated devices used to deliver the Services. Such scans shall be conducted on at least a weekly basis, and such practices and procedures will include the remediation of identified vulnerabilities.

13 PROTECTION OF INDIVIDUAL PRIVACY (PRIVACY ACT)

13.1 Work from a task order under this MAS SIN SOW may result in the design, development, or operation of a system of records on individuals. Therefore, in accordance with the Privacy Act of 1974 (5 U.S.C. § 552a) and FAR 24.103, the system of records on individuals that is applicable at the agency TO level. The Contractor and its employees are subject to criminal penalties for violations of the Act (5 U.S.C. § 552a(i)) to the same extent as employees of the General Services Administration (GSA).

13.2 The Contractor hereby agrees and assures that each one of its employees know the prescribed rules of conduct, and each employee is aware that he/she can be subjected to criminal penalties for violations of the Privacy Act. A copy of the rules of conduct and other requirements are set forth in 45 CFR Part 5b.

13.3 Immediately notify the ordering agency's COR upon discovery or awareness that PII data pertaining to any/all related services to support official travel activities of authorized travelers has been lost, stolen, or compromised. In coordination with the COR, the Contractor shall notify all affected travelers, or other affected parties.

13.4 The Contractor will comply with host nation privacy laws, e.g. General Data Protection Regulation (GDPR), when operating in OCONUS locations.

14 PERSONNEL SECURITY

14.1 Establish appropriate administrative, technical, and physical safeguards to protect all non-public Government data to ensure the confidentiality, integrity, and availability of Government data. All Contractor personnel with access to or responsibility for non-public Government data under this contract shall comply with all security directives and instructions.

14.1.1 **Cleared Personnel: (If requested by an agency at the Task Order Level)** Provide personnel capable of obtaining the National Agency Check with Inquiries (NACI) - Non-Sensitive level and must receive a favorably adjudicated Tier-1 investigation from the Office of Personnel Management (OPM). The cost will be borne by the

Government. The NACI process for designated Contractor employees supporting the TMC services shall be initiated immediately after contract award and shall be completed prior to the end of the transition period.

14.1.2 Submit a request and list of personnel for security investigation to the civilian federal agency Security Office point of contact(s) to be provided by the ordering agency's COR NLT five (5) business days after contract award.

14.1.3 Submit confirmation via contractor-generated email to the ordering agency's COR NLT five (5) business days after submission of the request and list of personnel to the Government Security Office. The Government Security Office will initiate the Contractor's Electronic Questionnaire for Investigations Processing (eQIP). Contractor employees shall provide all requested information pursuant to the Privacy Act of 1974 when requested by the Government. For information visit: https://www.dcsa.mil/is/eqip/.

14.1.4 Contractor personnel with NACI who are assigned to perform work under this contract shall be required to obtain a Personal Identity Verification (PIV) when supporting civilian federal agencies. The cost is borne by the Government.

14.1.5 Personnel who are assigned to perform work under this contract may require access to Government resources (e.g., websites requiring CAC, Public Key Infrastructure [PKI], local badges, Contractor PIVs, and facility specific identification/access badges). Personnel required to obtain a PIV may be issued GFE (e.g., computer/laptop, etc.).

14.1.6 Provide a list of all contractor personnel requiring entry to on-site staffed locations to the ordering agency's COR No Later Than 60 calendar days prior to the service start date. List shall be submitted via contractor-generated email and include the individuals' full name, aliases, social security number (if applicable), home address and indicate the location which everyone will require entry.

14.1.7 As the contractor replaces employees, the contractor shall submit the outgoing employee's installation access badge/identification card (PIV) immediately to the local Installation Access Control Office or Government Security Office and prior to the request of issuance of a new badge/identification card(s). The list shall be updated within three (3) business days of changes or every 90 calendar days whichever comes first.

14.1.8 Submit confirmation via contractor-generated email to the ordering agency COR within three (3) business days of turning in the outgoing employee's access badge/identification card(s). The confirmation email shall include the employee's name, location(s)/installation(s), and date the installation access badge/identification card(s) (PIV) were turned into the local Installation Access Control Office or Government Security Office.

14.1.9 Return all PIVs and identification badges/cards issued to personnel to the Installation Access Control Office or DoD Government Security Office at the Government site/location upon completion of the contract, relocation, or termination of an employee, or upon request from the ordering agency COR in accordance with the facility information and security policies.

14.1.10 When the policy for a particular site/location requires only U.S. citizens to be hired, the Contractor shall adhere to the policy.

15 SERVICE LEVEL AGREEMENTS (SLA)

A service-level agreement (SLA) sets the expectations between the service provider and the customer and describes the products or services to be delivered, the single point of contact for end-user problems, and the metrics by which the effectiveness of the process is monitored and approved. The Government expects the TMCs under this schedule to meet the following SLAs**.**

Additional SLAs may be negotiated at the ordering agency TO Level. NEW Service Levels negotiated at the TO level cannot reduce the service level of the service (be less than) the SLAs in the Travel Agent Services SOW, however an ordering agency can request a higher service level.

SLAs in existing TOs, under this Schedule, may remain until the end of the full period of performance of the TO, which may not exceed a total period of performance of five (5) years from the date of award or when service begins, whichever is later.

To support this, **the Contractor will submit a monthly standardized scorecard** with all the key metrics for simplified performance management to the Task Ordering agency and to the GSA TMC PMO at tmcstrategy@gsa.gov.

15.1 Provide customer service and support 24 hours a day, 7 days a week, 365 days a year, including holidays or as requested by agencies.

15.2 Passenger Name Record (PNR)

15.2.1 Travel requests are processed accurately in a timely manner.

15.2.2 Urgent PNRs, for travel occurring in less than 24 hours, are processed within one (1) hour.

15.2.3 Canceled PNRs are canceled within one (1) calendar day.

15.2.4 Ticketed PNRs are processed immediately.

15.2.5 All PNRs are processed accurately 95% of the time.

15.3 Telephone and message handling.

15.3.1 Provide a **Service Level** of 70/30; 70% of calls answered within 30 seconds. The remaining 30% of call hold times should not exceed 60 seconds (1-minute).

15.3.2 Provide an **Abandoned Call** (abandonment) rate of less than 5%.

15.3.3 Provide the option for an automated call back service at any time while on hold.

15.4 Email response time.

15.4.1 Respond to 80% of emails within two (2) hours for urgent travel assistance during and after core (business) hours.

15.5 Chat response time (**Only applicable if Chat is offered by the TMC**).

15.5.1 **Live**[5]First Chat Response Time:

[5] Answered by a Travel Agent

15.5.1.1 Calculating Live Chat Metric: Average response time = Total time taken for an agent to respond during the selected period divided by the number of responses in the selected period.

15.5.1.2 Live Chat Performance Benchmark: 80% of chats are answered within 40 seconds.

15.5.1.3 First Response Time: 40 seconds

15.5.2 Live First Contact Resolution (FCR):

15.5.2.1 Calculating Live Chat Metric: For gross FCR: Number of contacts resolved initially ÷ All incoming contacts. For net FCR: Number of contacts resolved initially ÷ (All incoming contacts – Contacts that cannot be resolved at level one)

15.5.2.2 Live Chat Performance Benchmark: 70% of chats are resolved on First Contact

15.5.2.3 Live Chat FCR: 70%

15.6 Chatbot Response Time

15.6.1.1 Calculating Chat Metric: Average response time = Total time taken for a Chatbot to respond during the selected period divided by the number of responses in the selected period.

15.6.1.2 Chat Performance Benchmark: 80% of chats are answered within 40 seconds.

15.6.1.3 Chatbot First Response Time: 40 seconds

15.7 Customer satisfaction rating of at least 85%, based on a standardized government survey. The baseline survey will be developed by GSA and provided once approved by the appropriate organizations within GSA. GSA will work with the ordering agencies and the TMCs to update the survey at the ordering agency level.

15.8 GSA Data Transfer (See REPORTS)

15.8.1 This data transfer, to GSA, shall (1) meet a quality rate of 100% and (2) meet an on-time delivery expectation for ten out of twelve months in each Fiscal Year. If these goals are missed, the Contractor shall be required to provide a remediation plan within 10 business days to the GSA CO and shall be subject to monitoring of the performance of that plan. If not remediated timely, the contractor may be subject to additional task order consideration to offset the cost and performance impact to the government.

15.8.2 The data quality rate equals 1 minus (submissions with defects/total submissions) where a submission with defect is defined as a file that is missing required data elements or includes data that is not accurate and requires correction and resubmission by the contractor.

15.8.3 The on-time delivery expectation is on time delivery of all files for at least 10 out of 12 months in a fiscal year, where an on-time delivery is defined as a transmission to the GSA or a designated third-party data aggregator on or before the 15th of the

month following the month that data covers (unless a later delivery date is agreed to in advance by GSA).

15.8.4 For example, data for the month of July 2024 is due on or before the 15th of August 2024. Any data for this time provided after the 15th of August 2024 would be considered a late submission of data.

15.9 CBA reconciliation timeliness and accuracy.

15.9.1 The Contractor shall reconcile centrally billed accounts within five (5) business days of the receipt of travel card information. This may include an electronic CBA statement; for OCONUS locations this may include files associated with the CBA statement that can be downloaded via secure File Transfer Protocol (SFTP) or similar process.

15.10 Complaint resolution time

15.10.1 95% of complaints acknowledged within 24 hours; 95% of Contractor caused issues resolved within five (5) business days and Supplier caused issues resolved within 10 business days. The requestor will be notified of any delays in reaching a conclusion.

16 TMC IMPLEMENTATION & TRANSITION IN & OUT SERVICES

The Contractor shall, upon written notice, furnish phase-in, phase-out services for a minimum of ninety (90) business days prior to the expiration date of the task order or upon notification from the Government, agency, or organization. The Contractor shall provide sufficient, experienced personnel during the phase-in, phase-out period to ensure that there is no reduction in the quality of services provided under its task order.

16.1 Transition Out

16.1.1 The Contractor shall provide both transition (implementation) in and out services for a customer agency upon award of the customer agency task order and at the end of the period of performance if service is awarded to a successor Contractor. The Contractor shall submit and maintain a transition plan detailing all related transition-in activities and milestones to ensure successful on-time performance. The plan shall also include all transition out activities for transitioning services to a successor Contractor, under a future contract to ensure minimal disruption and no diminution in the quality of services.

16.1.2 The Contractor will comply with host nation employment laws, e.g. Transfer of Undertakings Protection of Employment (TUPE), when operating in OCONUS locations, and support such sharing of information during the Request for Quote process.

16.1.3 Phase-out plan updates shall be provided to the ordering agency's COR NLT 90 calendar days prior to the task order contract expiration date. The modified transition plan shall be submitted in a file format agreed upon by the Contractor and ordering agency's Contracting Officer (CO).

16.1.4 The Contractor shall maintain an adequate knowledge base of the Government's travel program to facilitate the transition to a new TMC with minimal disruption. Cooperative, orderly, and seamless transitions are crucial to the Government's mission requirements.

16.1.5 The Contractor shall furnish phase-in training to agencies or organizations transitioning to a new task order and exercise its best efforts to provide a cooperative, orderly, and seamless transition from the current TMC provider. This shall include a cooperative and professional arrangement with the incumbent as well as agencies and organizations.

16.1.6 Records Transfer: Upon request from the Government, agency, or organization, the Contractor shall provide to the successor Contractor copies of all bookings and Passenger Name Records (PNR) taken on or before the task order or contract expiration date, for travel taking place after the termination of the contract/task order. In addition, the Contractor shall provide the successor Contractor with all agency/organization profiles and all federal traveler sub-profiles as well as all federal travel preference profiles currently in possession of the Contractor.

16.1.7 Reservations: Upon request from the ordering agency, or organization, the Contractor shall book all requests it receives prior to contract expiration **regardless of the date of commencement of travel, if requested by the ordering agency**. Prior to the transition date, and for a window of time defined by the ordering agency, the Contractor shall issue tickets for booked travel that commences after the transition date and assist with changes to tickets.

16.1.8 Reconciliation: The Contractor shall reconcile each account balance and settle each transaction dispute within 180 calendar days of the completed agency or organization transition.

16.2 Transition In

16.2.1 The Contractor shall provide both transition (implementation) in and out services for a customer agency upon award of the customer agency task order and at the end of the period of performance if service is awarded to a successor Contractor. The Contractor shall submit and maintain a transition plan detailing all related transition-in activities and milestones to ensure successful on-time performance. The plan shall also include all transition out activities for transitioning services to a successor Contractor, under a future contract to ensure minimal disruption and no diminution in the quality of services.

16.2.2 The initial transition plan shall be submitted with the agency task order quote and a modified plan submitted to the ordering agency's COR via contractor-generated email no later than (NLT) ten (10) calendar days after contract award. In addition, the plan will be updated for each implementation phase to address any government agency, or organization requirements as mutually agreed during the planning and/or requirements gathering sessions, as defined in the modified plan. At a minimum, the plan should be updated no less than on a yearly basis or sooner if major operational changes occur that would necessitate an update to the plan.

16.3 Transition Services should be described in the transition plan. Services may include, but are not limited to:

16.3.1 Project schedule using Microsoft Office (or comparable software) established, including dates, owners, and tasks.

16.3.2 GDS installed.

16.3.3 GDS to GDS migration of un-ticketed travel records, if applicable.

16.3.4 Contractor Branch/Bridge Access between the Contractor pseudo city code (PCC)/OfficeID/SubscriberID and the ETS and/or the ETSNext Technology MSP OBT.

16.3.5 ARC/IATA numbers obtained.

16.3.6 Telephony established.

16.3.7 Reporting hierarchy set up.

16.3.8 Agreed staffing achieved, including on-site requirements, if applicable.

16.3.9 Verify that the Government preferred supplier rates (i.e., CPP, FedRooms, Amtrak, Rental Car) have been loaded and verified as accessible.

16.3.10 Profile Management (initial and ongoing feeds established based upon ETS vendor requirements).

16.3.11 Includes synchronization between GDS, ETS (ETS2 and the ETSNext Technology MSP) including the OBT, Authorization, and Voucher.

16.3.12 Customized counselor training completed, if applicable.

16.3.13 Execute change management process and communication to all stakeholders, as appropriate.

16.3.14 the ETSNext Technology MSP integration to TMC processes.

16.3.15 Quality assurance/file finishing processes and systems established and tested.

16.3.16 Other ancillary services deployed as agreed (traveler tracking, mobile app, etc.).

17 ETS2 REQUIREMENTS

17.1 In support of ETS2, as specified in agency task orders, the Contractor shall ensure that products/services provided to participating agencies complement and support ETS2 in an efficient and cost-effective manner.

17.2 The contractor will work with and exchange data with the ETS2 vendor as specified in the ETS2 contract, this schedule, and the ordering agency task order. This may include interfacing or integrating with the ETS provider by providing contact information, telephone numbers, file formats/sample PNRs, open branch access/pseudo city codes (PCC); participating in subcontractor or teaming agreements; participating in training and/or meetings; non-disclosure agreements; synchronization and security requirements; testing requirements; etc.

17.3 Unless otherwise mutually agreed to between the ETS and Contractor, ownership of the PNR shall reside with the ticketing entity.

17.4 The Contractor must state its understanding that its services, products, and processes offered must complement ETS2 for all agencies using ETS2. If the Contractor is offering a booking engine in conjunction with its offered services, it must state its understanding that such a booking engine may only be offered to those agencies not subject to the FTR and/or agencies with an approved exception per FTR 301-73.102 and 301-73.104.

18 ETSNext REQUIREMENTS

In support of ETSNext, as specified in ordering agency task orders, the Contractor shall ensure that products/services provided to participating agencies complement and support the ETSNext Technology MSP in an efficient and cost-effective manner.

The contractor will work with and exchange data with the ETSNext Technology MSP as specified in the ETSNext contract, this schedule, and the ordering agency task order. This may include interfacing or integrating with the ETSNext Technology MSP by providing contact information, telephone numbers, file formats/sample PNRs, open branch access/pseudo city codes (PCC); participating in subcontractor or teaming agreements; assisting the agency and ETSNext Technology MSP in completing the ETSNext **TMC Service Integration and Relationship Plan Guidance** , participating in training and/or meetings; non-disclosure agreements; synchronization and security requirements; testing requirements; etc.

Unless otherwise mutually agreed to between the ETSNext Technology MSP and contractors, ownership of the PNR shall reside with the ticketing entity.

The Contractor must state its understanding that its services, products, and processes offered must complement the ETSNext Technology MSP for all agencies using the ETSNext Technology MSP. If the Contractor is offering a booking engine in conjunction with its offered services, it must state its understanding that such a booking engine may only be offered to those agencies not subject to the FTR and/or agencies with an approved exception per FTR 301-73.102 and 301-73.104.

The Contractor shall utilize one of the following Global Distribution Systems (GDS) to support ETSNext: Amadeus, Sabre, and/or Travelport Plus.

18.1 ETSNext PNR Requirements

During the implementation of services to support the ETSNext Technology MSP, the Contractor must complete the Attachment *Travel Management Company Passenger Name Record Validation Configuration Worksheet*. This attachment will be available from the ETSNext Technology MSP upon award. This will occur as part of System Integration Testing (SIT) based upon guidance from the ETSNext Technology MSP.

The Passenger Name Record (PNR) Validation Configuration is a process that confirms the ETSNext Technology MSP Online Booking Tool (OBT) can exchange a PNR with the Travel Management Company (TMC) and provides the TMC with an example of an actual PNR that is delivered from the OBT. Additionally, the process assures that the OBT can send a PNR to the TMC on a specified queue and can sweep the PNR from the TMC outbound queue back into the OBT.

18.2 ETSNext Technology MSP and the Travel & Expense Business Standards

The ETSNext Technology MSP requirements are based upon the T&E Business Standards, which can be found at https://ussm.gsa.gov/fibf-travel/. TMCs that want to support agencies, as they transition to the ETSNext Technology MSP, beginning in 2024, shall support the T&E Business Standards including the Service, Function, Activities, Capabilities, Use Cases, and Data Elements for:

1. TRT.010.020 Travel Reservation Assistance and Processing
2. TRT.010.040 Travel Ticketing
3. TRT.010.050 Traveler Emergency Assistance Request Processing
4. TRT.010.070 Temporary Duty (TDY) and Local Travel Monitoring and Reconciliation
5. TRT.010.80 Temporary Duty (TDY) and Local Travel Regulatory Reporting
6. TRT.010.090 Temporary Duty (TDY) and Local Travel Management Reporting and Analysis
7. TRT.010.100 Temporary Duty (TDY) and Local Travel Policy Management and Audit
8. A RACI Chart breaking out the TMCs responsibilities will be available in the TMC Service Integration and Relationship Plan Guidance[6]

[6] The TMC Service Integration and Relationship Plan Guidance is being updated and may be renamed. The document will be provided prior to a kickoff meeting with the ETSNext Technology MSP.

Table 2 - T&E Service, Function, & Activities

Service Function ID and Name	Service ActivityID	Service Activity Name	Service Activity Description
TRT.010 Travel & Expense Management	TRT.010.020	Travel Reservation Assistance and Processing	Search for and identify transportation reservation information; Select transportation reservation information; Evaluate transportation reservation information (e.g., exception for contract city-pair fare, exception for coach-class accommodation); Translate common carrier fare basis code into terminology consistent with FTR; Calculate and document carbon footprint information; Search for and identify lodging reservation information; Select lodging reservation information; Evaluate exception information warranting reimbursement on an actual expenses basis; Search for and identify available lodging with rates above per diem at temporary duty (TDY) location(s) information; Search for and identify available lodging at alternate location(s) when lodging is not available at the temporary duty (TDY) location; Identify, apply, and document unused, partially used, or downgraded/exchanged ticket information; Identify, apply, and document promotional materials and frequent traveler benefits information; Develop and document travel reservation/updated reservation and fee information; Evaluate travel reservation/updated reservation information for completeness, errors, and compliance; Revise travel reservation/updated reservation to correct deficiencies, errors, and compliance issues; Develop and document notification to traveler of common carrier/commercial transportation schedule change(s) information; Develop and document updated reservation information; Cancel reservation information associated with canceled trip
TRT.010 Travel & Expense Management	TRT.010.040	Travel Ticketing	Evaluate ticket/updated ticket information for completeness, errors, and compliance; Revise ticket/updated ticket information to correct deficiencies, errors, and compliance issues; Issue ticket/updated ticket information to traveler; Receive notification to cancel or change issued ticket/updated ticket; Develop and document information for common carrier/commercial transportation to issue refund for unused, partially used, and exchanged ticket/updated ticket
TRT.010 Travel & Expense Management	TRT.010.050	Traveler Emergency Assistance Request Processing	Develop and document travel authorization information to interrupt or discontinue a temporary duty (TDY) travel assignment due to a personal emergency; Evaluate information to interrupt or discontinue a temporary duty (TDY) assignment due to a personal emergency; Route, review, date, and sign travel authorization information to interrupt or discontinue temporary duty (TDY) travel assignment due to personal emergency, and document results

Service Function ID and Name	Service ActivityID	Service Activity Name	Service Activity Description
TRT.010 Travel & Expense Management	TRT.010.70	Temporary Duty (TDY) and Local Travel Monitoring and Reconciliation	Develop and document completed trips with vouchers/claims for reimbursement not submitted information; Develop and document refundable unused, partially used, and exchanged ticket information; Collect non-refundable and Government Travel Request (GTR) unused, partially used, or downgraded/exchanged tickets, from travelers upon completion of travel; Develop and document penalty information for accepting unauthorized payment for expenses from a non-Federal source; Reconcile voucher and centrally billed account (CBA) travel card information
TRT.010 Travel & Expense Management	TRT.010.80	Temporary Duty (TDY) and Local Travel Regulatory Reporting	Develop and document travel and transportation payments (Travel Reporting Information Profile [TRIP] Report) information; Develop and document use of other than coach class transportation accommodations (Premium Class Travel Report [PCTR]) information; Identify and aggregate other than coach class transportation accommodations (Premium Class Travel Report [PCTR]) data that is protected from public disclosure by statute or Executive Order; Develop and document use of Government aircraft (to include chartered aircraft) by senior Federal officials and non-federal travelers (Senior Federal Travel Report [SFTR]) information; Develop and document travel expenses paid by non-Federal sources report information; Develop and document carbon footprint information for common carrier/commercial transportation and POV type
TRT.010 Travel & Expense Management	TRT.010.90	Temporary Duty (TDY) and Local Travel Management Reporting and Analysis	Develop and document travel information; Develop and document travel trends and patterns analysis content; Develop and document multiple government-designated sources
TRT.010 Travel & Expense Management	TRT.010.100	Temporary Duty (TDY) and Local Travel Policy Management and Audit	Determine and document per diem rate information and updates; Determine and document privately owned vehicle (POV) mileage reimbursement rate information; Develop and document government-wide and internal agency policies and associated compliance checks for Temporary Duty (TDY) and local travel; Develop and document traveler notification information for overpayment, or payment for expenses unnecessary or unjustified, with request for reimbursement to the Government

18.3 ETSNext PERFORMANCE WORK STATEMENT (PWS) TMC RELATED REQUIREMENTS

The following requirements, in the ETSNext PWS, require reciprocity between the ETSNext Technology MSP and the Contractor.

