Enterprise Infrastructure Solutions (EIS)
Contract

Section G
Contract Administration Data

Issued by:

General Services Administration

Office of Information Technology Category

1800 F St NW

Washington, DC 20405

May 2024

Table of Contents

G.1 Introduction 1
G.2 Contract Administration 2
G.2.1 Government Points of Contact 2
G.2.2 Roles and Responsibilities 2
G.2.2.1 Agency Role 2
G.2.2.2 GSA Role 4
G.2.3 BSS Final Contract Acceptance 5
G.2.4 Contract Modification 5
G.2.5 Contract Closeout 6
G.2.6 Past Performance 6
G.3 Ordering 7
G.3.1 Fair Opportunity Process 7
G.3.1.1 eBuy 8
G.3.2 Task Orders 8
G.3.2.1 Task Order Award 9
G.3.2.2 Task Order Modification 9
G.3.2.3 Protests and Complaints 10
G.3.2.4 Customer of Record 11
G.3.2.5 Authorization of Orders 12
G.3.3 Ordering Services 13
G.3.3.1 General Requirements for Ordering Services 13
G.3.3.2 Order Types 14
G.3.3.3 Special Order Handling 17
G.3.4 Testing and Acceptance of Services Ordered 20
G.3.5 Performance Management 20
G.4 Billing 20
G.4.1 Billing Prerequisites 20
G.4.1.1 Billing Cycle 21

G.4.1.2 Billing Start Date and End Date 21
G.4.1.3 90-Day Billing Requirement 21
G.4.1.4 Unique Billing Identifier 21
G.4.1.5 Agency Hierarchy Code 22
G.4.1.6 Agency Service Request Number 22
G.4.1.7 Electronic Billing 22
G.4.2 Direct Billing 22
G.4.3 Billing Functional Requirements 23
G.4.3.1 Adjustments 23
G.4.3.2 Monthly Billing Informational Memorandum 23
G.4.4 Disputes 23
G.4.4.1 Billing Disputes Resolution 24
G.4.5 Payment of a Bill by the Government 24
G.4.6 Associated Government Fee 25
G.4.7 Electronic Funds Transfer 25
G.4.8 Government Purchase Card Payments 25
G.4.9 Rounding of Charges for Billing and AGF 25
G.4.10 Proration of Monthly Charges 25
G.4.11 Taxes, Fees and Surcharges 26
G.4.11.1 Separate Billing of Taxes, Fees and Surcharges 26
G.4.11.2 Aggregated Taxes 26
G.4.12 Billing Performance Objectives 26
G.4.12.1 Billing Data Accuracy Key Performance Indicator 26
G.4.12.2 Billing Charges Accuracy