18.3.1 ETSNext PWS Requirements impacting the Contractor.

18.3.1.1 The ETSNext PWS requires the ETSNext Technology MSP to "establish a TMC Service Implementation, Integration, and Relationship Plan (Roles and Responsibilities) for each TMC and its Federal agency customer that ensures no degradation of services and documents the roles and responsibilities of the parties so that the Federal traveler experiences seamless, comprehensive, streamlined, high quality, and secure travel services."

18.3.2 ETSNext TMC Set-Up and Integration

18.3.2.1 The Contractor shall work with the ETSNext Technology MSP to complete an individual plan for each Federal agency's TMC set-up and integration.

18.3.2.2 The plans shall be reviewed by the Contractor, the ordering agency, and the ETSNext Technology MSP at least annually with updates incorporated as applicable.

18.3.2.3 The plans shall address all steps necessary to set up and implement the agency selected TMC.

18.3.2.4 The plans shall outline the tasks & responsibilities for transition to a successor TMC, in the event an agency changes TMCs during the period of performance of the ETSNext Technology MSP.

18.3.2.5 Sample plan is included in Attachment J-7 of the ETSNext Solicitation: TMC Service Integration and Relationship Plan Guidance.

18.3.3 ETSNext MSP & TMC Integration Operation

18.3.3.1 The Contractor shall review ETSNext Technology MSP written notice of pending ETSNext Technology MSP solution releases and communicate any impacts to the ordering agency and ETSNext Technology MSP within five (5) business days.

18.3.3.2 The Contractor shall review the written release notes from the ETSNext Technology MSP that explain the changes in functionality and any actions or updates required by the Contractor. The Contractor will notify the ordering agency, the GSA ETSNext shared service PMO, and the ETSNext Technology MSP how much time is necessary to make updates to Contractor systems.

18.3.3.3 The Contractor, after advanced written notice from the ETSNext Technology MSP, shall conduct System Interface Testing (SIT) and User Acceptance Testing (UAT), depending on the extent of the changes, as outlined in the agreed upon TMC Service Integration and Relationship Plan.

18.3.3.4 The Contractor shall review written notification from the ETSNext Technology MSP of planned outages, which will be provided at least one week in advance of the planned outage. The Contractor will notify the ordering agency, the GSA ETSNext shared service PMO, and the ETSNext Technology MSP of any issues with the timing of the proposed planned outages.

18.3.3.5 The Contractor will notify the ETSNext Technology MSP of any PNR content problems, believed to be a result of the ETSNext Technology MSP. The Contractor will utilize the issue prioritization categories outlined in Customer Support #40 of the ETSNext Solicitation. In the event the issue is not resolved

satisfactorily, the Contractor shall notify the GSA ETSNext shared service PMO and the ordering agency for adjudication:

18.3.3.5.1 "Respond and provide resolutions in accordance with an approved industry standard similar to the following (Performance Requirement Summary Item 27):

18.3.3.5.1.1 Critical - resolution <8 hrs.; response <1 hr.

18.3.3.5.1.2 b. High - resolution <48 hrs.; response <4 hrs.

18.3.3.5.1.3 c. Medium - resolution <5 days; response <24 hrs.

18.3.3.5.1.4 d. Low - resolution <4 weeks; response <48hrs"

18.3.3.6 The Contractor will utilize training, provided by the ETSNext Technology MSP, on the ETSNext solution(s), its functionality, and configurations. This will ensure the Contractor understands how its services impact the ETSNext Technology MSP.

18.3.3.6.1 Training will be included for initial implementation as well as for new employees and new major releases.

18.3.3.6.2 The Contractor will coordinate with the ETSNext Technology MSP to arrange the appropriate time for these training sessions.

18.3.3.7 The Contractor shall make improvement suggestions to increase online adoption, touchless rates, and efficiency to the ordering agency, and the GSA shared service PMO.

18.3.3.8 **Duty of Care**: The Contractor shall:

18.3.3.8.1 The Contractor shall, if asked by the ETSNext Shared Service PMO and the ETSNext Technology MSP, support, and queue reservation data to an ETSNext Shared Service PMO and the ETSNext Technology MSP to an approved third-party Duty of Care Solution / Service Provider at no added cost to the government.

18.3.3.8.2 If the ETSNext Shared Service PMO and the ETSNext Technology MSP do not request or provide a third-party Duty of Care Solution / Service Provider, the Contractor will provide **real-time location support** via the Contractor's own solution(s) e.g. reporting solution, GDS data, etc.

18.3.3.8.3 If the ETSNext Shared Service PMO and the ETSNext Technology MSP do not request or provide a third-party Duty of Care Solution / Service Provider, the Contractor will provide **Messaging** technology to alert travelers or managers with trip-specific messaging, before, during, and after the trip.

18.4 FEDERAL SECURITY STANDARDS FOR the ETSNext Technology MSP

18.4.1 Contractor (TMC) Non-Federal System with Controlled Unclassified Information (CUI) (800-171)

18.4.1.1 The Contractor shall adhere to and shall support the current and future versions of the NIST security standards for a Non-Federal System with CUI NIST 800-171 Rev.2 as defined in IT Security Procedural Guide: Protecting Controlled

Unclassified Information (CUI) in Nonfederal Systems and Organizations Process CIO-IT Security-21-112. The sections below include key highlights from the guide.

18.4.1.2 The Contractor shall build the cost of the current and future versions of the NIST 800-171 Rev.2 security standards into its transactional pricing using the Price Proposal Template provided for Refresh 21 and future versions.

18.4.1.3 The Contractor shall implement the controls to meet the standards as identified in the current and future versions of NIST 800-171 Rev.2 document and document it in their System Security and Privacy Plan (SSPP).

18.4.1.3.1 NIST 800-171 Rev.2, Appendix D Mapping Tables maps the 800-171 Controls to the ISO 27001/IEC 2013 controls.

18.4.1.3.2 For work supporting the Department of Defense, Defense Travel Management Office (DTMO) Contractors and the United States Coast Guard (USCG) shall also have to comply with current and future versions of DFARS 252.204-7012.

18.4.1.3.3 The Contractor shall complete the **CUI Nonfederal SSPP Template**, available from the GSA's Chief Information Security Officer's (CISO) office. This template will be provided, upon request, to the Contractor. This template is not publicly available.

18.4.1.4 The Contractor shall have a FedRAMP Third-Party Assessment Organization (3PAO) or independent assessor (to be accepted by the GSA Office of the Chief Information Security Officer) complete a Security Assessment Report (SAR) verifying that the Contractor has implemented the security controls.

18.4.1.5 The Contractor shall send the CUI Nonfederal SSPP, SAR, and supporting documents (approval package) to the GSA CISO's office for review, who will recommend remediations, and to make an informed risk-based approval decision.

18.4.1.5.1 After review and remediations (including a Plan of Actions and Milestones (POA&M)), if the level of residual risk is acceptable, the GSA CISO's office will issue a Memorandum for the Record (MFR). The MFR will record that the approval package provides sufficient evidence that CUI is appropriately protected by the Nonfederal System and authorize the system's use.

18.4.1.5.2 Ordering agencies issuing RFQs under this schedule will be provided with the MFR and approval package to leverage the work already completed by the Contractor.

18.4.1.5.2.1 Ordering agencies will still be responsible for documenting the Customer Responsible Controls in the agency's SSPP and issuing an Authority to Operate (ATO) or an Authority to Use (ATU) for their responsible controls.

18.4.1.6 Continuous Monitoring

18.4.1.6.1 The Contractor shall implement the proper process for ongoing Security Assessments, Section 3.12 of current and future versions of NIST

800-171 Rev.2, including Continuous Monitoring. GSA Continuous Monitoring requirements are identified in Section 2.5 of IT Security Procedural Guide: Protecting Controlled Unclassified Information (CUI) in Nonfederal Systems and Organizations Process CIO-IT Security-21-112.

18.4.1.6.2 The Contractor will provide GSA's CISO's office with the appropriate supporting documentation Quarterly, Annually, and every three (3) years.

18.4.1.6.2.1 Quarterly Deliverables include:

18.4.1.6.2.1.1 Authenticated Vulnerability Scanning Reports (Including compliance scans)

18.4.1.6.2.1.2 POA&M Update

18.4.1.6.2.2 Annual Deliverables include:

18.4.1.6.2.2.1 Updated CUI Nonfederal SSPP

18.4.1.6.2.2.2 Updated Privacy Threat Assessment (PTA) and Privacy Impact Assessment (PIA)

18.4.1.6.2.2.3 Penetration Test

18.4.1.6.2.3 Every three (3) years

18.4.1.6.2.3.1 SAR – Two (2) months prior to the completion of the government fiscal year, ending on September 30. Due date is the last workday of July.

18.4.1.6.2.3.2 GSA's CISO's Office will notify the Contractor of any issues and request an updated POA&M as needed.

18.4.1.6.2.4 Ad-Hoc Activities

18.4.1.6.2.4.1 Implement and Response to CISA Emergency Directive (ED) and Binding Operational Directive (BOD) - CISA BOD and EDs are compulsory directions for purposes of safeguarding federal information and information systems.

18.4.1.7 Additional Security Requirements for Non-Federal Systems with CUI (NIST 800-171)

18.4.1.7.1 The Contractor shall meet these additional security requirements if requested by the ordering agency at the TO level.

18.4.1.7.2 The Contractor should build the cost of the additional security requirements as separate CLINs using the Pricing Template provided for Refresh 21 and future versions.

18.4.1.7.3 **Contractor (TMC) Non-Federal System with CUI (800-171) - MFR including Leveraged FedRamp for Software as a Service (SaaS)**.

18.4.1.7.3.1 Contractors leveraging external cloud-based Software as a Service (SaaS) shall be limited to SaaS that is FedRAMP Authorized as listed in the FedRAMP Marketplace. The Contractor shall identify the leveraged FedRAMP Authorized SaaS in their SSPP and document the customer responsible controls for the leveraged SaaS in their SSPP.

18.4.1.7.3.1.1 Additional information is available in ATTACHMENT 1: - Data Elements - FedRamp.xlsx.

18.4.1.7.4 **Enhanced 800-171 Requirements** - Ordering agencies may issue their own Authority to Operate (ATO) or Authority to Use (ATU) in place of the GSA MFR for NIST SP 800-171 and/or require monthly submission of continuous monitoring deliverables and annual security assessments for one-third (1/3) of the required security controls plus a full security assessment of all required controls every 3 years.

18.4.2 **Contractor (TMC) Traditional Assessment & Authorization (A&A) in Agreement with NIST 800-37 Rev 2 and NIST 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations at the FIPS 199 Moderate Impact Level**.

18.4.2.1 The Contractor shall support ordering agency requirements for A&A following their Agency' specific security A&A policies and procedures aligned to NIST 800-37 Rev 2.

18.4.3 **Contractor (TMC)FedRamp ATO for fully cloud-based solution(s)**.

18.4.3.1 Contractor (TMC) solutions delivered as-a-service in the cloud, meeting the NIST 800-145 cloud definition, consistent with the OMB FedRAMP Policy memo, are subject to FedRAMP cloud information security and privacy requirements and shall be FedRamp authorized.

18.4.3.1.1 If the solution is hosted in an existing FedRamp environment, the associated FedRamp Authorization may be able to be leveraged for some of the required FedRAMP controls.

18.4.3.1.2 Refer to FedRAMP.gov for details about pursuing a FedRAMP Agency Authorization.

18.4.4 Cyber Supply Chain Risk Management (C-SCRM).

18.4.4.1 The Contractor must participate in GSA's C-SCRM Program including maintenance of a SCRM Plan and monitoring via third-party vendor risk illumination tools.

18.4.4.2 Please note, ordering agencies may have additional SCRM requirements at the task order level and will specify any additional requirements in the task order request.

18.4.4.3 Cyber-Supply Chain Risk Management (C-SCRM) Plan

18.4.4.3.1 The Contractor must maintain a C-SCRM plan which identifies, if available, any relevant SCRM-related International Organization for Standardization (ISO) certifications (e.g. ISO 20243:2018, ISO 27K series, ISO 28K series). The C-SCRM plan must address the NIST 800-161 cyber supply chain security controls identified in Table 1 below. These controls are derived from NIST 800-53 Rev 5 and related to expanded supplemental guidance for mitigating supply chain risk that are complementary to the NIST 800-171 requirements for CUI.

Table 3 - NIST 800-53 Rev.5 Controls selected for C-SCRM Plan

NIST SP 800-53 Rev 5 Control ID	NIST SP 800-53 Rev 5 Control Name
SA-4	Acquisition Process
SA-11	Developer Testing and Evaluation
SA-15	Development Process, Standards, and Tools
SA-8	Security and Privacy Engineering Principles
SI-7	Software, Firmware, and Information Integrity
SR-6	Supplier Assessments and Reviews
SR-8	Notification Agreements
SR-10	Inspection of Systems or Components
SR-11	Component Authenticity
SR-12	Component Disposal

18.4.4.3.2 The Contractor's C-SCRM Plan must describe in sufficient detail, beyond high level overview representations, how they will reduce and mitigate SCRM through application/mapping of their defined program appropriate security controls outlined and described in the current and future versions of CNSSI 1253, Appendix D, NIST SP 800-53, NIST SP 800-161, and related industry. Any Information Security Management Systems (e.g. ISO 27K series) controls, or related program standards, should be mapped to their associated NIST baseline controls, where applicable.

18.4.4.3.3 The supply chain must span from the lowest sub-component producer or manufacturer to the delivery point of the Contractor, or its designated agent, through third party installation, maintenance, and support. The C-SCRM plan, implementation, and risk assessment methodology processes must follow Appendix D and E of NIST SP 800-161 and NISTIR 7622 guidelines, ensuring application to the Contractor and their suppliers, partners, distributors, and any other entity that is responsible for handling or managing the supply chain of the products and services offered under these TOs. If a Contractor represents a Prime/Subcontractor relationship, then all C-SCRM plan requirements must also be flowed down to the respective subcontractor(s). The Prime must be responsible for C-SCRM plan implementation and adhere to reporting requirements represented by the defined relationship.

18.4.4.3.4 If the Contractor uses dealers/resellers in the performance of work under the TO, the C-SCRM plan must address the use of participating dealers/resellers and provide a listing of each participating dealer/reseller who is permitted to fulfill orders under the TO.

18.4.4.3.5 NOTE: Within 12 months after TO award all identified participating dealers/resellers specified in the SCRM plan must be International Organization for Standardization (ISO) 9001:2015 certified and maintain certification for the remaining performance period of the TO. Should any participating dealers/resellers not obtain ISO 9001:2015 certification within 12 months after TO award, the participating dealer/reseller will not be permitted to fulfill orders.

18.4.4.4 Vendor Risk Assessment Program - C-SCRM Monitoring

18.4.4.4.1 Upon award, GSA will execute their Vendor Risk Assessment Program (VRAP) as an on-going enterprise approach to continuously manage risk and vulnerabilities associated with the acquisition and sustainment of products or services provided by the Contractor. VRAP is a post-award execution activity from an oversight perspective. The program leverages big data analytics to identify, categorize, and assess risk information based on the Risk Factors listed in Table 2. GSA's VRAP utilizes customer defined priorities and risk tolerances, along with twelve defined Risk Factors, to compartmentalize risk findings and provide a well-defined process. As part of the VRAP, GSA may utilize supplier illumination tools to monitor and evaluate risks to its customer's supply chains. GSA reserves the right to identify to the Contractor for evaluation, known or potential risks in delivery order execution related to suppliers of products and ancillary service. The Contractor must provide any information requested by the Government to facilitate a VRA within 10 business days of receiving a written request.

Table 4 - Risk Factors and Definitions

Analytical Categories	Risk Factor	Description
Technical	**Quality Assurance**	Customer reviews, adherence to quality standards.
	Production / Manufacturing	Production/manufacturing strategy, plans, and implementation. Current state relative to controls and practices for assuring authenticity and integrity of product/service as received by the end-user, and instances of reported or alleged counterfeit product or fraudulent practices.
	R&D / Innovation	Current state, investment in and plans for product/process improvements and advancements.
Business Management	**Leadership & Organization**	Current and prior affiliations and associations of company leaders. Current state, strategy and plans relative to the organization of the operating unit and relationship to parent, subsidiary or affiliated organizations.
	Supplier Management	Current state, strategy and plans relative to suppliers and supply chain management.

Analytical Categories	Risk Factor	Description
	Business Alliances	Current state, strategy and plans relative to key joint ventures, partnerships, acquisitions, and agreements (including technology/intellectual property).
Market	**Revenue/Financial Health**	Financial status, sources of investment, and revenues by category/source, including indirect and direct funding from U.S. Government organizations.
	Industry/Market Position	Current state, strategy and plans relative to the market/industrial environment, potential customers, and competitors.
	Regulatory & Legal	Status relative to regulatory/legal trends, actions, issues, and concerns.
Security	**Socioeconomic Environment**	Current state, trends, issues and concerns relative to the geographical locations and socioeconomic conditions in which the business/enterprise is operating.
	Cybersecurity	Current state, issues, and concerns relative to cybersecurity. Technical vulnerabilities, instances of cyber breach or historic trends.
	Physical Security & Insider Threat	Physical security employed at design, manufacturing, packaging, and distribution facilities. Security issues and concerns emanating from people involved with the operating unit, including employees, former employees, Contractors, and business associates.

18.4.4.5 Ongoing C-SCRM Monitoring

18.4.4.5.1 During the Contractor's period of performance, the Contractor must provide an annual report to the GSA Contracting Officer, Program Manager, and COR on their SCRM activities, related to the TO, due upon the anniversary of the TO award and continuing on subsequent anniversary dates of the Contractor's TO award date until the end of the TO period of performance. The report must include reporting on the detection of all SCRM compromises/incidences associated with the performance under the TO, mitigation actions taken, and any resultant impacts to hardware, software, firmware, and data/information consistent with NIST SP 800-161, Appendix B – Incident Response Control Requirements. GSA reserves the right to verify performance against C-SCRM plan requirements through assessment and inspection of the Contractor's facilities and programs in accordance with proper notification procedures and contractual clauses. Successful incident identification and remediation will be viewed favorably with respect to overall strength of C-SCRM security program execution.

18.4.4.5.2 The Contractor must also provide a C-SCRM Plan Update to the GSA Contracting Officer, Program Manager, and the COR within 10 business days whenever there is a substantial change that affects one or more CNSSI 1253 security controls. At a minimum the following events substantiate the need for an update: changes in company ownership, changes in senior company leadership, supplier changes, including new capabilities added through new vendors or components, subcontractor changes, and Information and Communication Technology (ICT) supply chain compromises.

18.4.4.6 Off-Ramping - SCRM + VRAP Elements

18.4.4.6.1 The Government reserves the unilateral right to Off-Ramp nonperforming Contractors. Contractors that are Off-Ramped must still complete active orders at the time of the Off-Ramping. Off-ramping methods may result from one of the following conditions:

18.4.4.6.2 Failure to meet SCRM and SCRM reporting requirements in sections Cyber-Supply Chain Risk Management (C-SCRM) Plan or failure to remediate successive, repeated security process control failures (greater than two) within the annual reporting cycle. Additional audit/inspection assessment visits may be executed by the Government team to validate compliance.

18.4.4.6.3 Offerors assessed as high risk relative to defined Vendor Risk Assessment Program (VRAP) factors in Table 4 - Risk Factors and Definitions and the Supply Chain Risk Management (SCRM) Factor Information Disclosure Request. Additional audit/inspection assessment visits may be executed by the Government team to validate responses.

18.4.4.6.4 If an Offeror does not meet these expectations, it is the Government's intent to "off-ramp" the Offeror by:

18.4.4.6.4.1 Implementing a termination for convenience (if applicable and only if such action is in the Government's best interest); or

18.4.4.6.4.2 Implementing a termination for cause, if applicable; or

18.4.4.6.4.3 Taking any other action which may be permitted under the contract terms and conditions.

18.5 TMC SUPPORT FOR GSA SmartPay® AS PART OF THE ETSNext Technology MSP

18.5.1 The Contractor shall support the ETSNext Technology MSP and its use of the GSA SmartPay® program including follow-on contracts. The current contract, GSA SmartPay® 3 expires in 2031. The Contractor shall continue to support the ETSNext Technology MSP and the ability to support all required, no-cost items (as defined in the GSA Smartpay® contract as outlined in the next paragraph) included in the follow-on contract to the GSA SmartPay® 3 master contract (once established) at no additional cost to the Government.

18.5.2 Specifically, the Contractor shall support an agency's transition to the ETSNext Technology MSP and can support all required, no cost items detailed in the GSA SmartPay 3 master contract, including, but not limited to: chip cards, declining balance cards, ePayables, foreign currency cards, ghost cards, GSA SmartPay Tax Advantage Travel Card Account cards, mobile payments, single use accounts, and virtual cards.

18.5.3 In addition, the Contractor shall support the ETSNext Technology MSP and its ability to support all emerging technology, that is a part of the GSA SmartPay master contract.

18.5.4 When GSA's SmartPay 3 master contract expires or an agency decides to change GSA SmartPay vendors during the life of the GSA SmartPay or the ETSNext Technology MSP master contracts, the Contractor shall support the required capabilities to ensure a seamless transition including updating all or part of an agency's profiles or other authorization and expense accounting information with new account information (e.g., account numbers, expiration dates, etc.) without disruption of service.

19 CITY PAIR PROGRAM (CPP) REQUIREMENTS

The Contractor shall:

19.1 Ensure that the city pair carrier and the contract fares are booked unless a valid exception applies. Please see EXPLANATORY CODES.

19.2 There are currently four types of CPP contract fares, all of which are fully refundable, with no penalties or change/cancellation fees attached. Please see **YCA Fare**, _CA Fare, _CB Fare, and _CP Fare in the Definitions section.

19.2.1 Please see **Auto-cancellation** in the Definitions section for information on the CPP Auto-cancellation policy.

19.3 Though available only to military and Government personnel, Discount Government (DG) (sometimes referred to as "Me Too," fares are NOT contract fares under the CPP. They are only to be quoted and/or used when one of the FTR exceptions to the use of contract fares is applicable.

19.4 Where no contract fare exists and common carriers furnish the same service at different fares between the same points for the same type of accommodations, the Contractor shall ensure travelers use the lowest available fare in accordance with the ordering agency's policies unless the ordering agency determines that the use of higher cost service is more advantageous to the Government. This includes, but is not limited to a:

19.4.1 Combination of contract fares; or

19.4.2 Combination of a contract fares and the lowest available fare

19.5 In addition, the Contractor shall ensure that fare rules are followed in accordance with the Airline Tariff Publishing Company (ATPCO) tariffs or as contained in the carrier's contract of carriage for domestic markets, and for international markets, in accordance with the Fly America Act and the International Air Transportation Association (IATA) tariffs or as contained in the carrier's contract of carriage where no contract fare exists.

19.6 Ensure that only authorized users of the CPP, as specified by GSA, are given access to contract City-Pair fares. This entails understanding the Government's list of eligible/non-eligible entities (free training will be provided by the GSA, for official government travel only, on request—contact onthego@gsa.gov, subject: CPP Training).

19.7 Ensure that Government contractors are not provided access to contract City-Pair fares.

19.8 Ensure that when Government contractors need to travel for a federal customer, that the travel is arranged using the proper form of payment and account numbering sequence that denotes no access to the CPP.

19.9 Ensure that reason codes as defined in the Schedule Valid Exception Codes; and in Government T&E management systems such as ETS/DTS are captured for each air transaction.

19.10 Document and report City Pair usage/non-usage.

19.11 Provide information to the traveler as to fare availability when dual fares (two coach class contract City- Pair fares) exist for a requested City Pair.

20 FLY AMERICA ACT REQUIREMENTS

The Contractor shall:

20.1 Ensure that travel is made in accordance with the Fly America Act. This Act requires Federal travelers to use a U.S. flag air carrier service for all air travel funded by the Government except when:

20.1.1 Use of a foreign air carrier is determined to be a matter of necessity in accordance with Sec. 301-10.138 of the Federal Travel Regulation; or

20.1.2 The transportation is provided under a bilateral or multilateral air transportation agreement to which the United States Government and the government of a foreign country are parties, and which the Department of Transportation has determined meets the requirements of the Fly America Act; or

20.1.3 The traveler is an officer or employee of the Department of State, or USAID, and travel is paid with funds appropriated to one of these agencies, and travel is between two places outside the United States: or

20.1.4 No U.S. flag air carrier provides service on a particular leg of the route, in which case foreign air carrier service may be used, but only to or from the nearest interchange point on a usually traveled route to connect with U.S. flag air carrier service; or

20.1.5 A U.S. flag air carrier involuntarily re-routes travel on a foreign air carrier; or

20.1.6 Service on a foreign air carrier would be three hours or less, and use of the U.S. flag air carrier would at least double the enroute travel time; or

20.1.7 When the costs of transportation are reimbursed in full by a third party, such as a foreign government, international agency, or other organization.

20.2 For travel between the US and another country:

20.2.1 If a U.S. flag air carrier offers nonstop or direct service (no aircraft change) from the origin to destination, a U.S. flag air carrier service must be used unless such use would extend the travel time, including delay at origin, by 24 hours or more.

20.2.2 If a U.S. flag air carrier does not offer nonstop or direct service (no aircraft change) between the origin and destination, a U.S. flag air carrier must be used on every portion of the route where it provides service unless, when compared to using a foreign air carrier, such use would:

20.2.2.1 Increase the number of aircraft changes that the traveler must make outside of the U.S. by 2 or more; or

20.2.2.2 Extend the travel time by at least 6 hours or more; or

20.2.2.3 Require a connecting time of 4 hours or more at an overseas interchange point.

20.2.3 For travel solely outside the US, the traveler must always use a U.S. flag carrier for such travel, unless, when compared to using a foreign air carrier, such use would:

20.2.3.1 Increase the number of aircraft changes you must make en route by 2 or more; or

20.2.3.2 Extend your travel time by 6 hours or more; or

20.2.3.3 Require a connecting time of 4 hours or more at an overseas interchange point.

21 OPEN SKIES AGREEMENT REQUIREMENTS:

Under the United States-European Union (EU) Open Skies Agreement, community airlines have the right to transport passengers on scheduled and charter flights funded by the U.S. Government, when the transportation is between a point in the United States and any point in a Member State or between any two points outside the United States except when:

21.1 There is a city-pair contract fare in effect for air passenger transportation services, or

21.2 Transportation is obtained or funded by the Secretary of Defense or the Secretary of a military department.

A listing of the Member States as found in the U.S.-EU Open Skies Agreement may be accessed via the Department of State's Web site https://www.state.gov/open-skies-partners/.

22 LODGING REQUIREMENTS

22.1 The Contractor must first provide civilian federal travelers with access to FedRooms® properties and FedRooms® rates and book a FedRooms® rate, at a FedRooms® property, when it is available. FedRooms® rates should be booked using the XVU (FedRooms®), XVC (FedRooms® Commissionable), GDS, NDC, and other content supplier proprietary rate codes.

22.2 Contractors supporting the Department of Defense must provide DOD Preferred® Properties and DoD Preferred® Rates and book a DOD Preferred® Property and a DoD Preferred® Rate when it is available. DoD Preferred® rates should be booked using the XVL (DoD Preferred®), GDS, NDC, and other supplier proprietary rate codes. If DoD Preferred® Properties are not available, travelers should be provided with FedRooms® Properties and Rates per FTR 301-11.11.

22.3 The Contractor shall establish, at a minimum, a weekly feed (if not more frequently) of the current FedRooms® hotels and rates with the third-party contractor that manages the FedRooms® program on the government's behalf. This feed should be used to update the GDS weekly, (if not more frequently).

22.4 Where FedRooms® and DOD Preferred properties are not available, the Contractor shall endeavor to ensure access to reservations for quality lodging within allowable per diem reimbursement limits. Travelers within the United States should always stay in a fire safe facility that meets the fire safety requirements of the Hotel and Motel Fire Safety Act of 1990, as amended (see 5 U.S.C. 5707a). If a FedRooms® property is not available in the location to meet the

traveler needs, the contractor must provide the traveler with a list of alternative facilities that meet the fire safe requirements of the Act.

22.4.1 Fire Safety Act approved facilities can be found https://apps.usfa.fema.gov/hotel/. All FedRooms® properties are verified for FEMA certification and compliance.

22.5 Training and training materials for travel agents on how to book a FedRooms® property can be obtained by contacting the FedRooms® program manager at GSA and/or the third-party contractor for FedRooms®. The current Governmentwide TDY Lodging contract, which is the backbone for the FedRooms® program, runs through September 30, 2024. The next Governmentwide TDY Lodging contract will be awarded in the calendar year 2024 and begin on October 1, 2024.

22.6 FEDROOMS® PREFERENCING RULES

22.6.1 The Contractor shall first offer FedRooms® properties and offer travelers the FedRooms® rates.

22.6.1.1 Offer FedRooms® rates at FedRooms® hotels within 2 miles of densely populated, metropolitan areas.

22.6.1.2 Offer FedRooms® rates at FedRooms® hotels within 10 miles in rural areas.

23 RAIL & AMTRAK

23.1 AMTRAK

Amtrak offers federal government employees discounted fares for business travel within the Northeast Corridor, as well as discounts for business travel on coach fares nationwide. To receive the Federal Government discount, reservations must be booked through a federal employee's TMC or OBT. They may not be booked on Amtrak.com. For more information, contact AmtrakGovernmentTravel@Amtrak.com.

To access the government discounted fares, TMCs will need to load the appropriate Corporate Discount Number (CDN) into the GDS. All federal agencies use the same CDN to access the government discounted fare.

Government discounted fares are available on

- Acela
- Northeast Regional
- State Supported Routes
- National Network

Federal government travelers will find discounted fares available across the country on coach fares.

Business Class (except on Acela), Private Rooms or other upgrades are excluded from the Amtrak Federal Discount Program but are available to book as upgrades. Refund rules for those upgrades will apply. The Canadian Maple Leaf service offers the Federal Discount through Niagara Falls, NY. Discounts apply to all

dedicated Amtrak Thruway bus services. Dedicated means Thruway services contracted by or operated by Amtrak. Where non-dedicated Thruway buses are available (i.e., Greyhound), the discount will not apply.

23.2 INTERNATIONAL RAIL

Upon traveler request, the contractor shall facilitate the purchase of international rail tickets, passes, etc., either through the GDS, rail company websites, or third-party aggregators. The transactions will be considered part of a **Transaction A** for air/rail.

24 GROUND TRANSPORTATION

24.1 CAR RENTAL

When authorized to use a rental vehicle for TDY purposes, the Contractor shall ensure that the traveler is informed that they must rent a vehicle from a vendor that participates in the DTMO Government Rental Car Program and Rental Truck Program, which provides pickup, cargo van, utility, and commercial straight truck rentals for authorized military members and federal employees during official travel, unless no agreement is in place for the TDY location or as otherwise exempted by agency policy. DTMO administers the programs through car and truck rental agreements with participating vehicle rental companies.

For more information on the U.S. Government Rental Car or Truck Programs, go to https://www.travel.dod.mil/Programs/.

The DTMO has negotiated rental car agreements that include automatic unlimited mileage, collision damage insurance and maximum rates. The Contractor shall ensure that the traveler is informed of any insurance requirements for cars or trucks booked outside of the Rental Car and Rental Truck programs.

The negotiated rates are based upon the Corporate Discount (CD) Number assigned to each agency and provided by the DTMO. The TMC will receive the file as part of the Implementation / Transition In or it can be requested from the DTMO at dodhra.mc-alex.dtmo.mbx.rental-car-program@mail.mil.

25 GSA SmartPay® SUPPORT

Established in 1998, the GSA SmartPay program is the world's largest government charge card and commercial payment solutions program, providing services to more than 560 federal agencies/organizations and Native American tribal governments.

GSA SmartPay payment solutions enable authorized government employees to make purchases on behalf of the federal government in support of their agency's mission. For additional information, please visit https://smartpay.gsa.gov/.

25.1 The Contractor should propose any costs related to supporting the products and services available in the GSA SmartPay® 3 and follow on contract, e.g., costs for supporting Virtual cards, single use accounts, etc.

25.2 When the GSA's SmartPay 3 master contract expires it will create a requirement for all travel charge card numbers (IBAs and CBAs) resident in the traveler's profiles to be replaced with new charge card numbers and expiration dates on (or before) the expiration date. This same requirement may result from an agency's decision to change SmartPay vendors during the life of the SmartPay.

The contractor shall support the required capabilities to ensure a seamless transition in updating profiles, as necessary, from existing to new charge card numbers without disruption of service.

26 REPORTS

26.1 Standard Reports to be provided to the Ordering Agency

The Contractor shall provide to the ordering agency the Standard Reports, listed below, and any reports requested by the ordering agency, that are not available in the Contractor's reporting solution.

The following standard reports shall be provided to the ordering agency. The Contractor shall define what information it will provide in the report or what will be available in the offered reporting solution as part of its proposal and response to a Request for Quote (RFQ).

Table 5 - Standard Travel Reports for the Ordering Agency

	Report Name	Category	Purpose	Minimum Frequency
1	Total Airline Spend	Air	Look at volume for trends/anomalies	Quarterly
2	Total Airline Spend by Carrier	Air	Look at volume for trends/anomalies	Quarterly
3	Total Air Spend by City Pair	Air	Look at volume for trends/anomalies	Quarterly
4	Total Air Spend Domestic vs International	Air	Look at volume for trends/anomalies	Quarterly
5	Total Air # of Tickets Issued	Air	Look at volume for trends/anomalies	Quarterly
6	Average Air Ticket Price	Air	Review spending on non-contract fares to see impact and analyze for policy compliance	Monthly
7	Air Unused Tickets	Air	Ensure reuse of tickets when available	Monthly
8	Total Hotel Spend	Hotel	Look at volume for trends/anomalies	Quarterly
9	Total Spend by Hotel	Hotel	Review spending on non FedRooms® and/or Rates to see impact and analyze for policy compliance	Quarterly
10	Total Room Nights by Hotel	Hotel	Look at volume for trends/anomalies	Quarterly

	Report Name	Category	Purpose	Minimum Frequency
11	Total Car Rental Spend	Car	Look at volume for trends/anomalies	Quarterly
12	Total Spend by Rental Car Company	Car	Review spending on rental cars to see impact and analyze for policy compliance	Quarterly
13	Total Car Rental Spend by City	Car	Look at volume for trends/anomalies	Quarterly
14	Total Car Rental Days	Car	Look at volume for trends/anomalies	Quarterly
15	Total Rail Spend	Rail	Look at volume for trends/anomalies	Quarterly
16	Total Spend by Rail Company (If applicable)	Rail	Review spending on rail to see impact and analyze for policy compliance	Quarterly
17	Total Rail Spend by City Pair	Rail	Look at volume for trends/anomalies	Quarterly
18	Top 100 Travelers	Other	Watch for fraudulent behavior/trends	Monthly
19	Spend by Traveler Type(s)	Other	Look at employee vs invitational traveler spend	Quarterly
20	Top 100 Exception Violators	Other	Watch for fraudulent behavior	Monthly
21	Carbon Emissions	Other	ESG compliance tracking	Quarterly
22	Customer Service Issues	Other	Report of customer service issues, status, issue type, & resolution	Monthly
23	Rental Car: Class of Car by Volume and Spend	Other	Report supporting OMB Memorandum M-24-05	Quarterly
24	Standard Call Center Metrics (Supporting Customer Service Key Performance Indicators (KPIs))	Other	Statistics of customer service and staffing levels in support of SLAs. Including but not limited to Average Speed of Answer (ASA), Average Handling Time (AHT), First Call Resolution, Abandonment Rate, Agent Utilization or Occupancy Rate, Chatbot Handoff and Fallback rate, etc.	Monthly

26.1.1 Additional Reports may be requested and defined in the ordering agency TO

26.2 Standard Reports provided to GSA's TMC PMO

26.2.1 Each Month, the Contractor shall provide the Standard Call Center Metrics (Supporting Key Performance Indicators (KPIs)) Report from Table 5 Item 24 to GSA via TMCStrategy@gsa.gov.

26.2.2 Chatbot Handoff and Fallback

26.2.2.1 Fallback rate:

26.2.2.1.1 Calculating Chatbot Fallback rate: Queries not resolved by a bot divided by total number of interactions with a bot.

26.2.2.2 Handoff Rate

26.2.2.2.1 Calculating Chatbot Handoff Rate: Queries routed to human "live" chat agents divided by the total number of interactions with a bot.

26.2.2.3 Chatbot Performance Benchmark: Less than 70% of chatbot interactions/queries handed off to live chat agents.

26.2.2.4 Handoff Performance Benchmark: Less than 70%

26.3 Regulatory Reports

26.3.1 Provide the necessary data and / or support for the following Regulatory Reports.

26.3.1.1 **First Class and Business Class Transportation Reporting**: Formerly referred to as the Premium Class Travel Report (PCTR) or Other than Coach Class Travel. The Contractor will provide the data extracts, to the ordering agency, necessary to populate the GSA Travel Reporting Tool for all first class and business class transportation used by federal employees while traveling for official business.

26.3.1.1.1 The extract will be provided in the format available from the GSA Reporting Tool.

26.3.1.1.2 The Contractor will assist with data clean up and validation, including but not limited to removing trips upgraded by the traveler at their own expense or using miles and removing "instant upgrade" (UP) fares, which are not considered first or business class seats by the government.

26.3.1.1.3 Please see Attachment 1 "*Travel User Guide Data Elements"* Tab for the data fields. You can also view the "Travel User Guide v8.pdf" page 20 and 21 "Data Entry (PCTR Travel Data)" for the data fields.

26.3.1.2 **Travel Reporting Information Profile (TRIP) Report**: Provide the travel data necessary, via the PNR to the ETS2 or ETSNext Technology MSP, to assist agencies in populating the GSA Travel Reporting Tool for all business and relocation travel used by federal employees while traveling for official business.

26.3.1.2.1 Please see Attachment 1 "*Travel User Guide Data Elements"* Tab for the data fields. You can also view the "Travel User Guide v8.pdf" pages 49-52 "TRIP Travel Data Entry" for the data fields.

26.3.1.3 **Senior Federal Travel Reporting (SFTR)**: Each agency must report information, twice a year, on senior federal officials and non-federal travelers

who fly aboard their government aircraft in the GSA Travel Reporting Tool. Each year, data for the period from October 1 to March 31 is due on April 30, and data for the period from April 1 to September 30 is due on October 31. If the agency does not have data to submit, but owns a government aircraft, it must submit a negative report.

26.3.1.3.1 The Contractor may not be able to provide information for this report, unless the Contractor facilitates acquiring charter and/or aircraft on behalf of the agency.

26.3.1.3.2 Please see Attachment 1 "*Travel User Guide Data Elements"* Tab for the data fields. You can also view the "Travel User Guide v8.pdf" pages 40-42 "SFTR Travel Data Entry" for the data fields.

26.3.1.3.3 The extract will be provided in the format available from the GSA Reporting Tool.

26.3.1.4 **Relocation Reporting**: By end of the reporting period, November 30th of each year, all agencies must report 1) obligated relocation information for the previous fiscal year and 2) Final relocation information for the Fiscal Year, two years prior.

26.3.1.4.1 The Contractor may not have information for this report, unless it supports relocation related travel, e.g., house-hunting trips, en route travel, etc., on behalf of the agency.

26.3.1.4.2 Please see Attachment 1 "*Travel User Guide Data Elements"* Tab for the data fields. You can also view the "Travel User Guide v8.pdf" pages 30-35 "Final (Fiscal Year Data Entry & Obligated (Fiscal Year) Data Entry" for the data fields.

26.3.2 Additional Data Elements may be included as part of the T&E Business Standards.

26.4 GSA Data Transfer

26.4.1 **GSA Data Capture**: The Contractor must capture the data elements for domestic and international travel (e.g. transportation, lodging and car rental, reason codes for non-use of City Pair contracts) as defined in the Schedule and in **Attachment 1 – Data Elements – FedRamp.xlsx**. This list is NOT all inclusive and other data elements may be required by GSA or the ordering agency at the TO level.

26.4.1.1 Defined Data Element Tabs in Attachment 1

26.4.1.1.1 GSA Ticket Extract

26.4.1.1.2 GSA Segment Extract

26.4.1.1.3 TMC Data Elements

26.4.1.1.4 Travel User Guide Data Elements

26.4.1.1.5 Standard Extract Specifications Guide Version 5.5, March 2015

26.4.1.1.5.1 From Tab "Overview" to TCSVCFEES

26.4.1.1.5.2 And future versions from Cornerstone and future contractors supporting GSA's government wide reporting requirements.

26.4.1.1.6 FedRamp SaaS Qualification

26.4.2 **GSA Data Transfer**: The Contractor shall provide, at a minimum, a transfer of data with all the data elements in the above referenced attachment (and any additional data elements requested).

26.4.2.1 The Contractor shall transfer the data to GSA or a designated third-party data aggregator.

26.4.2.2 The data shall be provided in an electronic commercial format readable in Microsoft Excel 365 and future releases (or other standard industry format specified by GSA).

26.4.2.3 Data transfer will be done over SFTP connection unless another method is agreed upon between the contractor and GSA or a designated third-party aggregator.

26.4.2.4 The contractor will allow the use of third-party data transfer software that is approved by GSA. If such a tool is used, this tool will ensure that data is transferred using an approved method (such as SFTP).

26.4.2.5 Data will be sent, at a minimum, monthly to GSA.

26.4.3 **GSA Reports**:

26.4.3.1 Reports submitted to GSA should be identified with: Name of Contractor, IATA number, report period and type of report (i.e. Monthly Agency/CPP Report)

26.4.3.2 The following reports shall be provided to the GSA, for additional information, see Appendix D:

26.4.4 **Lodging Report – Quarterly**:

26.4.4.1 See Section 30 APPENDIX B – LODGING REPORT for additional information.

Table 6 - Lodging Report - Monthly

Field No.	Field Name	Comments
1	Agency / Organization	Agency code
2	Hotel Chain Code	
3	Hotel Name	
4	Hotel City	
5	Hotel State	2 letter abbreviation

6	Hotel Zip Code	5 digits
7	Hotel Rate Plan or Rate Code reserved	Source: Reservation History, (E.g. FedRooms [XVU], Government [GOV], Best Available [BAR], etc.)
8	Daily Room Rate, excluding taxes and fees	
9	No Hotel Booking Reason codes (lodging)	If lodging reservations were not made with overnight air/rail reservations, the traveler must provide a justification from the list found below.
10	Reserved check-in date	
11	Reserved check-out date	
12	Booking Source	(E.g. GDS)
13	GDS Hotel ID	Could be alpha, alphanumeric, or numeric

27 EXPLANATORY CODES

This section defines the standardized, text based Explanatory Codes (ECs) (also referred to as reason codes or exception codes or non-use codes) for inclusion in the travel booking record (PNR). The purpose is to ensure the availability of booking data for itinerary review and approval, comprehensive reporting purposes, and analysis to support the travel programs managed by GSA including ETS.

All applicable ECs shall be recorded in User Definable Interface Data Storage (UDIDS) remarks (or their equivalent) of each ETS PNR, such that the **Explanatory Response** text can be readily incorporated into the body of the traveler's invoice and itinerary, and included in reports prepared by the fulfilling TMC, if requested by the ordering agency. It is acknowledged that to meet all the requirements, it may be necessary to duplicate (as remark items) some informational elements that are already present in the PNR in other forms.

Some EC reporting elements are mandated by the FTR, and are summarized in Section I, Mandatory Explanatory Codes Stipulated by the FTR below, and are mandatory in all cases. The remaining ECs addressed in Section II; Loding & Rental Car Explanatory Codes represent additional transactional information that are required by GSA. The Contractor shall implement automation and automation-assisted functionality at the Point of Sale (POS) and the Mid-Office (MID) as necessary to enable and ensure accurate capture and recording of all EC information in the PNRs whether originated via the OBT or a reservation made directly with a Travel Agent.

Some EC related information cannot be determined without assistance from the traveler or user. For such items, **Traveler Selectable** (TS) EC shall be required. Note that it may not be possible to compel travelers or users to comply with certain TS EC. Therefore, all TS EC include a default value, indicating No Response by User.

Response Codes may be two- or three-digit, alphanumeric data elements that are associated with longer formed, standardized **Explanatory Response** text. For ease of interpretation by the reader, all EC elements presented to the User (whether in text [itineraries, reports], or in the ETS application user interface), shall be presented in their long form syntax shown in the following table by the ETS vendor.

The following list of EC elements comprises the reportable ECs that the government currently requires. However, the list may be modified in the respective Task Order or within the MAS SOW. Further, EC requirements may change over the life of the contract term, as necessitated by updates or changes to the FTR or other applicable laws or regulation. In such cases, the Contractor shall accommodate the associated changes to EC without additional charge to the Government.

27.1 Mandatory Explanatory Codes Stipulated by the FTR

The FTR stipulates certain reporting requirements, including conformation to the following ECs justifying non-use of GSA Contract City Pair Airfares. Provisions must be made to accommodate reporting of itineraries traveling CPP city pair markets but not utilizing CPP contract fares. Additional ECs, if implemented, shall be mapped to the following Reason Codes for this specific reporting requirement.

EC Item	Response Code	Explanatory Response	Probable Data Source
Travel Purpose Codes			
Travel Purpose ID	P1	EMPLOYEE EMERGENCY	TAVS, POS, TS
	P2	MISSION (OPERATIONAL)	
	P3	SPECIAL MISSION	
	P4	CONFERENCE	TAVS, POS, TS
	P5	TRAINING	
	P6	RELOCATION	
Reason for Non-use of Contract City Pair Fare			

EC Item	Response Code	Explanatory Response	Probable Data Source
CPP Non-Use Reason Code	C0	CONTRACT FARE USED OR NO CONTRACT FARE EXISTS FOR CITY-PAIR MARKET.	POS, TS
CPP Non-Use Reason Code	C1	SPACE ON A SCHEDULED CONTRACT FLIGHT IS NOT AVAILABLE IN TIME TO ACCOMPLISH THE PURPOSE OF TRAVEL.	POS, TS
CPP Non-Use Reason Code	C2	USE OF CONTRACT SERVICE WOULD REQUIRE TRAVELERS TO INCUR UNNECESSARY OVERNIGHT LODGING COSTS WHICH WOULD INCREASE THE TOTAL COST OF THE TRIP.	POS, TS
CPP Non-Use Reason Code	C3	THE CONTRACT CARRIER'S FLIGHT SCHEDULE IS INCONSISTENT WITH EXPLICIT POLICIES OF INDIVIDUAL FEDERAL DEPARTMENTS AND AGENCIES WHERE APPLICABLE TO SCHEDULE TRAVEL DURING NORMAL WORKING HOURS.	POS, TS
CPP Non-Use Reason Code	C4	A NON-CONTRACT CARRIER OFFERS A LOWER FARE TO THE GENERAL PUBLIC THAT, IF USED, WILL RESULT IN A LOWER TOTAL TRIP COST TO THE GOVERNMENT (THE COMBINED COSTS OF TRANSPORTATION, LODGING, MEALS, AND RELATED EXPENSES CONSIDERED). [***NOTE:*** THIS EXCEPTION DOES NOT APPLY IF THE CONTRACT CARRIER OFFERS THE SAME OR LOWER FARE AND HAS SEATS AVAILABLE AT THAT FARE, OR IF THE FARE OFFERED BY THE NON-CONTRACT CARRIER IS RESTRICTED TO GOVERNMENT AND MILITARY TRAVELERS PERFORMING OFFICIAL BUSINESS AND MAY BE PURCHASED ONLY WITH A CONTRACTOR-ISSUED CHARGE CARD, CENTRALLY BILLED ACCOUNT (E.G., YDG, MDG, QDG, VDG, AND SIMILAR FARES) OR GTR WHERE THE TWO PREVIOUS OPTIONS ARE NOT AVAILABLE.]	POS, TS
CPP Non-Use	C5	COST EFFECTIVE RAIL SERVICE IS AVAILABLE AND IS CONSISTENT WITH MISSION REQUIREMENTS.	POS, TS

Reason Code			
Reason for Using Non-US Carrier			
Non-US Carrier Reason Code	R1	USE OF A FOREIGN AIR CARRIER IS DETERMINED TO BE A MATTER OF NECESSITY IN ACCORDANCE WITH FTR §301-10.138.	POS, TS
	R2	THE TRANSPORTATION IS PROVIDED UNDER A BILATERAL OR MULTILATERAL AIR TRANSPORTATION AGREEMENT TO WHICH THE UNITED STATES GOVERNMENT AND THE GOVERNMENT OF A FOREIGN COUNTRY ARE PARTIES, AND WHICH THE DEPARTMENT OF TRANSPORTATION HAS DETERMINED MEETS THE REQUIREMENTS OF THE FLY AMERICA ACT.	POS, TS
	R3	TRAVELER IS AN OFFICER OR EMPLOYEE OF THE DEPARTMENT OF STATE, UNITED STATES INFORMATION AGENCY, UNITED STATES INTERNATIONAL DEVELOPMENT COOPERATION AGENCY, OR THE ARMS CONTROL DISARMAMENT AGENCY, AND TRAVEL IS PAID WITH FUNDS APPROPRIATED TO ONE OF THESE AGENCIES, AND TRAVEL IS BETWEEN TWO PLACES OUTSIDE THE UNITED STATES.	POS, TS
	R4	NO U.S. FLAG AIR CARRIER PROVIDES SERVICE ON A PARTICULAR LEG OF THE ROUTE, IN WHICH CASE FOREIGN AIR CARRIER SERVICE MAY BE USED, BUT ONLY TO OR FROM THE NEAREST INTERCHANGE POINT ON A USUALLY TRAVELED ROUTE TO CONNECT WITH U.S. FLAG AIR CARRIER SERVICE.	POS, TS
	R5	A U.S. FLAG AIR CARRIER INVOLUNTARILY REROUTES TRAVEL ON A FOREIGN AIR CARRIER.	POS, TS
Non-US Carrier	R6	SERVICE ON A FOREIGN AIR CARRIER WOULD BE THREE HOURS OR LESS, AND USE OF THE U.S. FLAG AIR CARRIER WOULD AT LEAST DOUBLE EN ROUTE TRAVEL TIME.	POS, TS

EC Item	Response Code	Explanatory Response	Probable Data Source
Reason Code	R7	COSTS OF TRANSPORTATION ARE REIMBURSED IN FULL BY A THIRD PARTY, SUCH AS A FOREIGN GOVERNMENT, INTERNATIONAL AGENCY, OR OTHER ORGANIZATION.	POS, TS
	R8	INTERNATIONAL TRAVEL - USE OF U.S. FLAG AIR CARRIER (NONSTOP) SERVICE WOULD EXTEND TRAVEL TIME, INCLUDING DELAY AT ORIGIN, BY 24 HOURS OR MORE.	POS, TS
	R9	INTERNATIONAL TRAVEL - NO U.S. FLAG AIR CARRIER (NONSTOP) SERVICE AVAILABLE. U.S. FLAG AIR CARRIER SERVICE AVAILABLE ON ONE OR MORE PORTION OF THE ROUTE BUT USE OF SUCH SERVICE (ON ONE OR MORE OF THESE PORTIONS) WHEN COMPARED TO USING A FOREIGN AIR CARRIER, WOULD: (A) INCREASE THE NUMBER OF AIRCRAFT CHANGES TRAVELER MUST MAKE OUTSIDE OF THE U.S. BY 2 OR MORE; OR (B) EXTEND TRAVEL TIME BY AT LEAST 6 HOURS OR MORE; OR (A) REQUIRE A CONNECTING TIME OF 4 HOURS OR MORE AT AN OVERSEAS INTERCHANGE POINT.	POS, TS
	R10	TRAVEL IS BETWEEN TWO PLACES OUTSIDE THE UNITED STATES - U.S. FLAG AIR CARRIER PROVIDES SERVICE BETWEEN MY ORIGIN AND MY DESTINATION BUT WHEN COMPARED TO USING A FOREIGN AIR CARRIER, SUCH USE WOULD EITHER: (A) INCREASE THE NUMBER OF AIRCRAFT CHANGES TRAVELER MUST MAKE EN ROUTE BY 2 OR MORE; OR (B) EXTEND TRAVEL TIME BY 6 HOURS OR MORE; OR (C) REQUIRE A CONNECTING TIME OF 4 HOURS OR MORE AT AN OVERSEAS INTERCHANGE POINT.	POS, TS

EC Item	Response Code	Explanatory Response	Probable Data Source
For all Air itineraries: If the booking includes FIRST CLASS segment			
	F1	NO COACH-CLASS ACCOMMODATIONS ARE REASONABLY AVAILABLE (WITHIN 24 HOURS OF MY PROPOSED DEPARTURE OR ARRIVAL TIME).	POS, TS
	F2	I HAVE AN AGENCY-CERTIFIED MEDICAL DISABILITY OR OTHER SPECIAL NEED.	POS, TS
	F3	MY AGENCY HAS DETERMINED THAT EXCEPTIONAL SECURITY CIRCUMSTANCES EXIST.	POS, TS
	F4	THIS IS REQUIRED BECAUSE OF MY AGENCY MISSION, CONSISTENT WITH MY AGENCY'S INTERNAL PROCEDURES.	POS, TS
For all Air itineraries: If the booking includes BUSINESS CLASS segments			
UG Justification	B1	I HAVE AN AGENCY-CERTIFIED MEDICAL DISABILITY OR OTHER SPECIAL NEED.	POS, TS
	B2	MY AGENCY HAS DETERMINED THAT EXCEPTIONAL SECURITY CIRCUMSTANCES EXIST.	POS, TS
	B3	COACH-CLASS ACCOMMODATIONS ON AN AUTHORIZED/APPROVED FOREIGN AIR CARRIER DO NOT PROVIDE ADEQUATE SANITATION OR HEALTH STANDARDS.	POS, TS
	B4	NO COACH-CLASS ACCOMMODATIONS ARE PROVIDED FOR REGULARLY SCHEDULED FLIGHTS BETWEEN MY ORIGIN AND DESTINATION POINTS.	POS, TS
	B5	MY TRANSPORTATION COSTS ARE PAID IN FULL THROUGH AGENCY ACCEPTANCE OF PAYMENT FROM A NON-FEDERAL SOURCE.	POS, TS

EC Item	Response Code	Explanatory Response	Probable Data Source
	B6	MY ORIGIN AND/OR DESTINATION ARE/IS OCONUS AND THE SCHEDULED FLIGHT TIME (INCLUDING STOPOVERS AND CHANGE OF PLANES) EXCEEDS 14 HOURS.	POS, TS
	B7	THIS WILL RESULT IN AN OVERALL COST SAVINGS TO THE GOVERNMENT BY AVOIDING ADDITIONAL SUBSISTENCE COSTS, OVERTIME, OR LOST PRODUCTIVE TIME.	POS, TS
	B8	NO SPACE IS AVAILABLE IN COACH-CLASS ACCOMMODATIONS IN TIME TO ACCOMPLISH MY MISSION, WHICH IS URGENT AND CANNOT BE POSTPONED.	POS, TS
	B9	REQUIRED BECAUSE OF AGENCY MISSION, CONSISTENT WITH AGENCY'S INTERNAL PROCEDURES.	POS, TS
RAIL BOOKINGS RELATED **If the Rail Fare selected is "Other than Coach": Which Explanatory Code best describes the justification for "Other than Coach" upgraded train service?**			
UG Justification	T1	NO COACH-CLASS ACCOMMODATIONS ARE REASONABLY AVAILABLE (WITHIN 24 HOURS OF MY PROPOSED DEPARTURE OR ARRIVAL TIME).	POS, TS
	T2	I HAVE AN AGENCY-CERTIFIED MEDICAL DISABILITY OR OTHER SPECIAL NEED.	POS, TS
	T3	MY AGENCY HAS DETERMINED THAT EXCEPTIONAL SECURITY CIRCUMSTANCES EXIST.	POS, TS
	T4	COACH-CLASS ACCOMMODATIONS ON AN AUTHORIZED/APPROVED FOREIGN RAIL CARRIER DO NOT PROVIDE ADEQUATE SANITATION OR HEALTH STANDARDS.	POS, TS

EC Item	Response Code	Explanatory Response	Probable Data Source
	T5	THIS IS REQUIRED BECAUSE OF MY AGENCY MISSION, CONSISTENT WITH MY AGENCY'S INTERNAL PROCEDURES.	POS, TS
If booking is for an "Extra Fare Train" (Acela): Which Explanatory Code best describes the justification for "Extra Fare" upgraded train service?			
UG Justification	T6	MY AGENCY HAS DETERMINED THAT THIS IS ADVANTAGEOUS TO THE GOVERNMENT.	POS, TS
	T7	MY AGENCY HAS DETERMINED THAT EXCEPTIONAL SECURITY CIRCUMSTANCES EXIST.	POS, TS
SHIP BOOKINGS RELATED: If the Booking Class is "Other than Lowest First Class": Which Code best describes the justification for "Other than lowest First Class" upgraded ship service?			
UG Justification	S1	LOWEST FIRST-CLASS ACCOMMODATIONS ARE NOT AVAILABLE.	POS, TS
	S2	I HAVE AN AGENCY-CERTIFIED MEDICAL DISABILITY OR OTHER SPECIAL NEED.	POS, TS
	S3	MY AGENCY HAS DETERMINED THAT EXCEPTIONAL SECURITY CIRCUMSTANCES EXIST.	POS, TS
	S4	THIS IS REQUIRED BECAUSE OF MY AGENCY MISSION, CONSISTENT WITH MY AGENCY'S INTERNAL PROCEDURES.	POS, TS

27.2 Additional Explanatory Codes

To enable the government and the agencies to control and manage its travel spend, and achieve their desired threshold of performance, the Contractor shall support the capture of these additional Explanatory Codes to facilitate more informed travel authorization, transactional analysis, and improved travel program management more effectively.

EC Item	Response Code	Explanatory Response	Probable Data Source
CAR BOOKINGS RELATED If no Car booking is present upon record closing…			
No Car	CC0	PLEASE SELECT (Default, recorded as No Response)	POS, TS
	CC1	NO CAR BOOKING - CAR NOT REQUIRED.	POS, TS
	CC2	NO CAR BOOKING - SOLD OUT.	POS, TS
	CC3	CAR BOOKED DIRECTLY OR VIA OTHER MEANS.	POS, TS
For all Car bookings…			
	Car Vendor Selection		
Car VS	CV1	BOOKED PREF CAR VENDOR AND TYPE.	MID
	CV2	ALT. CAR BOOKED, NON-PREF VENDOR OR TYPE.	MID
	Car Rate/Type Selection		
Car R/TS	CR0	PLEASE SELECT (Default, recorded as No Response).	POS, TS
	CR1	LOWEST RATE FOR AUTHORIZED CAR TYPE.	POS, TS
	CR2	LOWER RATE BOOKED W NON-PREF VENDOR.	POS, TS
	CR3	HIGHER RATE BOOKED - DECLINED PREF CAR TYPE.	POS, TS
	CR4	HIGHER RATE BOOKED - LC CAR TYPE SOLD OUT.	POS, TS
	CR5	HIGHER RATE BOOKED - PREF VENDOR SOLD OUT.	POS, TS

EC Item	Response Code	Explanatory Response	Probable Data Source
	CR6	HIGHER RATE BOOKED - MULTI-TRAVELERS USING ONE CAR.	POS, TS
	CR7	HIGHER RATE BOOKED - TRAVELING WITH EQUIPMENT.	POS, TS
	CR8	HIGHER RATE BOOKED - TRAVELING IN POOR WEATHER.	POS, TS
	CR9	HIGHER RATE BOOKED - PREF VENDOR LOCATION INCONVENIENT.	POS, TS
	CR10	NO PREFERRED VENDOR IN LOCATION.	POS, TS
HOTEL BOOKINGS RELATED If no Hotel booking is present upon record closing…			
No Hotel	HC0	PLEASE SELECT (Default, recorded as No Response)	POS, TS
	HC1	NO HOTEL BOOKING - HOTEL NOT REQUIRED.	POS, TS
	HC2	HOTEL BOOKED DIRECTLY OR VIA OTHER MEANS.	POS, TS
For all Hotel bookings…			
	Hotel Vendor Selection		
FedRooms Usage	HVF	BOOKED FEDROOMS PROPERTY / XVU RATE CODE.	POS, MID
	HVN	BOOKED NON-FEDROOMS PROPERTY.	POS, MID
If FedRooms is not utilized…			

EC Item		Response Code	Explanatory Response	Probable Data Source
	Hotel VS	HV0	PLEASE SELECT (Default, recorded as No Response)	POS, TS
		HV1	NO FEDROOMS FACILITIES WITHIN A REASONABLE PROXIMITY OF TDY.	POS, TS
		HV2	FEDROOMS PROPERTIES SOLD OUT.	POS, TS
		HV3	BOOKED AGENCY NEGOTIATED CONTRACT.	POS, TS
		HV4	BOOKED AGENCY AUTHORIZED ALTERNATIVE.	POS, TS
		HV5	MEETING/CONFERENCE REQUIREMENT.	POS, TS
		HV6	TRAVEL IS OCONUS.	POS, TS
		Rate / Room Type Selection		
	Hotel R/TS	HR0	PLEASE SELECT (Default, recorded as No Response)	POS, TS
		HR1	LOWEST RATE FOR AUTHORIZED ROOM TYPE.	POS, TS
		HR2	LOWER RATE BOOKED W NON-PREF VENDOR.	POS, TS
		HR3	HIGHER RATE BOOKED - ROOM SHARING.	POS, TS
		HR4	HIGHER RATE BOOKED - LC ROOM TYPE SOLD OUT.	POS, TS
		HR5	HIGHER RATE BOOKED - NO PROPS AVAIL W/I PER DIEM.	POS, TS
		HR6	HIGHER RATE BOOKED - DECLINED PREF ROOM TYPE.	POS, MID

EC Item	Response Code	Explanatory Response	Probable Data Source
	HR7	HIGHER RATE BOOKED - DECLINED LOWER COST ALTERNATIVES.	POS, MID

Probable Sources of EC Data include:

TAVS = Travel Authorization and Vouchering System

POS = Point-Of-Sale (including, OBT and booking scripts used by the TMC)

MID = Mid-Office / Quality Control (QC) Solution

TS = Selected by Traveler/User from list of available Explanatory Codes offered at the POS

Agent = travel agency staff person.

28 STANDARD SERVICES TO BE PRICED FOR ETSNEXT, DOD, AND OTHER USERS OF 561510

Please see the required Price Proposal Template (PPT) for the Contract Line Item Number (CLIN) assigned to each service.

28.1 TICKETING AND FULFILLMENT

Table 7 - Ticketing & Fulfillment Services

SIN	Description of Service	Unit Per	Type	Domestic or International	Full Service or Self Service
CONUS & U.S. Based Territory TMCs					
561510	Self Service	Transaction	Transaction A	Both	Self Service
561510	Self Service	Transaction	Transaction B	Both	Self-Service
561510	Full-Service Air/Rail, Domestic Travel	Transaction	Transaction A	Domestic	Full Service

SIN	Description of Service	Unit Per	Type	Domestic or International	Full Service or Self Service
561510	Full-Service Air/Rail, International Travel	Transaction	Transaction A	International	Full Service
561510	Full-Service Hotel/Car Only	Transaction	Transaction B	Both	Full Service
OCONUS Based TMC Locations (Can be a single rate and negotiated at the task order for each country requested by the Task Ordering Agency.)					
561510	Self Service	Transaction	Transaction A	Both	Self Service
561510	Self Service	Transaction	Transaction B	Both	Self Service
561510	Full-Service Air/Rail, Domestic Travel	Transaction	Transaction A	Domestic	Full Service
561510	Full-Service Air/Rail, International Travel	Transaction	Transaction A	International	Full Service
561510	Full-Service Hotel/Car Only Domestic Travel	Transaction	Transaction B	Both	Full Service
Managed Service Fee					
561510	Managed Service Fee	Per Year			
561510	Managed Service Fee	Per Quarter			
561510	Managed Service Fee	Per Month			

28.2 ONSITE TMC SERVICES

Table 8 - Onsite TMC Services

SIN	Description of Service	Unit of Issue
Per Year – 2080 Hours		
Ancillary	On-site Administrative Support e.g., Lead Agent/Agent Manager	Per Year
Ancillary	On-site Agent Support (including support for reservations)	Per Year
Ancillary	On-site Administrative Support e.g., Lead Agent/Agent Manager	Per Hour
Ancillary	On-site Agent Support (including support for reservations)	Per Hour
Part Time Support		
Ancillary	On-site Administrative Support e.g., Lead Agent/Agent Manager	Per Hour
Ancillary	On-site Agent Support (including support for reservations)	Per Hour
Part Time Support - Overtime		
Ancillary	On-site Administrative Support e.g., Lead Agent/Agent Manager	Per Hour
Ancillary	On-site Agent Support (including support for reservations)	Per Hour
Additional Onsite Support Related Services		
Ancillary	**GDS**: GDS connectivity and computer equipment including printers	Per terminal
Ancillary	**GDS Software and License**: This includes GDS software and GDS license / login access	Per month

28.3 OPTIONAL (ANCILLARY) SERVICES TO BE PRICED

Table 9 - Optional (Ancillary) Services

SIN	Description of Service	Unit of Issue
Ancillary	**Very Important Person (VIP) (Remote or Hybrid)**: Enhanced reservations support for designated VIP Personnel. (e.g., dedicated toll-free number, originate and/or change arrangements or reservations (air/rail, lodging, car rental), and ticketing, for one or multiple locations, special seat confirmation/accommodation services, Loyalty Program support (air/rail, lodging, car rental), monitor travel and provide notification of disruption, etc.).	Per Itinerary
Ancillary	**International Rate Desk Services**: May be applicable when no GSA City Pair Program (CPP) is available for international destinations, which may not be auto price within the GDS. Includes capability for faring complex international itineraries using a comprehensive set of faring methods, exceptions and interpretations of airline policies, Department of Transportation (DOT) regulations, International Air Transport Association (IATA) policies, etc. to optimize best pricing for international travel. Does not apply for CPP or combinations thereof or simple round trip commercial itineraries.	Per Itinerary
Ancillary	**Security-cleared Personnel**: Obtaining cleared agents who can meet or already have the appropriate security clearances as requested by the agency task order.	Per Employee
Ancillary	**Passport and/ or Visa Processing & Support**: Provide advice on Visa, Passport, and other travel document requirements to travelers. Refer to a Third-Party supplier for Visa & Passport processing, as available.	Per Passport and/or Visa Request
Ancillary	**Travel Arrangements for services not available in the GDS or other content sources**: These may include but are not limited to: Charter Bus, Alaska Marine Highway System, Boat / Ship including cruise ships and ferries, bush pilots in Alaska and other remote locations, snowmobile, dog sled, horses, etc. This service may include direct billing by the TMC, when credit cards cannot be used, and passed through “at cost” to the agency for the services acquired.	Per Itinerary
Ancillary	**Travel Arrangements for services not available in the GDS or other content sources**: These may include but are not limited to: Charter Bus, Alaska Marine Highway System, Boat / Ship including cruise ships and ferries, bush pilots in Alaska and other remote locations, snowmobile, dog sled, horses, etc. This service may include direct billing by the TMC, when credit cards cannot be used, and passed through “at cost” to the agency for the services acquired.	Per Hour

SIN	Description of Service	Unit of Issue
Ancillary	**Non GDS Air/Rail Surcharge**: Surcharge for processing air/rail transactions not available in the GDS	Per Transaction
Ancillary	**NDC Air Surcharge**: Surcharge for processing air transactions through an NDC channel not in the GDS	Per Transaction
Ancillary	**Virtual Card Payment Support**: Service to support a virtual card payment through GSA SmartPay program for hotels or other suppliers as available	Per Card provisioned
Ancillary	**Centrally Billed Account (CBA) Reconciliation**: Monthly reconciliation of charges to an agency provided CBA for air and other services. Reconciliation should be submitted to the agency no later than the fifth (5th) day after receipt of the billing file from the GSA SmartPay® bank.	Per CBA
Ancillary	**Leave in Conjunction with Official Travel (LICWO) / Leisure Travel**: Travel services to an individual on TDY, family members, or others accompanying that individual, when requested by the traveler. **Travelers are responsible for any costs that exceed the official portion of the trip.** The Contractor shall not invoice the Government for any leisure only reservations or services. The transaction fee for LICWO services shall be charged directly to the traveler. The Contractor shall separate costs for official travel from leisure travel costs.	Per Transaction
Ancillary	**Cost-Constructed Travel:** Travel services to an individual on TDY, family members, or others accompanying that individual, when requested by the traveler. Travel based on a cost comparison between the cost of official (i.e., direct) travel and the cost of personal (i.e., indirect) travel. When cost constructing travel, the traveler can only claim the cost of the fare(s) the U.S. Government would have paid to the contract and/or common carrier or the cost of the commercial fare(s) the traveler actually paid to common carriers, whichever is less. Travelers are responsible for any costs that exceed the official portion of the trip. As defined in Section 11.20, the fee is charged for all cost-constructed itineraries that are completed that require more than one cost-constructed itinerary (quote) **but no more than a total of three itineraries (quotes)**. It is	Per Transaction

SIN	Description of Service	Unit of Issue
	charged per itinerary (not per person) so, for example, a family of five with the same itinerary would be charged one fee. The Contractor shall not invoice the Government for any Cost-Constructed reservations or services in conjunction with Leisure or Leave in Conjunction with Official (LICWO) Travel. The transaction fee for Cost-Constructed services shall be charged directly to the traveler in conjunction with Leisure or Leave in Conjunction with Official (LICWO) Travel.	
Ancillary	**Rate Reshopping:** Costs associated with using a rate Reshopping Service, which may be a third party. This includes the fee paid to the third-party rate Reshopping service.	Per PNR
Ancillary	**Custom Reports / Ad Hoc Reports:** Set up, development, and programming of custom and/or Ad Hoc reports, not included as part of the standard reporting capabilities. This does not include reporting ad hoc report creation capabilities available as part of the reporting solution (if available).	Per Hour
Ancillary	**Custom Reports / Ad Hoc Reports:** Set up, development, and programming of custom and/or Ad Hoc reports, not included as part of the standard reporting capabilities. This does not include reporting ad hoc report creation capabilities available as part of the reporting solution (if available).	Per Report

28.4 CYBERSECURITY - ADDITIONAL REQUIREMENTS FOR ETSNEXT- ORDERED AT THE TASK ORDER LEVEL

Table 10 - Cybersecurity - Additional Requirements for ETSNext Technology MSP

CYBERSECURITY - ADDITIONAL REQUIREMENTS FOR ETSNEXT- ORDERED AT THE TASK ORDER LEVEL		
Ancillary	**Contractor (TMC) Non-Federal System with CUI (800-171) - MFR including Leveraged FedRamp for Software as a Service (SaaS):** Accounts for any additional cost associated with leveraging an **existing FedRamp ATO for any cloud-based solutions** (Infrastructure as a Service (IaaS) and Software as a Service (SaaS) or Platform as a Service (PaaS) that is offered as part of the TMCs overall offering. e.g., if a TMC offers a cloud-based reporting solution, as part of its total offerings, any additional costs for the agency to utilize the SaaS in coordination with the FedRamp office.	Per FedRamp environment for cloud-based solution(s)

	Contractor (TMC) Non-Federal System with CUI (800-171) - MFR including Leveraged FedRamp for Software as a Service (SaaS): Accounts for any additional cost associated with leveraging an **existing FedRamp ATO for any cloud-based solutions** (Infrastructure as a Service (IaaS) and Software as a Service (SaaS) or Platform as a Service (PaaS) that is offered as part of the TMCs overall offering. e.g., if a TMC offers a cloud-based reporting solution, as part of its total offerings, any additional costs for the agency to utilize the SaaS in coordination with the FedRamp office.	Hourly Labor Rate **(Inclusive of additional Software and Technology to support the additional requirements)**
Ancillary	**Contractor (TMC) Non-Federal System with CUI (800-171) - MFR including Leveraged FedRamp for Software as a Service (SaaS):** Accounts for any additional cost associated with **assisting a third-party cloud-based offering in acquiring a FedRamp ATO**.	Per FedRamp environment for cloud-based solution(s)
	Contractor (TMC) Non-Federal System with CUI (800-171) - MFR including Leveraged FedRamp for Software as a Service (SaaS): Accounts for any additional cost associated with **assisting a third-party cloud-based offering in acquiring a FedRamp ATO**.	Hourly Labor Rate **(Inclusive of additional Software and Technology to support the additional requirements)**
Ancillary	**Enhanced 800-171 Requirements:** The costs, over and above the 800-171 MFR approach included in the transaction costs, associated with enhanced 800-171 requirements including, Assessment & Authorization (A&A), having an ATO or ATU issued by an ordering agency, in place of the GSA MFR for NIST SP 800-171 and/or require monthly submission of continuous monitoring deliverables and annual security assessments for one-third (1/3) of the required security controls plus a full security assessment of all required controls every 3 years.	Per A&A & ATO
	Enhanced 800-171 Requirements: The costs, over and above the 800-171 MFR approach included in the transaction costs, associated with enhanced 800-171 requirements including, Assessment & Authorization (A&A), having an ATO or ATU issued by an ordering agency, in place of the GSA MFR for NIST SP 800-171 and/or require monthly submission of continuous monitoring deliverables and annual security assessments for one-third (1/3) of the required security controls plus a full security assessment of all required controls every 3 years.	Hourly Labor Rate **(Inclusive of additional Software and Technology to support the additional requirements)**
Ancillary	**Contractor (TMC) Traditional Assessment & Authorization in Agreement with NIST 800-37 Rev 2 and NIST 800-53 Rev.5 Security and Privacy Controls for Information Systems and**	Per A&A & ATO

	Organizations at the FIPS 199 Moderate Impact Level 1: The Contractor shall support ordering agency requirements for Assessment and Authorization following their Agency' specific security assessment and authorization policies and procedures aligned to NIST 800-37 Rev 2. The additional work necessary to complete the System Security and Privacy Plan (SSPP), other documentation, and monthly continuous monitoring, which is over and above the 800-171 MFR approach included in the transaction costs.	
	Contractor (TMC) Traditional Assessment & Authorization in Agreement with NIST 800-37 Rev 2 and NIST 800-53 Rev.5 Security and Privacy Controls for Information Systems and Organizations at the FIPS 199 Moderate Impact Level 1: The Contractor shall support ordering agency requirements for Assessment and Authorization following their Agency' specific security assessment and authorization policies and procedures aligned to NIST 800-37 Rev 2. The additional work necessary to complete the System Security and Privacy Plan (SSPP), other documentation, and monthly continuous monitoring, which is over and above the 800-171 MFR approach included in the transaction costs.	Hourly Labor Rate **(Inclusive of additional Software and Technology to support the additional requirements)**
Ancillary	**Contractor (TMC)FedRamp ATO for fully cloud-based solution(s):** The costs for a fully cloud-based solution(s) offering from the TMC. Contractor (TMC) solutions delivered as-a-service in the cloud, meeting NIST 800-145 cloud definition, consistent with the OMB FedRAMP Policy memo, are subject to FedRAMP cloud information security and privacy requirements and shall be FedRamp authorized	Per FedRamp environment for cloud-based solution(s)

28.5 Account Management

Table 11 - Account Management

SIN	**Description of Service**	**Unit of Issue**
Full Time 2,080 Hours		
Price Per Year		
Ancillary	Account Manager	Per Year
Price Per Hour		

SIN	Description of Service	Unit of Issue
Ancillary	Account Manager	Per Hour
Part Time Support		
Price Per Hour		
Ancillary	Account Manager	Per Hour
Overtime		
Price Per Hour		
Ancillary	Account Manager	Per Hour

28.6 Non-IFF Services

Table 12 - Non-IFF Services

SIN	Description of Service	Unit of Issue
Ancillary	**Debit Memo**: Charge to the agency for a traveler caused debit memo, as defined in Section 8: Definitions. The Debit Memo is passed through at cost and there is no reimbursement to the TMC for submitting the Debit Memo to the agency/customer	Per Debit Memo

29 APPENDIX A: SCHEDULE & TASK ORDER INFORMATION

29.1 INDUSTRIAL FUNDING FEE (IFF) AND SALES REPORTING

The IFF reimburses GSA for the costs of running the Multiple Award Schedule (MAS) program. The IFF is paid by the authorized ordering activity (agency, traveler, etc.) but is collected and remitted to GSA by the contractor.

Please note that the Industrial Funding Fee is $3.10 for each instance involving an airline/rail transaction (i.e., **Transaction A**).

All other products & services, including the **Transaction B,** unless otherwise specified in writing by the GSA Schedule Contracting Officer, shall be responsible for remitting at 0.75% (.0075) of sales. Debit Memos are excluded from the IFF in accordance with the Price Proposal Template.

All MAS sales are reported through the **Federal Acquisition Service (FAS) Sales Reporting Portal (SRP)**, which is available at the **Vendor Support Center** at http://srp.fas.gsa.gov. The FAS SRP is a safe, secure website to report both transactional and aggregate-level sales and payment data required by FAS procurement programs, including MAS, non-MAS programs such as the Governmentwide Acquisition Contracts (GWACs), and others.

For information on how to get started, check out the FAS Sales Reporting Video Tutorials, the FAS SRP QuickStart Guide, and Frequently Asked Questions. You need multi-factor authentication to access the system.

The Contractor must report the number of Transaction A Air/Rail with Lodging and/or Rental Car transactions quarterly via the Vendor Support Center at http://srp.fas.gsa.gov. If there are no transactions for the report period, the Contractor must still report zero transactions.

Sales and IFF reports are due quarterly in accordance with the following schedule:

Report Period	Due Date
January 1 and March 31	April 30
April 1 and June 30	July 30
July 1 and September 30	October 30
October 1 and December 31	January 31

29.2 Sales and IFF Reporting Submission Instructions

The information shall be provided in an electronic commercial format readable in Microsoft Excel.

The report shall be:

- Uploaded into the Sales Reporting Portal (SRP) https://srp.fas.gsa.gov/ as an attachment to the contractor's quarterly IFF and sales reporting., AND E-mailed to the TMC PMO at tmcstrategy@gsa.gov,
- The Email Subject Line must read: Quarterly Sales Report by Agency

- The Email content must include:
    - GSA Contract Number
    - Company's Name
    - Special Item Number (SIN)
    - Agency Task Order Number (if applicable)

29.3 TASK ORDERS

An informational copy of all Task Order (TO) negotiated Service Level Agreements (SLAs) shall be provided to the TMC PMO at tmcstrategy@gsa.gov, with the subject line: SLAs for task order XXX, contractor name and contract number, within five (5) business days of execution.

The Contractor shall provide a copy of all awarded agency TOs and all modifications to GSA. After receipt of an awarded TO, the Contractor shall provide one complete electronic copy of the TO and its technical and price proposal and all later modifications thereto, to the TMC PMO within 10 calendar days after execution. Copies should be emailed to tmcstrategy@gsa.gov.

30 APPENDIX B – LODGING REPORT

30.1 Lodging Report Monthly for the Fiscal Year

The Contractor shall provide a list of hotel data elements, see Section 26.3.4, for all Government traveler hotel bookings per each individual passenger name record (PNR) The data shall be provided in an electronic commercial format readable in Microsoft Excel 365 and future updates and emailed to 1) onthego@gsa.gov and 2) lodging@gsa.gov.

The data for each month, of the Fiscal Year, October 1 through September 30, shall be submitted such that the data for each month is added to the previous month's data, on the same tab. This will result in a "Running Total" for the Fiscal Year with the entire Fiscal Year's Data being available at the end of the Fiscal Year.

The subject of the email must state "LODGING REPORT, the reporting period and the contractor's name and contract number." This helps GSA identify your company for determination of your compliance. Data shall be sent by the 15th calendar day (or the next business day if the due date is on a weekend or Federal holiday) beginning with the end of the first month after contract award, for new TOs, and the end of the first month, after Refresh #21, for existing TOs. Negative reports are required.

The data must include all Government traveler hotel bookings under FedRooms® rate code and all bookings at non-FedRooms® rates (e.g. GOV, MIL, and TMC specific). FedRooms® uses the secure rate access code of "XVU" for all rooms booked exclusively under the Government- wide lodging program. This data shall cover all FedRooms® and non-FedRooms® bookings within the Continental United States (CONUS), Non-Continental US and Overseas Non-Foreign areas, and Non-US Overseas locations (OCONUS). All GSA reporting is at no additional cost to the Government.

31 APPENDIX C: GSA PROGRAMS & GOVERNMENT TRAVEL PROGRAMS

The following section provides additional information on GSA's and other government travel programs that a TMC may be requested to support at the TO level.

31.1 LONG TERM LODGING

The **Long-Term Lodging (LTL)** contract solution is designed for lodging needs of 30 nights or more. Properties include apartments and condominiums that are furnished with the amenities and comforts of home. For additional information, please visit https://www.gsa.gov/longtermlodging.

LTL Property-Specific Solution	**LTL Vendor-Aided Solution**
Best pricing and most flexible terms. Available in select U.S. markets.	Greater U.S. market coverage with pre-negotiated ceiling rates.
How it works: You and your Contracting Officer select from a list of 350+ properties, then request bids from each of the vendors in that market and select the best option.	How it works: You and your Contracting Officer collect bids from three vetted LTL vendors via GSA eLibrary and select the best option.
Pros: • No cancellation fees. • Deepest discounts.	Pros: • More availability in the U.S. than the Self Property Specific Solution.
Cons: • Only available in select U.S. markets.	Cons: • Higher ceiling rates. • More restrictive cancellation terms.
Who you work with: Your agency's Contracting Officer.	Who you work with: Your agency's Contracting Officer.
View the steps involved for procurement.	View the steps involved for procurement.

31.2 EMERGENCY LODGING SERVICES

GSA's **Emergency Lodging Services (ELS)** program quickly secures lodging accommodations and support services for federal agencies, state/local governments, first responders, and displaced evacuees to a declared disaster or emergency. ELS may be used by a federal or state government agency that requests to become an authorized user of the Blanket Purchase Agreement (BPA). ELS may be utilized for both unplanned and planned emergency related events including emergency preparedness or response. For additional information, please visit https://www.gsa.gov/els.

32 RIDESHARE

The GSA Rideshare Program provides rideshare/ride-hail services to federal travelers in the top 50 US markets, while utilizing a fully commercial capability. Travelers can book their rides using on-demand and concierge services in the Uber and Lyft apps/websites for their TDY and local travel needs. Enrollment is easy; agencies work directly with the vendors to set-up accounts, deploy the apps, and launch services for their travelers.

For additional information, please visit https://www.gsa.gov/travel/travel-and-lodging-services/rideshare.

32.1 RELOCATION & PERMANENT CHANGE OF STATION (PCS)

The **Employee Relocation Resource Center (ERRC)** provides agencies access to Permanent Change of Station (PCS) relocation assistance services. The relocation support services assist agencies to give their employees a smooth transition to new work locations. ERRC helps agencies establish procurement strategies and implement the most effective and cost-efficient programs that respond to their individual cultures and philosophies.

The relocation procurement solutions provide end-to-end relocation services. Programs include:

GSA's Centralized Household Goods Traffic Management Program (CHAMP) features agency customization and no lead time for household goods moving services procurement. It offers worldwide relocation services, a consistent pricing structure, highly competitive rates, comprehensive tender of service, vetted suppliers, and a customer satisfaction index built into the program.

Multiple Awards Schedule (MAS) contract's SIN 531 Employee Relocation Solution Requirements includes services relating to employee relocation, such as home sale assistance, property management, entitlement counseling, expense management and household goods move management. The requirements incorporate proven best practices that can be customized to meet agency's mission requirements.

Multiple Awards Schedule (MAS) contract's SIN 541511T Employee Relocation Management Software Requirements include relocation software and automation/technology tools that help agencies track, manage and report on their relocation programs. It includes authorization, planning, repatriation, expense management, tax gross ups, expense entry, communications, and integrations with financial systems.

For additional information, please visit https://www.gsa.gov/travel/agency-services/employee-relocation.

33 APPENDIX D - SECURITY GUIDANCE

The following appendix supplies information about the Federal Laws, Regulations, Standards, and Guidance that may apply to the TMC, based upon the type of Information System designation that an agency decides applies to the TMC. The most likely designation is a Nonfederal system with Controlled Unclassified Information (CUI), but it is up to each agency to do its due diligence and make the appropriate determination.

Ordering Agencies decide the applicability of the Federal Information Security Modernization Act (FISMA) requirements to their procurement at the task order level. In addition, ordering agencies shall conduct their due diligence security activities by coordinating with their chosen/applicable TMC to complete and authorize the TMCs prior to issuing any work by the awarded TMC.

This guidance is based upon the *GSA SECURITY AND PRIVACY REQUIREMENTS FOR IT ACQUISITION EFFORTS CIO-IT SECURITY-09-48*. Please see each individual agency's Information System Security Office for the proper guidance.

34 INTRODUCTION

The Federal Information Security Modernization Act of 2014 (FISMA of 2014) describes Federal agency security and privacy responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency." This includes services which are either fully or partially provided; including other agency hosted, outsourced, and cloud computing solutions. Agency information security programs apply to all organizations (sources) which possess or use Federal information – or which operate, use, or have access to Federal information systems (whether automated or manual) – on behalf of a federal agency, information systems used or operated by an agency or other organization on behalf of an agency. Deliverables that contain CUI must be marked, handled, and transmitted as described in the Additional Stipulations sections of this guide.

34.1 Scope

This guide provides security and privacy requirements for the information system types outlined below:

- **External Information Systems**. External information systems reside in contractor facilities and typically do not connect to an agency's network. External information systems may be government owned, and contractor operated, or contractor owned and operated on behalf of an agency or the Federal Government.
- **Cloud Information Systems**. Includes Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or SaaS. The service offering must be FedRAMP authorized, in-process, or ready.
- **Mobile Application**. A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer.
- **Nonfederal Systems and Organizations**. A system or organization: (1) when Controlled Unclassified Information (CUI) is resident in a nonfederal system and organization; (2) not collecting or maintaining information on behalf of a federal agency or using or operating a

system on behalf of an agency[1]; and (3) where there are no specific safeguarding requirements for protecting the confidentiality of CUI prescribed by the authorizing law, regulation, or governmentwide policy for the CUI category listed in the CUI Registry.

34.2 Purpose

The purpose of this document is to define and establish consistent security and privacy requirements for IT acquisition contracts involving externally hosted information systems that do not connect to the network; cloud information systems; mobile applications; and nonfederal systems with CUI. The security and privacy requirements are appropriately formatted to allow the respective security and privacy contract language to be placed in-line within a statement of work for each system type. The security and privacy requirements identified in this guide will ensure compliance with the appropriate provisions of FISMA of 2014, OMB Circular A-130, and NIST Special Publication (SP) 800-53, Revision 5.

35 EXTERNAL INFORMATION SYSTEMS – IT SECURITY AND PRIVACY REQUIREMENTS

35.1 Required Policies and Regulations

Federal Laws, Regulations, and Guidance:

The contractor shall comply with all applicable Federal Laws and Regulations.

- 40 U.S.C. 11331, "Responsibilities for Federal Information Systems Standards"
- Cybersecurity & Infrastructure Security Agency (CISA) Cybersecurity Directives - Listing of Emergency and Binding Operational Directives
- Executive Order (EO) 13556, "Controlled Unclassified Information."
- FISMA of 2014, "The Federal Information Security Modernization Act of 2014"
- HSPD 12, "Homeland Security Presidential Directive 12 – Policy for a Common
- Identification Standard for Federal Employees and Contractors"
- OMB Circular A-130, "Managing Information as a Strategic Resource."
- OMB M-10-23, "Guidance for Agency Use of Third-Party Websites and Applications"
- OMB M-14-03, "Enhancing the Security of Federal Information and Information Systems."
- OMB M-15-13, "Policy to Require Secure Connections across Federal Websites and Web Services."
- OMB M-17-12, "Preparing for and Responding to a Breach of Personally Identifiable Information."
- OMB M-21-07, "Completing the Transition to Internet Protocol Version 6 (IPv6)" Privacy Act of 1974, "5 USC, § 552a."
- National Archives and Records Administration (NARA) Controlled Unclassified Information (CUI) Registry
- OMB Memoranda, location of current fiscal year guidance on Federal Information Security and Privacy Management Requirements, including FISMA reporting.

Federal Standards and Guidance:

The contractor shall comply with all applicable Federal Information Processing Standards (FIPS). NIST Special Publications (800 Series) are guidance, unless required by a FIPS publication, in which case usage is mandatory.

- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"

- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems"
- FIPS PUB 140-3[2], "Security Requirements for Cryptographic Modules"
- NIST SP 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems."
- NIST SP 800-30, Revision 1, "Guide for Conducting Risk Assessments."
- NIST SP 800-34, Revision 1, "Contingency Planning Guide for Federal Information Systems"
- NIST SP 800-37, Revision 2, "Risk Management Framework for Information Systems and
- Organizations: A System Life Cycle Approach for Security and Privacy"
- NIST SP 800-47, Revision 1, "Managing the Security of Information Exchanges."
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations"
- NIST SP 800-53A, Revision 5, "Assessing Security and Privacy Controls in Information Systems and Organizations."
- NIST SP 800-63-3, "Digital Identity Guidelines"
- NIST SP 800-81-2, "Secure Domain Name System (DNS) Deployment Guide"
- NIST SP 800-122, "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
- NIST SP 800-137, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations"
- NIST SP 800-161, Revision 1, "Supply Chain Risk Management Practices for Federal Information Systems and Organizations"
- NIST SP 800-218, "Secure Software Development Framework (SSDF) Version 1.1: Recommendations for Mitigating the Risk of Software Vulnerabilities."

35.2 Security Compliance Requirements

FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems," is a mandatory federal standard that defines the minimum-security requirements for federal information and information systems in seventeen security-related areas. Information systems supporting the federal government must meet the minimum security and privacy requirements through the use of security controls in accordance with NIST Special Publication 800-53, Revision 5 (hereafter described as NIST 800-53), "Security and Privacy Controls for Information Systems and Organizations."

To comply with the Federal standard, an agency must determine the security category of the information and information system in accordance with FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems," and then the contractor shall apply the appropriately tailored set of Low, Moderate, or High impact baseline security controls in NIST 800-53, as determined by the agency. NIST 800-53 controls requiring organization-defined parameters (i.e., password settings) shall be consistent with agency specifications.

The Contractor shall use Agency technical guidelines, NIST guidelines, Center for Internet Security (CIS) guidelines (Level 1), or industry best practice guidelines in hardening their systems.

35.3 Essential Security Controls

All NIST 800-53 controls must be implemented as per the applicable FIPS PUB 199 Low (L), Moderate (M), or High (H) baseline. Controls in the Privacy baseline are applicable if PII data is being collected, stored, or transmitted. The Contractor shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code) or use in production.

Note: Privacy controls are not associated with a FIPS PUB 199 baseline. Controls are applicable if PII data is being collected, stored, or transmitted.

35.4 Assessment and Authorization (A&A) Activities

The implementation of a new Federal Government IT system requires a formal approval process known as Assessment and Authorization (A&A). NIST Special Publication 800-37, Revision 2 (hereafter described as NIST 800-37) and GSA IT Security Procedural Guide 06-30: Managing Enterprise Cybersecurity Risk, provides guidelines for performing the A&A process. The Contractor system/application must have a valid assessment and authorization, known as an Authorization to Operate (ATO) (signed by the Federal government) before going into operation and processing federal information. The failure to obtain and maintain a valid ATO will result in the termination of the contract. The system must have a new A&A conducted (signed by the Federal government) when significant changes are made to the system.

35.4.1 Assessing the System

The Contractor shall comply with Assessment and Authorization (A&A) requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's NIST Federal Information Processing Standard (FIPS) Publication 199 categorization. Documents that contain CUI must be marked, handled, and transmitted as described in Additional Stipulations. The contractor shall create, maintain, and update the following A&A documentation:

- System Security and Privacy Plan (SSPP) completed in agreement with NIST Special Publication 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems". The SSPP shall include as appendices required policies and procedures across 19 control families mandated per FIPS PUB 200, Rules of Behavior, and Interconnection Security Agreements (in agreement with NIST Special Publication 800-47, "Managing the Security of Information Exchanges").
    - Note: A description of how the system will transition to IPv6, as required by OMB M-21-07, must be included as part of the system's SSPP.
- Contingency Plan completed in agreement with NIST Special Publication 800-34.
- Business Impact Assessment completed in agreement with NIST Special Publication 800-34.
- Contingency Plan Test Report.
- Incident Response Plan completed in agreement with NIST Special Publication 800-61, "Computer Security Incident Handling Guide".

- Incident Response Test Report completed in agreement with NIST Special Publication 800-61, “Computer Security Incident Handling Guide”.
- Configuration Management Plan.
- Plan of Action & Milestones (POA&M).
- Penetration Test Reports documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. These systems are required to complete an independent penetration test and provide an Independent Penetration Test Report documenting the results of the exercise as part of the A&A package.

Information systems must be assessed and authorized every three (3) years or whenever there is a significant change to the system's security posture in accordance with NIST Special Publication 800-37, Revision 2, " Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy," and CIO IT Security 06-30: Managing Enterprise Cybersecurity Risk or via continuous monitoring.

At the Moderate impact level and higher, the Contractor is responsible for providing an independent Security Assessment/Risk Assessment.

If the Agency chooses to perform a Security Assessment/Risk Assessment and Penetration Test, the Contractor shall allow Agency employees (or Agency designated third party contractors) to conduct A&A activities to include control reviews in accordance with NIST 800-53/NIST 800-53A. Review activities include but are not limited to operating system vulnerability scanning, web application scanning, and database scanning of applicable systems that support the processing, transportation, storage, or security of Agency information. This includes the general support system infrastructure.

Identified gaps between required NIST 800-53 controls and the contractor’s implementation as documented in the Security Assessment/Risk Assessment report shall be tracked for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before an Authorization to Operate is issued.

The Contractor is responsible for mitigating all security risks found during the A&A and continuous monitoring activities. Vulnerabilities must be mitigated as follows:

35.4.2 BOD Timelines:

- Within 14 days for vulnerabilities added to CISA’s KEV Catalog with a CVE date post FY 21.
- Per the CISA KEV catalog date or Agency Standard timelines below.
- Within 15 days for Critical (Very High) vulnerabilities for Internet-accessible systems or services.

SAMPLE Agency Standard Timelines

- Within 30 days for Critical (Very High) and High vulnerabilities.
- Within 90 days for Moderate vulnerabilities.
- Within 120 days for Low vulnerabilities for Internet-accessible systems/services.

The Government will determine the risk rating of vulnerabilities.

The Contractor shall comply with all actions specified in DHS Cybersecurity Directives as specified in Additional Stipulations.

35.4.3 Authorization of the System

Upon receipt of the documentation (A&A Package) described in NIST Special Publication 800-37 as documented above, the Agency Authorizing Official (AO) for the system (in coordination with the Agency Chief Information Security Officer (CISO), System Owner, Information System Security Manager (ISSM), and Information System Security Officer (ISSO) will render an authorization decision to:

Authorize system operation w/out any restrictions or limitations on its operation;

Authorize system operation w/restriction or limitation on its operation, or;

Not authorized for operation.

The Contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. At its option, the Government may choose to conduct on site surveys. The Contractor shall make appropriate personnel available for interviews and documentation during this review.

35.5 Reporting and Continuous Monitoring

Maintenance of the security authorization to operate will be through continuous monitoring of security controls of the external system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the Agency per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. They allow Agency AOs to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.

Vendor deliverables as identified below will be reviewed and accepted or rejected by the process described in Agency guidance.

SAMPLE Deliverables to be provided Quarterly to the Agency ISSO, ISSM, and/or COR.

- Vulnerability Monitoring and Scanning (Due NLT 25th of the third month each quarter)
    - Reference: NIST 800-53 control RA-5
    - Provide the most recent Web Application and Operating System vulnerability scan reports. An Agency's control parameter for RA-5, Vulnerability Monitoring and Scanning, may specify the following type and frequency of scans; weekly authenticated scans of operating systems (OS)-including databases, monthly unauthenticated scans of web applications, annual authenticated scans of web applications.

- Plan of Action & Milestones (POA&M) Update (Due NLT the 1st day of the third month of each quarter)
    - Reference: NIST 800-53 control CA-5
    - Provide POA&M updates in accordance with requirements and the schedule set forth by the Agency.
- FISMA Quarterly Metrics data, as necessary (i.e., when a FISMA quarterly data call is issued that is applicable to the system). (Due per data call request deadline)

Deliverables to be provided Annually (or when there is a major change) to the Agency ISSO, ISSM, and/or COR (Due dates for annual deliverables are as indicated in the following lists.) Note: Deliverables annotated with a "*" below may be attested to via an attestation letter.

- Annual Deliverables due NLT February 25th:
    - Annual FISMA Self-Assessment Reference: NIST 800-53 control CA-2
    - Deliver the results of the annual FISMA self-assessment conducted per Agency IT Security guidelines. Based on the controls selected for self-assessment, the Agency OCISO will provide the appropriate test cases for completion.

Updated A&A documentation including the SSPP, Contingency Plan, and Business Impact Analysis

- SSPP
    - Reference: NIST 800-53 control PL-2
    - Review and update the SSPP annually to ensure the plan is current and accurately describes implemented system controls and reflects changes to the contractor system and its environment of operation. The SSPP must be in accordance with NIST 800-18, Revision 1, "Guide for Developing Security Plans for Federal Information Systems."
- Contingency Plan
    - Reference: NIST 800-53 control CP-2
    - Provide an annual update to the contingency plan completed in accordance with NIST 800-34, "Contingency Planning Guide for Federal Information Systems."
- Business Impact Analysis (as an appendix or attachment to the Contingency Plan)
    - Reference: NIST 800-53 control CP-2
    - Provide an annual update to the business impact analysis completed in accordance with NIST 800-34, "Contingency Planning Guide for Federal Information Systems."
    - Contingency Plan Test Report
    - Reference: NIST 800-53 control CP-4
    - Provide a contingency plan test report completed in accordance with Agency Guidelines." A continuity test shall be conducted annually prior to mid-July of each year. The continuity test can be a tabletop test while the system is at the FIPS PUB 199 Low Impact level. The tabletop test must include Federal and hosting Contractor representatives. Functional exercises must be completed once every three years for FIPS PUB 199 Moderate impact systems and annually for FIPS PUB 199 High impact systems.
- Incident Response Test Report
    - Reference: NIST 800-53 control IR-3
    - Provide an incident response test report documenting results of incident reporting.
- User Certification/Authorization Review Documents

  - Reference: NIST 800-53 control AC-2
  - Provide the results of the annual review and validation of system users' accounts to ensure the continued need for system access. The user certification and authorization documents will illustrate how the organization establishes, activates, modifies, reviews, disables, and removes information system accounts in accordance with documented account management procedures.
- *Separation of Duties Document/Matrix
  - Reference: NIST 800-53 control AC-5
  - Develop and furnish a separation of duties matrix reflecting proper segregation of duties for IT system maintenance, management, and development processes. The separation of duties matrix will be updated or reviewed on an annual basis.

Annual Deliverables due NLT June 25th:

- Penetration Testing Report (if applicable)
  - Reference: NIST 800-53 control CA-8
  - All Internet accessible systems, all FIPS PUB 199 High impact systems, and all High Value Asset (HVA) systems are required to complete an independent penetration test and provide a Penetration Test Report documenting the results of the exercise as part of their A&A package. Annual penetration tests are required for these same systems.
- *Information Security Awareness and Training Records (Due NLT June 25th)
  - Reference: NIST 800-53 control AT-4
  - Provide the results of the literacy training and awareness (AT-2) and role-based information security technical training (AT-3). AT-2 requires basic security awareness training for employees and contractors that support the operation of the contractor system. AT-3 requires information security technical training for information system security roles. Training shall be consistent with the requirements contained in C.F.R. Part 5 Subpart C (5 C.F.R 930.301) and conducted at least annually.
- *System(s) Baseline Configuration Standard Document
  - Reference: NIST 800-53 control CM-2
  - Provide a well-defined, documented, and up-to-date specification to which the information system is built.
- Information Exchanges (if applicable)
  - Reference: NIST 800-53 control CA-3
  - Provide Interconnection Security Agreements (ISA), Information Exchange Agreements and any supporting Memoranda of Agreement/Understanding (MOA/U), completed in accordance with NIST 800-47, "Managing the Security of Information Exchanges" if there are existing or new interconnections. Agreements shall include, if applicable, any changes since the last submission; updated agreements are required at least every three years.
- *Rules of Behavior
  - Reference: NIST 800-53 control PL-4
  - Define and establish Rules of Behavior for information system users. Rules of Behavior shall be submitted as an appendix to the SSPP.
- Configuration Management Plan Reference:

  - NIST 800-53 control CM-9
  - Provide an annual update to the Configuration Management Plan for the information system.
- Incident Response Plan
  - Reference: NIST 800-53 control IR-8
  - Provide an annual update to the Incident Response Plan for the information system.
- Personnel Screening and Security
- Reference: NIST 800-53 control PS-3, NIST 800-53 control PS-7
  - Furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. An Agency may separate the risk levels for personnel working on Federal computer systems as follows:

1. A favorable initial fitness/suitability determination must be granted, and a Tier 1 or higher background investigation initiated before access to the Agency network or any Agency IT system. There shall be no waivers to this requirement for Agency network and IT system access for Agency employees or contractors.
2. A favorable initial fitness/suitability determination must be granted, and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate Agency Supervisor (for Agency employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the request of the Agency Supervisor, Data Owner, or CO, shall evaluate the risks associated with each such request.
3. A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the Agency network or IT systems is granted. A waiver may be requested in order to maintain Agency business operations; however, such requests should be used judiciously and not incur unnecessary risks to Agency.

If final adjudication of a background investigation is unfavorable, the Agency network and IT system access must be revoked, and any GFE, including the Agency PIV card, must be retrieved, and returned to OMA.

- System Configuration Settings Verification (e.g., scans)
  - Reference: NIST 800-53 control CM-6/CM-6(1)
  - Establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Configuration settings are the configurable security-related parameters of information technology products that compose the information system. Systems should be configured in agreement with the Agency technical guidelines, NIST guidelines, Center for Internet Security guidelines (Level 1), or industry best practice guidelines in hardening systems, as reviewed and accepted by the Agency AO.
  - Provide the most recent operating system Configuration Settings Compliance scan report.
- Supply Chain Risk Management Plan Reference:
  - NIST 800-53 control SR-2

- Systems must have their own system specific SCRM Plans that detail response activities and reporting requirements to the Agency consistent with NIST SP 800-161.

Annual Deliverable due NLT August 30th:

- HVA Data Call (if applicable)
  - Reference: CISA HVA Program Management Office
  - Respond to the annual HVA data call, if applicable (i.e., when an HVA Data call is issued that is applicable to the vendor/contractor system).
- *Deliverables to be provided Biennially to the Agency ISSO, ISSM, and/or COR (Due NLT June 25th in even numbered years)*

Note: Deliverables annotated with a "*" below may be attested to via an attestation letter.

1. Policies and Procedures

Develop and maintain policies and procedures for the following control families:

- *Access Control (NIST 800-53 AC-1 Policy and Procedures)
- *Awareness and Training (NIST 800-53 AT-1 Policy and Procedures)
- *Audit and Accountability (NIST 800-53 AU-1 Policy and Procedures)
- *Identification and Authentication (NIST 800-53 IA-1 Policy and Procedures)
- *Incident Response (NIST 800-53 IR-1 Policy and Procedures)"
- *System Maintenance (NIST 800-53 MA-1 Policy and Procedures)
- *Media Protection (NIST 800-53 MP-1 Policy and Procedures)
- *Physical and Environmental Protection (NIST 800-53 PE-1 Policy and
- Procedures)
- *Personnel Security (NIST 800-53 PS-1 Policy and Procedures)
- *PII Processing and Transparency (NIST 800-53 PT-1 Policy and Procedures) (if applicable)
- *System and Information Integrity (NIST 800-53 SI-1 Policy and Procedures)
- *System and Communication Protection (NIST 800-53 SC-1 Policy and
- Procedures)
- *Key Management Policy (NIST 800-53 SC-12 Cryptographic Key Establishment and Management)
- *Supply Chain Risk Management (NIST 800-53 SR-1 Policy and Procedures)

35.6 Privacy Requirements

Personally identifiable information (PII) is in the scope of the acquisition and PII is expected to be stored, processed, or transmitted in the vendor's information system. The collection, maintenance, or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all the Agency rules of conduct and in accordance with the Agency Privacy Program requirements.

The contractor shall work with the Agency to prepare a Privacy Threshold Assessment (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the system. The PTA must be completed before development begins and whenever a change with a privacy impact (e.g., a new category of information is collected) is made to an existing system. PTAs are required as part of the Agency's process to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains, or disseminates PII, a PIA must be completed by the contractor and provided to the Agency Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies, and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Per OMB A-130 Privacy Act Statements must include:

1. the authority (whether granted by statute or executive order) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
2. the principal purpose(s) for which the information is intended to be used;
3. the published routine uses to which the information is subject;
4. the effects on the individual, if any, of not providing all or any part of the requested information; and
5. an appropriate citation (and, if practicable, a link) to the relevant SORN(s).

Note: Systems that access data a user creates must assume a user may include privacy data/PII in the system unless the data creation is restricted to data controlled by the system.

All contractor staff who have significant privacy information responsibilities must complete GSA's mandatory privacy awareness and role-based training courses. This includes contractors who work with PII as part of their work duties (e.g., Human Resource staff, Finance staff, and managers/supervisors).

35.7 Additional Stipulations

Security documentation will be marked as follows:

a. Attestation letters, PTAs, and PIAs will not be marked.
b. CP, BIA, and CP Test Reports will be marked CUI//EMGT.

c. All other security documentation will be marked CUI//ISVI.
d. Documents will be marked in bold text on the top of all pages. Spelling out of acronyms is not required.
e. The cover page of each CUI document must contain the following statement on the lower left of the page.
f. Controlled by: Agency Division: Agencyemail@agency.
g. External transmission/dissemination of CUI to or from a government system must be encrypted. A FIPS PUB 140-3/140-2 validated encryption module must be used to encrypt the CUI data.

The Contractor shall certify applications are fully functional and operate correctly as intended on systems using benchmarks from the Agency technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the Agency AO. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved benchmark configuration. Information technology for Windows systems should use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use tools to verify their products operate correctly with the approved benchmark configurations and do not alter the benchmark settings.

The Contractor shall cooperate in good faith in defining non-disclosure agreements (NDAs) that other third parties must sign when acting as the Federal government's agent.

Note: An agency's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements and advising on NDA development.

The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the connect.gov portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified

tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor conduct scans shall be provided in full to the Government.

If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

The Contractor shall comply with 52.204-23 of the Federal Acquisition Regulation (FAR). It prohibits under Section 1634 of Public Law 115-91 the use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

The Contractor shall comply with 52.204-25 of the FAR. It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

The Contractor shall comply with 52.204-27 of the FAR. It prohibits under Section 102 of the Consolidated Appropriations Act 2023, Public Law 117-328, the presence or use of TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited from being used on any information technology as defined in 40 U.S.C. § 11101(6) that is owned or operated by an agency, or used by a contractor under a contract with the agency, or requires the use of such technology expressly or to a significant extent in the performance of a service or the furnishing of a product for an agency.

The Contractor shall comply with requests for data or perform actions based on DHS issued requirements per the Federal Cybersecurity Coordination, Assessment, and Response (C-CAR) Protocol.

The Contractor shall comply with all actions specified in DHS Cybersecurity Directives based on a Directive being applicable to their system or the components therein. In addition, contractors shall update their vulnerability management procedures in accordance with BOD 22-01, including:

- Subscribing to the CISA KEV Catalog automated updates;
- Remediating vulnerabilities as identified for control SI-2 above;

- Providing within 7 days from the required remediation date an email to the ISSO/ISSM or COR certifying remediation consistent with BOD 22-01 requirements.

The Contractor shall comply with all actions specified in Federal mandates, including but not limited to Federal Laws, Executive Orders, and OMB Memoranda, when the mandate is applicable to their system or the components therein. The contractor shall provide data to support compliance with the applicable Federal mandates when requested.

36 CLOUD INFORMATION SYSTEMS – IT SECURITY AND PRIVACY REQUIREMENTS

The contractor shall implement the controls contained within the FedRAMP Cloud Computing Security Requirements Baseline and FedRAMP Continuous Monitoring Requirements for Moderate impact systems (as defined in FIPS PUB 199). These documents define requirements for compliance to meet minimum Federal information security and privacy requirements for Moderate impact systems. The FedRAMP baseline controls are based on NIST Special Publication 800-53, Revision 4, "Security and Privacy Controls for Information Systems and Organizations," and includes a set of additional controls for use within systems providing cloud services to the federal government. FedRAMP is in the process of transitioning to Revision 5 once the transition is complete the controls in the table in Section 5.3 and other text in this section will be updated to reflect FedRAMP's transition.

The contractor shall generally, substantially, and in good faith follow FedRAMP guidelines and Security guidance. In situations where there are no procedural guides, the contractor shall use generally accepted industry best practices for IT security.

The Agency may choose to cancel the contract and terminate any outstanding orders if the contractor has its FedRAMP authorization (Joint Authorization Board [JAB] Provisional or Agency) revoked, and the deficiencies are greater than agency risk tolerance thresholds.

36.1 Assessment and Authorization

36.2 Assessment of the System

If the CSP Software as a Service (SaaS) or Platform as a Service (PaaS) is FedRAMP authorized (i.e., listed as FedRAMP authorized on the FedRAMP Marketplace website), the Agency will leverage the CSP's FedRAMP Assessment and Authorization package to document and assess the customer controls for which the Agency has responsibility for the agency's instance of the CSP's SaaS or PaaS offering. The CSP shall work with the Agency to facilitate documentation and assessment of required customer controls, as necessary.

If the CSP SaaS or PaaS offering is NOT already FedRAMP authorized, the contractor shall comply with FedRAMP requirements as mandated by Federal laws and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The Level of Effort for the A&A is based on the System's FIPS PUB 199 categorizations. The contractor shall create, maintain, and update the following documentation using FedRAMP requirements and templates, which are available at FedRAMP.

- Privacy Impact Assessment (PIA)
- FedRAMP Test Procedures and Results
- Security Assessment Report (SAR)
- System Security Plan (SSP)

- Contingency Plan (CP)
- Business Impact Analysis
- Contingency Plan (CP) Test Results
- Plan of Action and Milestones (POA&M)
- Continuous Monitoring Plan (CMP)
- FedRAMP Control Tailoring Workbook
- Control Implementation Summary Table
- Results of Penetration Testing
- Software Code Review
- Interconnection Security Agreements/Service Level Agreements/Memorandum of Agreements

Information systems must be assessed by an accredited FedRAMP Third Party Assessment Organization (3PAO) initially and whenever there is a significant change to the system's security posture in accordance with the FedRAMP Continuous Monitoring Plan.

The Government reserves the right to perform Security Assessment and Penetration Testing (of its instance). If the Government exercises this right, the contractor shall allow Government employees (or designated third parties) to conduct Security Assessment and Penetration Testing activities to include control reviews in accordance with FedRAMP requirements. Penetration shall be supported by mutually agreed upon Rules of Engagement (RoE). Review activities include but are not limited to manual penetration testing; automated scanning of operating systems, web applications; wireless scanning; network device scanning to include routers, switches, and firewall, and IDS/IPS; databases and other applicable systems, including general support structure, that support the processing, transportation, storage, or security of Government information for vulnerabilities.

The contractor shall provide access to the Federal Government, or their designee acting as their agent, when requested, in order to verify compliance with the requirements for an Information Technology security program. The Government reserves the right to conduct on-site inspections. The contractor shall make appropriate personnel available for interviews and provide all necessary documentation during this review.

Physical Access Considerations – If the Cloud Service Provider (CSP) is operated within an Infrastructure as a Service (IaaS) that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

Identified gaps between required FedRAMP Security Control Baselines and Continuous Monitoring controls and the contractor's implementation as documented in the Security Assessment Report shall be tracked by the contractor for mitigation in a Plan of Action and Milestones (POA&M) document. Depending on the severity of the gaps, the Government may require them to be remediated before the Agency authorization is issued.

The contractor is responsible for mitigating all security risks found during A&A and continuous monitoring activities. All high-risk vulnerabilities must be mitigated within 30 days and all moderate risk vulnerabilities must be mitigated within 90 days from the date vulnerabilities are formally identified. The Government will determine the risk rating of vulnerabilities.

36.3 Authorization of the System

If the CSP Software as a Service (SaaS) or Platform as a Service (PaaS) is FedRAMP authorized (i.e., listed as FedRAMP authorized on the FedRAMP Marketplace website), the Agency will leverage the CSP's FedRAMP Assessment and Authorization package and the Agency's assessment of the customer controls for which the Agency has responsibility to issue a the Agency ATO for the agency's instance of the CSP's SaaS or PaaS offering.

If the CSP SaaS or PaaS offering is NOT already FedRAMP authorized, it shall:

- Operate on an CSP IaaS environment that is FedRAMP authorized; AND
- Be listed on the FedRAMP In Process Website OR be listed on the FedRAMP Ready website.
- Shall deliver within 90 days of contract award a FedRAMP Readiness Assessment
- Review completed by a FedRAMP 3PAO following the FedRAMP Readiness Assessment Guidelines. The FedRAMP Readiness Assessment Review demonstrates the CSPs overall readiness for FedRAMP authorization and whether it has a viable path to achieve a FedRAMP authorization within one (1) year of the contract award. If the CSP does not provide a FedRAMP Readiness Assessment as prescribed or the assessment demonstrates a significant gap in capabilities that will preclude achievement of a FedRAMP authorization within 1 year of the contract award, then, the Agency will terminate the contract.
- CSP shall ensure these essential NIST SP 800-53 security controls (AC-2, AU-2, CM-6, CP-7, CP-8, IA-2 (1), IA-2 (2), IA-2 (12), IA-7, MP-4, MP-5, PL-8, RA-5, SC-8 / SC-8(1), SC-13, SC-17, SC-18, SC-22, SC-28 (1), SI-2, SI-3, SI-4, and SI-10) are implemented for the applicable baselines (Low, Medium, High, Tailored LiSaaS). CSP shall implement FedRAMP control parameters and implementation guidance, as applicable. Further, the CSP shall make the proposed system and security architecture of the information system available to the Security Engineering Division, in the Office of the Chief Information Security Officer for review and approval before commencement of system build (architecture, infrastructure, and code (as applicable)) and/or the start as A&A activities.

If requirements a-d, as defined above, are met the CSP will have one (1) year from the date of contract award to achieve FedRAMP authorization. During this transitional period, the Agency may issue an agency specific authorization (i.e., not FedRAMP) not to exceed one (1) year (to allow the CSP to achieve FedRAMP compliance) leveraging an existing ATO with another Federal Department/Agency (D/A) (with supporting A&A Package). The CSP may have a non-FedRAMP ATO with another D/A or be based on the Agency Moderate Impact SaaS Solutions process as described in the Agency IT Security Procedural Guide. The CSP shall make available any existing assessment and authorization package for agency review and provide necessary documentation and access to facilitate the Agency Moderate Impact SaaS A&A process. If a FedRAMP authorization is not obtained within 1 year of contract award; the Agency will not be able to use the product for the option years and shall terminate the contract.

36.4 Reporting and Continuous Monitoring

If the CSP Software as a Service (SaaS) or Platform as a Service (PaaS) is FedRAMP authorized:

Maintenance of the FedRAMP Authorization will be through continuous monitoring and periodic audit of the operational controls within a contractor's system, environment, and processes to

determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated in agreement with FedRAMP guidelines and submitted to the connect.gov Portal or repository designated by the FedRAMP program.

The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information systems. The deliverables will allow the Federal Departments/Agencies leveraging the services providers' cloud offering to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur. Contractors will be required to provide updated deliverables and automated data feeds as defined in the FedRAMP Continuous Monitoring Plan.

If the CSP SaaS or PaaS offering is NOT already FedRAMP authorized, the contractor shall provide continuous monitoring deliverables in support of a one (1) year conditional authorization until FedRAMP authorization is achieved at which time the contractor will follow the FedRAMP process. Deliverables to be provided during this conditional authorization shall include:

- Quarterly, provide the most recent Web Application and Operating System vulnerability scan reports. the Agency's control parameter for RA-5, Vulnerability Monitoring and Scanning, specifies the following type and frequency of scans; weekly authenticated scans of operating systems (OS)-including databases, monthly unauthenticated scans of web applications, annual authenticated scans of web applications (deliverable shall include raw results and findings shall be included in the POA&M document).
- Quarterly, provide POA&M updates in accordance with requirements and the schedule set forth in the Agency CIO IT Security Procedural Guide.
- Annually, provide A&A Package updates including the System Security Plan, Contingency Plan, Business Impact Analysis, Configuration Management Plan, Contingency Plan Test Report, and Annual FISMA Assessment.

Upon achievement of FedRAMP authorization, the Agency will accept the FedRAMP A&A and continuous monitoring documentation made available on a repository designated by the FedRAMP program in agreement with FedRAMP guidelines to satisfy the continuous monitoring requirement.

36.5 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. An Agency may separate the risk levels for personnel working on Federal computer systems as follows:

- A favorable initial fitness/suitability determination must be granted, and a Tier 1 or higher background investigation initiated before access to the Agency network or any Agency IT system. There shall be no waivers to this requirement for Agency network and IT system access for Agency employees or contractors.
- A favorable initial fitness/suitability determination must be granted, and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate Agency Supervisor (for Agency employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the

request of the Agency Supervisor, Data Owner, or CO, shall evaluate the risks associated with each such request.

- A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the Agency network or IT systems is granted. A waiver may be requested in order to maintain Agency business operations; however, such requests should be used judiciously and not incur unnecessary risks to Agency.

If final adjudication of a background investigation is unfavorable, Agency network and IT system access must be revoked, and any GFE, including the PIV card, must be retrieved, and returned to the Agency.

Agency shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period.

36.6 Sensitive Information Storage

Controlled Unclassified Information (CUI), data, and/or equipment will only be disclosed to authorized personnel on a need-to-know basis. The contractor shall ensure that appropriate administrative, technical, and physical safeguards are established to ensure the security and confidentiality of this information, data, and/or equipment is properly protected. When no longer required, this information, data, and/or equipment will be returned to Government control, destroyed, or held until otherwise directed. Destruction of items shall be accomplished by following NIST Special Publication 800-88, Revision 1, “Guidelines for Media Sanitization.” The destruction, purging or clearing of media specific to the CSP will be recorded and supplied upon request of the Government.

36.7 Protection of Information

The contractor shall be responsible for properly protecting all information used, gathered, or developed as a result of work under this contract. The contractor shall also protect all Government data, equipment, etc. by treating the information in accordance with its FISMA system categorization.

All information about the systems gathered or created under this contract should be considered as CUI information. If contractor personnel must remove any information from the primary work area that is included in the ATO boundary, they should protect it to the same FedRAMP requirements. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

36.7.1 Unrestricted Rights to Data

The government will retain unrestricted rights to government data. The ordering activity retains ownership of any user created/loaded data and applications hosted on vendor's infrastructure, as well as maintains the right to request full copies of these at any time.

36.7.2 Personally Identifiable Information

Personally identifiable information (PII) is in the scope of acquisition and PII is expected to be stored in the vendor's cloud solution. The vendor shall prepare a Privacy Threshold Assessment (PTA) to either document PII is not in scope, or determine which categories of information will be stored, processed, or transmitted by the system. The use of any information that is subject to the Privacy Act will be utilized in full accordance with all rules of conduct as applicable to Privacy Act Information.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's information system must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains, or disseminates PII, a PIA must be completed by the contractor and provided to the Agency Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies, and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

36.7.3 Data Availability

The data must be available to the Government upon request within one business day or within the timeframe negotiated with the Contractor and shall not be used for any other purpose other than that specified herein. The contractor shall provide requested data at no additional cost to the government.

36.7.4 Data Release

Any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor

that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

Contractor will not disclose Customer Data to any government or third party or access or use Customer Data; except in each case as necessary to maintain the Cloud Services or to provide the Cloud Services to Customer in accordance with this contract, or as necessary to comply with the law or a valid and binding order of a governmental or regulatory body (such as a subpoena or court order). Unless it would be in violation of a court order or other legal requirement, the Contractor will give the Government reasonable notice of any such legal requirement or order, to allow the Government to seek a protective order or other appropriate remedy.

36.8 Data Ownership

All Government data collected in the system is the property of the Federal Government. All data collected by the system shall be provided by the Contractor (system provider) as requested during the contract period and at the completion of the contract period.

36.9 Confidentiality and Nondisclosure

Personnel working on any of the described tasks, may at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

36.10 Agency Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee NDA. The Contractor shall submit to the COR a completed confidentiality and NDA for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this NDA, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

Note: Agency's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, Agency OGC can advise on NDA development.

36.11 Additional Stipulations

If the CSP SaaS or PaaS is FedRAMP authorized security documentation will be marked in accordance with FedRAMP guidelines.

If the CSP SaaS or PaaS offering is NOT already FedRAMP authorized security documentation will be marked as follows:

- PTAs, and PIAs will not be marked.
- CP, BIA, and CP Test Reports will be marked CUI//EMGT.
- All other security documentation will be marked CUI//ISVI.
- Documents will be marked in bold text on the top of all pages. Spelling out of acronyms is not required.
- The cover page of each CUI document must contain the following statement on the lower left of the page.
- Controlled by: Agency:
- External transmission/dissemination of CUI to or from a government system must be encrypted. A FIPS PUB 140-3/140-2 validated encryption module must be used to encrypt the CUI data.

The Contractor shall certify applications are fully functional and operate correctly as intended on systems using benchmarks from agency technical guidelines, NIST guidelines, Center for Internet Security guidelines, or industry best practice guidelines, as reviewed and accepted by the agency AO. The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved benchmark configuration. Information technology for Windows systems should use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall. Applications designed for normal end users shall run in the standard user context without elevated system administration privileges. The contractor shall use tools to verify their products operate correctly with the approved benchmark configurations and do not alter the benchmark settings.

The contractor shall cooperate in good faith in defining an NDA that other third parties must sign when acting as the Federal government's agent.

Note: The Agency's Office of the General Counsel (OGC) is available to coordinate on defining NDA requirements. Upon request, GSA OGC can advise on NDA development.

The contractor shall comply with any additional FedRAMP privacy requirements.

The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to connect.gov. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

Physical Access Considerations – If the SaaS provider is operated within an IaaS that is FedRAMP authorized (e.g., AWS); physical access to the physical datacenter environment will be governed by the terms of access allowed by the underlying infrastructure provider as defined in the FedRAMP A&A authorization package.

The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor conduct scans shall be provided in full to the Government.

If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

The Contractor shall comply with 52.204-23 of the Federal Acquisition Regulation (FAR). It prohibits under Section 1634 of Public Law 115-91 the use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

The Contractor shall comply with 52.204-25 of the FAR. It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses

telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

The Contractor shall comply with 52.204-27 of the FAR. It prohibits under Section 102 of the Consolidated Appropriations Act 2023, Public Law 117-328, the presence or use of TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited from being used on any information technology as defined in 40 U.S.C. § 11101(6) that is owned or operated by an agency, or used by a contractor under a contract with the agency, or requires the use of such technology expressly or to a significant extent in the performance of a service or the furnishing of a product for an agency.

If the CSP SaaS or PaaS is NOT FedRAMP authorized, the Contractor shall comply with all actions specified in Federal mandates, including but not limited to Federal Laws, Executive Orders, and OMB Memoranda, when the mandate is applicable to their system or the components therein. The contractor shall provide data to support compliance with the applicable Federal mandates when requested.

36.12 References

- FIPS PUB 140-3[4], "Security Requirements for Cryptographic Modules"
- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
- NIST SP 800-53, Revision 4, Security and Privacy Controls for Information Systems and
- Organizations
- NIST SP 800-88, Revision 1, "Guidelines for Media Sanitization"
- NIST SP 800-218, "Secure Software Development Framework (SSDF) Version 1.1:
- Recommendations for Mitigating the Risk of Software Vulnerabilities"
- CSP Authorization Playbook-Getting Started with FedRAMP
- GSA Order CIO 2100.1, "GSA Information Technology (IT) Security Policy"
- GSA Order ADM 2181.1, "Homeland Security Presidential Directive-12 Personal Identity Verification and Credentialing Policy, and Background Investigations for Contractor Employees"

37 MOBILE APPLICATION - IT SECURITY AND PRIVACY REQUIREMENTS

The contractor shall generally, substantially, and in good faith follow agency IT Security Policy and Guidelines In situations where there is no procedural guidance, the contractor shall use generally accepted industry best practices for IT security.

37.1 General Mobile Application Guidelines

The Mobile Application (App) shall be integrated with a Mobile Device Management (MDM) solution. [specify agency MDM solution here] (e.g. GSA currently uses MAAS 360 and Google MDM solutions).

The contractor shall provide, upon request, to the agency IT Contracting Officer Representative (COR) all supporting artifacts of security testing of the source code for the mobile application (i.e. evidence of static application security testing/ dynamic application security testing (SAST/DAST) code reviews of completed application code).

The contractor shall maintain clear and concise documentation so that future developers and programmers can understand the processes used and are able to enhance, edit or build upon the original App.

- The contractor shall maintain detailed process and code documentation.
- The contractor shall provide App features documentation.
- The contractor shall support development and updates of a security authorization package for the App.

37.2 Mobile Device Security

The contractor shall adhere to the following requirements and guidelines for developing mobile applications.

A mobile application, most commonly referred to as an app, is a type of application software designed to run on a mobile device, such as a smartphone or tablet computer. Mobile applications frequently serve to provide users with similar services to those accessed on PCs. Apps are generally small, individual software units with limited capabilities and isolated functionality. The simplest apps are developed to utilize the web browser of the mobile device to provide a feature set integration much like what is found on a user's PC. However, as mobile app development has grown, a more sophisticated approach involves developing applications specifically for the mobile environment, taking advantage of both its limitations and advantages. For example, apps that use location-based features are inherently built from the ground up with an eye to mobile devices given that you do not have the same concept of location on a PC. With this new paradigm in both mobile platforms and the applications loaded on them, the Agency will concentrate security focus on the following goals:

- All apps loaded have an initial assessment by the Agency for acceptability and then a security assessment & authorization, when required.

- All apps are deployed from only trusted sources, following their security/assessment process – This presently is the Apple iTunes store for iOS and the Google Play store for Android. A MDM solution may also be used, once retrieved from these sources, for enterprise deployment.
- Terms of Service (ToS) discipline is adhered to, based on acceptability of an app – either as an individual user or for an Agency.
- Apps deemed to be unacceptable are blacklisted.
- Mobile app inventory for all devices is maintained using an MDM.
- Agency developed apps are assessed, evaluated, and approved by the AO for the system they support before deployment.

37.3 Application Sources

Allowing mobile apps to be loaded from an unknown source presents one of the greatest risks to the Federal government's IT environment when using mobile devices. "Side loading" of apps is a process where a user installs an application from a source other than the Apple ITunes store or Google Play store. If a user jailbreaks a device, side loading can occur as well. Jailbreaking, or rooting, is a process where an Operating System (OS) of a mobile device grants a user or application root level access to the OS. While iOS devices that are not jailbroken/rooted protect against sideloading, the Android OS allows a user to turn such protection on/off (allow unknown sources) if not managed by MDM. Any mobile apps provided by the contractor must be compatible with the agency's MDM solution(s).

37.4 Terms of Service (ToS)

Many terms found in commercial TOS or End User License Agreements (EULA) are not acceptable when the Government is the end user. The Office of Chief Information Officer (OCIO) requires that software and services within the Agency Enterprise have approved ToS or EULA.

Apps deemed to be acceptable are loaded at the discretion of the user for either personal use or as a personal productivity tool to further enhance the work experience. As such, use of the App is not mandated by the agency. Therefore, acceptance of the ToS falls upon the user as an individual. This is true even if the App is loaded using an agency.gov domain account or registered with a user's .gov email address.

Apps that are approved after formal assessment: and include a formal review by Agency Counsel as part of the review/approval process, where the ToS was found to be acceptable to the government or a modified ToS was negotiated as part of the approval review, prior to final authorization. When loaded and activated, the user is accepting the ToS (often a technical function required of the user), not as an individual, but as an employee or contract employee assigned to perform work functions for the Agency.

37.5 Privacy Requirements

Personally identifiable information (PII) is expected to be stored, processed, or transmitted in the vendor's App. The collection, maintenance, or dissemination of any PII that is subject to the Privacy Act and/or the E-Government Act will be handled in full accordance with all Agency rules of conduct and in accordance with Agency Privacy Program requirements.

The contractor shall work with the Agency to prepare a Privacy Threshold Assessment (PTA) to confirm and document PII is not in scope, or to determine which categories of information will be stored, processed, or transmitted by the App. The PTA must be completed before development begins and whenever a change with privacy impact (e.g., a new category of information is collected) is made to an existing App. PTAs are required to determine whether a Privacy Impact Assessment (PIA) and/or a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the App.

PII (should it come into scope) will require the following guidelines be adhered to.

- The vendor's App must be authorized at least at the FIPS PUB 199 Moderate level.
- For any system that collects, maintains, or disseminates PII, a PIA must be completed by the contractor and provided to the Agency Privacy Office for review along with the other authorization to operate (ATO) documents.
- If the system retrieves information using PII, the Privacy Act applies, and it must have a system of records notice (SORN) published in the Federal Register.
- If PII is collected from individuals by the system, a Privacy Act Statement (i.e., Privacy Notice) must be provided to users prior to their use of the application on what data is being collected and why, as well as the authority for the collection and the impact of not providing some or all of it. The Privacy Act Statement must be available to the individual directly on the form used to collect the information. Providing a link back to the Statement from the form is acceptable.

Per OMB A-130 Privacy Act Statements must include:

1. the authority (whether granted by statute or executive order) that authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
2. the principal purpose(s) for which the information is intended to be used;
3. the published routine uses to which the information is subject;
4. the effects on the individual, if any, of not providing all or any part of the requested information; and
5. an appropriate citation (and, if practicable, a link) to the relevant SORN(s).

Note: Apps that access data a user creates must assume a user may include privacy data/PII in the application unless the data creation is restricted to data controlled by the App.

All contractor staff who have significant privacy information responsibilities must complete the Agency's mandatory privacy awareness and role-based training courses. This includes contractors who work with PII as part of their work duties (e.g., Human Resource staff, Finance staff, and managers/supervisors).

37.6 Agency App Development, Assessment, Authorization and Deployment

Agency developed apps are designed to take advantage of the concept of Anytime, Any Where, Any Device (A3) to allow Agency users and customers to access Agency data while mobile. As such, as the Agency develops apps for use on the iOS and Android environment, these apps must undergo an

assessment and authorization process before being deployed. With that in mind, the following guidelines are to be followed:

An Agency developed app that supports a FISMA system must be documented in the System Security and Privacy Plan and authorized to operate as part of a current ATO letter from the respective AO before deployment. Any app that is not directly tied to an already existing system authorized to operate must have an assessment performed and subsequently approved for release by the Chief Information Security Officer (CISO).

Any mobile app development shall result in a minimum of the release of both an iOS and Android version of the app. This ensures coverage to all users within the Agency and the maximum coverage for apps released to the public. Any additional application versions for alternate OS mobile platforms may be developed for such apps, but iOS and Android shall remain as the core base OSs for Agency developed mobile apps for all releases.

All developed apps must follow the respective application review and publication guidelines for the OS to which they were, and the release process documented in this section.

Other than for testing purposes on non-user provisioned mobile devices, side loading of apps in the environment is not authorized.

Where available, the Agency Mobile App Store is authorized for enterprise deployment of apps to Agency user devices once that app has been assessed, authorized, and published according to the guidelines outlined in this section.

Mobile code scanning throughout the development cycle is critical, but before release by the Mobile Device Team, a mobile app must be scanned by the Systems Engineering Division Team within the OCISO. This scan is a source code scan using an Agency approved source code scanner. As with all applications at the Agency, no High/Critical findings are allowed from these scan results. Moderate findings should be documented in the respective POA&M for the system by which the app is authorized and accepted by the AO; Low and Informational findings should be taken into consideration by the developers for their next iteration of app development. A detailed process for mobile app release is documented at the end of this section.

All mobile application development should take into consideration the Open Web Application Security Project (OWASP) Mobile Security Project when developing mobile apps either within GSA or for use by the general public. The guidelines for mobile application security testing from OWASP are linked below:

- –OWASP Mobile Security Project Home Page
- –OWASP Mobile Security Testing Guide

Agency developed mobile apps must undergo an assessment review and approval process before being released for use. These apps fall into two categories that shall have slightly different processes for approval, with many common steps.

Mobile apps that are developed as part of another system with a current ATO and provide access to an application using a different form factor (smartphones/tablets), such apps must be documented in the System Security and Privacy Plan for the system they support.

Mobile apps designed for a specific purpose not part of a current ATO stand alone in their ATO. As these apps do not have a parent system they support, the below listed process is the complete assessment process required for these apps.

All apps must follow the approval processes outlined below:

1. Apps must be scanned prior to release by the Office of the CISO using an Agency approved source code scanner. No Critical/High findings may remain for approval to be received and any moderate/medium findings must be contained in a POA&M, either for the system the app is a part of, or a separate POA&M if a standalone mobile app.
2. The privacy requirements as stated above must be met.
3. A mobile application security assessment review must be completed and signed by the mobile App owner, mobile App assessor, mobile App Information System Security Manager (ISSM), a representative of the Office of the CISO, to denote a proper assessment and review was conducted of the mobile app prior to release.

37.7 Intellectual Property

This SIN SOW and resulting task orders are funded by the United States Government. All intellectual property generated and/or delivered pursuant to this Firm-Fixed Price Statement of Work will be subject to appropriate federal acquisition regulations which entitle the Government to unlimited license rights in technical data and computer software developed exclusively with Government funds, a nonexclusive “paid-up” license to practice any patentable invention or discovery made during the performance of the ordering agency TO, and a “paid-up” nonexclusive and irrevocable worldwide license to reproduce all works (including technical and scientific articles) produced during this task order.

37.8 Confidentiality and Nondisclosure

The preliminary and final deliverables and all associated working papers and other material deemed relevant by the agency that have been generated by the contractor in the performance of an ordering agency task order, are the property of the U.S. Government and must be submitted to the ordering agency COR at the conclusion of the contract. The U.S. Government has unlimited data rights to all deliverables and associated working papers and materials.

All documents produced for this project are the property of the U.S. Government and cannot be reproduced or retained by the contractor. All appropriate project documentation will be given to the agency during and at the end of this contract. The contractor shall not release any information without the written consent of the ordering agency Contracting Officer.

Personnel working on any of the described tasks may, at Government request, be required to sign formal non-disclosure and/or conflict of interest agreements (NDA/COI) to guarantee the protection and integrity of Government information and documents.

Additionally, any information made available to the Contractor by the Government shall be used only for the purpose of carrying out the provisions of this contract and shall not be divulged or made known in any manner to any persons except as may be necessary in the performance of the contract. In performance of this contract, the Contractor assumes responsibility for protection of the

confidentiality of Government records and shall ensure that all work performed by its subcontractors shall be under the supervision of the Contractor or the Contractor's responsible employees. Each officer or employee of the Contractor or any of its subcontractors to whom any Government record may be made available or disclosed shall be notified in writing by the Contractor that information disclosed to such officer or employee can be used only for that purpose and to the extent authorized herein. Further disclosure of any such information, by any means, for a purpose or to an extent unauthorized herein, may subject the offender to criminal sanctions imposed by 18 U.S.C. §§ 1030.

37.9 Agency Non-Disclosure Agreement

Each individual contractor/subcontractor employee who performs work on this contract is required to sign an Employee NDA. The Contractor shall submit to the ordering agency COR a completed confidentiality and NDA form for each individual contractor/subcontractor.

The Contractor and all contractor/subcontractor employees may have access to sensitive data, proprietary, or confidential business information of other companies or the Government in the course of performing official duties on this contract. The term "proprietary information" means any information considered so valuable by its owners that it is held in secret by them and their licensees and is not available to the public.

All information that is (1) obtained related to or derived from this contract, and (2) results from or derived from any actual tasks assigned to contractor employees while participating on this contract is considered proprietary.

The Contractor and all contractor/subcontractor employees will not use vendor proprietary information except as necessary to perform this contract and shall agree not to disclose such information to third parties, including any employee of the contractor/subcontractor who has not executed this NDA, or use such information in any manner inconsistent with the purpose for which it was obtained. Anyone failing to comply with the agreement may be subject to disciplinary action or termination of employment by the contractor/subcontractor, and possible administrative, civil, or criminal penalties.

37.10 Personnel Security Requirements

Contractor shall furnish documentation reflecting favorable adjudication of background investigations for all personnel (including subcontractors) supporting the system. An Agency may separate the risk levels for personnel working on Federal computer systems as follows:

- A favorable initial fitness/suitability determination must be granted, and a Tier 1 or higher background investigation initiated before access to the Agency network or any Agency IT system. There shall be no waivers to this requirement for Agency network and IT system access for Agency employees or contractors.
- A favorable initial fitness/suitability determination must be granted, and a Tier 2 or higher background investigation initiated before access to PII/CUI is granted. The authority and access shall be determined by the appropriate Agency Supervisor (for Agency employees) or CO (for contract personnel), Data Owner, and the System's AO. Each System's AO, with the request of the Agency Supervisor, Data Owner, or CO, shall evaluate the risks associated with each such request.

- A favorable suitability determination must be completed at a Tier 2 or higher background investigation before privileged access to the Agency network or IT systems is granted. A waiver may be requested in order to maintain Agency business operations; however, such requests should be used judiciously and not incur unnecessary risks to the Agency.

If final adjudication of a background investigation is unfavorable, Agency network and IT system access must be revoked, and any GFE, including the PIV card, must be retrieved, and returned to the Agency.

The Agency shall sponsor the investigation when deemed necessary. No access shall be given to government computer information systems and government sensitive information without a background investigation being verified or in process. If results of background investigation are not acceptable, then access shall be terminated.

The Contractor shall provide a report of separated staff on a monthly basis, beginning 60 days after execution of the option period of a task order.

37.11 Additional Stipulations

If the following documentation regarding a Mobile app is provided, it will be marked as follows:

- PTAs and PIAs will not be marked.
- CP, BIA, and CP Test Reports will be marked CUI//EMGT.
- All other security documentation will be marked CUI//ISVI.
- Documents will be marked in bold text on the top of all pages. Spelling out of acronyms is not required.
- The cover page of each CUI document must contain the following statement on the lower left of the page.
- Controlled by: Agency.
- External transmission/dissemination of CUI to or from a government system must be encrypted. A FIPS PUB 140-3/140-2 validated encryption module must be used to encrypt the CUI data.

The Contractor shall certify mobile applications are fully functional and operate correctly as intended on mobile devices in accordance with Agency guidance. The standard installation, operation, maintenance, update, and/or patching of mobile applications shall not alter configuration settings as documented in Agency Guidance. Mobile applications designed for normal end users shall run in the standard user context without elevated administrator privileges.

The Contractor shall cooperate in good faith in defining NDAs that other third parties must sign when acting as the Federal government's agent.

The Government has the right to perform manual or automated audits, scans, reviews, or other inspections of the vendor's IT environment being used to provide or facilitate services for the Government. The Contractor shall be responsible for the following privacy and security safeguards:

The Contractor shall not publish or disclose in any manner, without the Contracting Officer's written consent, the details of any safeguards either designed or developed by the Contractor under this

contract or otherwise provided by the Government. Exception - Disclosure to a Consumer Agency for purposes of A&A verification or to the FedRamp portal. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of Government data, the Contractor shall afford the Government access to the Contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Access to support incident investigations, shall be provided as soon as possible but not longer than 72 hours after request.

The program of inspection shall include, but is not limited to:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Authenticated and unauthenticated database application vulnerability scans

Automated scans can be performed by Government personnel, or agents acting on behalf of the Government, using Government operated equipment, and Government specified tools. If the vendor chooses to run its own automated scans or audits, results from these scans may at the Government's discretion, be accepted in lieu of Government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the Government. In addition, the results of vendor conduct scans shall be provided in full to the Government.

If new or unanticipated threats or hazards are discovered by either the Government or the Contractor, or if existing safeguards have ceased to function, the discoverer shall immediately bring the situation to the attention of the other party.

The Contractor shall comply with all actions specified in Federal mandates, including but not limited to Federal Laws, Executive Orders, and OMB Memoranda, when the mandate is applicable to their system or the components therein. The contractor shall provide data to support compliance with the applicable Federal mandates when requested.

38 NONFEDERAL SYSTEMS AND ORGANIZATIONS – IT SECURITY AND PRIVACY REQUIREMENTS

38.1 Required Policies and Regulations for Contracts

Federal Laws, Regulations, and Guidance:

The contractor shall comply with all applicable Federal Laws, Regulations, and Guidance.

- CUI Regulation 32 CFR Part 2002, "Controlled Unclassified Information (CUI)"
- FISMA of 2014, "The Federal Information Security Modernization Act of 2014"
- Privacy Act of 1974, "5 USC, § 552a"
- E-Government Act of 2002 section 208, "44 USC 3501"
- OMB Circular A-108, "Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act"
- OMB M-03-22, "OMB Guidance for Implementing the Privacy Provisions of the E-
- Government Act of 2002"
- Title 44 U.S. Code, Sec. 3554, "Federal agency responsibilities"

Federal Standards and Guidance:

The contractor shall comply with the following Federal Information Processing Standards (FIPS) and NIST guidelines.

- FIPS PUB 199, "Standards for Security Categorization of Federal Information and Information Systems"
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems"
- NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations"
- NIST SP 800-53A, Revision 5, "Assessing Security and Privacy Controls in Information Systems and Organizations."
- NIST SP 800-60, Volume I, Revision 1, "Volume I: Guide for Mapping Types of
- Information and Information Systems to Security Categories"
- NIST SP 800-60, Volume II, Revision 1, "Volume II: Appendices to Guide for Mapping
- Types of Information and Information Systems to Security Categories"
- NIST 800-63B, "Digital Identity Guidelines, Authentication and Lifecycle Management"
- NIST SP 800-161, Revision 1, "Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations"
- NIST SP 800-171, Revision 2, "Protecting Controlled Unclassified Information in
- Nonfederal Systems and Organizations"

- NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information."
- NIST SP 800-172, "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171."
- NIST SP 800-172A, "Assessing Enhanced Security Requirements for Controlled Unclassified Information."

38.2 Agency Security Compliance Requirements

To comply with the Federal standard, nonfederal systems and organizations shall implement the specific security requirements in NIST SP 800-171 and NIST SP 800-172 controls requirements have been tailored for non-federal entities, eliminating requirements, controls, or parts of controls that are uniquely Federal, not directly related to protecting the confidentiality of CUI; or expected to be routinely satisfied by nonfederal organizations without specification. NIST SP 800-171 and NIST SP 800-172 controls are derived from FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems," the moderate security control baseline in NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations," and are based on the CUI regulation 32 CFR Part 2002, "Controlled Unclassified Information." For systems storing, processing, or transmitting Personally Identifiable Information (PII) selected Privacy requirements from NIST SP 800-53, Revision 5, "Security and Privacy Controls for Information Systems and Organizations" are also required.

The basic and derived security requirements in NIST SP 800-171, NIST SP 800-172, and NIST SP 800-53-when applicable, provide protection from unauthorized disclosure and unauthorized modification of CUI. The requirements apply only to the components of non-federal systems that process, store, or transmit CUI, or that provide security protection for such components.

38.3 Security Assessment Activities and Required Documentation

The non-federal system/organization shall implement the NIST SP 800-171, Revision 2 and NIST SP 800-172 controls; conduct an independent security assessment using NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information" and NIST SP 800172A, "Assessing Enhanced Security Requirements for Controlled Unclassified Information" with results documented in a security assessment report; and security vulnerabilities or gaps in security requirements documented in a Plan of Action and Milestones (POA&M).

The resultant documents including the System Security and Privacy Plan (SSPP), Security Assessment Report (SAR), and POA&M will be critical inputs to a risk management decision by the Agency to process, store, or transmit CUI on a system hosted by a nonfederal organization and whether it is advisable to pursue an agreement or contract with the non-federal organization. The failure to implement the security requirements and controls identified by the Agency and maintain the supporting documentation will result in the termination of the contract.

The non-federal system must have a new independent security assessment conducted at least every three (3) years or at the discretion of the Agency when there is a significant change to the system's security posture or via continuous monitoring. Documents that contain CUI must be marked as such. Not all deliverables contain CUI. When in question, the contractor should use the NARA CUI Registry to help determine the appropriate designation for marking, handling, or transmitting. The contractor

shall create, maintain, and update the following security documentation and make available to the Government:

- **System Security and Privacy Plan (SSPP)** The SSPP will document the system's implementation of NIST SP 800-171, SP 800-172, and NIST SP 800-53 (required if PII is in scope).
- **Security Assessment Report (SAR)** The SAR will document the assessment results for the system. Nonfederal information systems must have an independent assessment performed and authorized every three (3) years or whenever there is a significant change to the non-federal system's security posture. The independent assessor shall be a FedRAMP accredited Third Party Assessment Organizations (3PAOs) or be approved by the Agency if not a 3PAO. A Penetration Test Report shall be included as an attachment (if performed) documenting the results of an independent exercise.
- **Plan of Action & Milestones (POA&M)** document completed in accordance with Agency Guidance.
- **Penetration Test Report** documenting the results of an independent exercise.

38.4 Reporting and Continuous Monitoring

Maintenance of security will be through continuous monitoring of security controls of the nonfederal system and its environment of operation to determine if the security controls in the information system continue to be effective over time in light of changes that occur in the system and environment. Through continuous monitoring, security controls and supporting deliverables are updated and submitted to the Agency per the schedules below. The submitted deliverables (or lack thereof) provide a current understanding of the security state and risk posture of the information system(s). They allow the Agency to make credible risk-based decisions regarding the continued usage of non-federal systems and initiate appropriate responses as needed when changes occur.

Deliverables to be provided Quarterly to the Information System Security Officer (ISSO), Information System Security Manager (ISSM), and/or Contracting Officer (COR)

- Vulnerability Scanning
    - Reference: NIST SP 800-171, Revision 2 Security Requirement 3.11.2
    - Scan for vulnerabilities in organizational systems and applications periodically and when new vulnerabilities affecting those systems and applications are identified. Provide the most recent Web Application and Operating System vulnerability scan reports.
- Plan of Action & Milestones (POA&M) Update
    - Reference: NIST SP 800-171, Revision 2 Security Requirement 3.12.2
    - Develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational systems. Provide POA&M updates in accordance with requirements and the schedule set forth in GSA CIO-IT Security-09-44: Plan of Action and Milestones (POA&M).
- Shared Drive Access Review
    - The Vendor and Agency ISSO shall review the membership and access to the shared collaboration drive.

Quarterly Deliverables are due one month prior to the completion of each quarter in the government fiscal year, ending on September 30. Due dates are the last workday of the months listed:

- Quarter 1 – November
- Quarter 2 – February
- Quarter 3 – May
- Quarter 4 – August

Deliverables to be provided to the ISSO, ISSM, and/or COR annually or when there is a major change to the system.

- Updated SSPP
    - Reference NIST SP 800-171, Revision 2 security requirement 3.12.4
    - Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security and privacy requirements are implemented, and the relationships with or connections to other systems.

Annual deliverables are due two months prior to completion of the government fiscal year, ending on September 30. Due date is the last workday of July.

Deliverables to be provided to the ISSO, ISSM, and/or COR every three years or when there is a major change to the system.

- Security Assessment Report
    - Reference: NIST 800-171, Revision 2 Security Requirement 3.12.1
    - Periodically assess the security controls in organizational systems to determine if the controls are effective in their application. Deliver the results of the security assessment conducted by a 3PAO/independent security assessor using the assessment procedures in NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information, to be completed using the SAR template provided by the GSA. The SAR is completed in accordance with a security assessment plan that is mutually agreed upon by the GSA, the vendor, and the 3PAO/independent security assessor following the process requirements in CIO-IT Security 21-112. The SAR deliverable is due two months prior to completion of the government fiscal year, ending on September 30. Due date is the last workday of July.

The SAR deliverable is due two months prior to completion of the government fiscal year, ending on September 30. Due date is the last workday of July.

38.5 Privacy Assessment Activities and Required Documentation

Assessment of the privacy posture of the non-federal system and its environment of operation will be through continuous monitoring of privacy controls to determine if they remain effective over time in light of changes that occur in the system and environment. Through continuous monitoring, privacy controls and supporting deliverables are updated and submitted to GSA per the schedules

below. The submitted deliverables (or lack thereof) provide a current understanding of the privacy risk posture of the information system(s). They allow GSA to make credible risk-based decisions regarding the continued protection of CUI residents in non-federal systems and initiation of appropriate responses as needed when changes occur.

Deliverables to be provided to the ISSO, ISSM, and/or COR every three years or when there is a major change to the system.

- Privacy Threshold Assessment (PTA)
  - Reference: NIST SP 800-171 Revision 2 Security Requirement 3.1.9 and 3.1.22
  - The contractor shall prepare a PTA to confirm and document whether Personally Identifiable Information (PII) is in scope or not, and to determine which other categories of CUI will be stored, processed, or transmitted by the system. The PTA must be completed before the Agency begins using the non-federal system.
- If through the initial PTA an Agency finds that no PII or other CUI is in scope, then vendor shall both:
  - Recertify the PTA every three years to confirm the absence of such sensitive information; AND
  - Update the PTA any time there is a change that may impact the privacy posture of the system or its environment of operation (e.g., collection of a new information type (see OMB Circular A-108, paragraph 6(b) for additional examples of significant changes requiring a PTA update).

If PII is in scope, deliverables to be provided to the ISSO, ISSM, and/or COR every three years or when there is a major change to the system.

- Privacy Impact Assessment (PIA)
  - Reference: NIST SP 800-171 Revision 2 Security Requirement 3.12.1[5]
  - For any system that collects, maintains, or disseminates PII or other CUI, a PIA must be completed by the contractor and provided to the Privacy Office for review. Then vendor shall:
    - Limit system access to those with a Lawful Government Purpose; display login notifications or warning banners that CUI is present in the system and must be protected consistent with the CUI Program;
    - Prohibit any CUI from being posted or processed on publicly accessible systems;
    - Recertify the PIA every three years to confirm the collection, maintenance, or dissemination of such sensitive information;
    - Update the PIA any time there is a change that may impact the privacy posture of the system or its environment of operation (e.g., collection of a new information type (see OMB Circular A-108, paragraph 6(b) for additional examples of significant changes requiring a PIA update).

OMB's PIA guidance: OMB Guidance for Implementing the Privacy Provisions of the EGovernment Act of 2002

If PII is in scope, the vendor shall include the following NIST SP 800-53, Revision 5 controls in its SSPP. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII.

- AC-3(14) Access Enforcement | Individual Access
- AC-21 Information Sharing
- PL-8 Security and Privacy Architectures
- PM-25 Minimization of Personally Identifiable Information Used in Testing, Training, and Research
- PM-26 Complaint Management
- PT-3 Personally Identifiable Information Processing Purposes
- PT-4 Consent
- PT-5 Privacy Notice
- RA-8 Privacy Impact Assessments
- SA-9 External System Services
- SI-12(2) Information Management and Retention | Minimize Personally
- Identifiable Information in Testing, Training, and Research
- SI-18 Personally Identifiable Information Quality Operations

A Privacy Policy/Notice shall be provided to users prior to their use of the application on what data is being collected and why, as well as the impact of not providing some or all of it. The Privacy Policy/Notice must be available to the individual directly on the form used to collect the information. Providing a link back to the Policy/Notice from the form is acceptable.

Other requirements: Government-approved terms of service.

38.6 Additional Stipulations

Security documentation will be marked as follows:

- PTAs and PIAs will not be marked.
- CP, BIA, and CP Test Reports will be marked CUI//EMGT.
- All other security documentation will be marked CUI//ISVI.
- Documents will be marked in bold text on the top of all pages. Spelling out of acronyms is not required.
- The cover page of each CUI document must contain the following statement on the lower left of the page.
    - Controlled by: General Services Administration OCISO ISP Division: ispcompliance@gsa.gov.
    - External transmission/dissemination of CUI to or from a government system must be encrypted. A FIPS PUB 140-3/140-2 validated encryption module must be used to encrypt the CUI data.

The Contractor shall comply with 52.204-23 of the Federal Acquisition Regulation (FAR). It prohibits under Section 1634 of Public Law 115-91 the use of any hardware, software, or services developed or provided, in whole or in part, by— (1) Kaspersky Lab (or any successor entity); (2) any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or (3) any entity of which Kaspersky Lab has majority ownership.

The Contractor shall comply with 52.204-25 of the FAR. It prohibits, under Section 889(a)(1)(A) of the John S. McCain National Defense Authorization Act for Fiscal Year 2019 (Pub. L. 115-232), contractors from providing to the Government any equipment, system, or service that uses telecommunications equipment or video surveillance services from certain named companies as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. It also prohibits, under Section 889(a)(1)(B), contractors from using any equipment, system, or service that uses telecommunications or video surveillance equipment or services from certain named companies as a substantial or essential component of any system or as critical technology as part of any system, unless an exception or waiver is granted per the FAR. The proscribed companies are Huawei Technologies Company, ZTE Corporation, Hytera Communications Corporation,

Hangzhou Hikvision Digital Technology Company, and Dahua Technology Company and their subsidiaries and affiliates.

The Contractor shall comply with 52.204-27 of the FAR. It prohibits under Section 102 of the Consolidated Appropriations Act 2023, Public Law 117-328, the presence or use of TikTok or any successor application or service developed or provided by ByteDance Limited or an entity owned by ByteDance Limited from being used on any information technology as defined in 40 U.S.C. § 11101(6) that is owned or operated by an agency, or used by a contractor under a contract with the agency, or requires the use of such technology expressly or to a significant extent in the performance of a service or the furnishing of a product for an agency.

---

[1] Nonfederal organizations that collect or maintain information on behalf of a federal agency or that use or operate a system on behalf of an agency, must comply with the requirements in FISMA of 2014, including the requirements in FIPS 200 and the security controls in NIST SP 800-53. (See [44 USC 3554] (a)(1)(A) and Section 2.1 for referenced documents).

[2] NIST has issued FIPS 140-3 and no longer accepts FIPS 140-2 modules for validation. However, previously validated 140-2 modules will be accepted through September 22, 2026. For additional information see the NIST Cryptographic Module Validation Program website.

[3] NIST has issued FIPS 140-3 and no longer accepts FIPS 140-2 modules for validation. However, previously validated 140-2 modules will be accepted through September 22, 2026. For additional information see the NIST Cryptographic Module Validation Program website.

[4] NIST has issued FIPS 140-3 and no longer accepts FIPS 140-2 modules for validation. However, previously validated 140-2 modules will be accepted through September 22, 2026. For additional information see the NIST Cryptographic Module Validation Program website.

[5] NIST SP 800-53 provides guidance on security and privacy controls for systems and organizations.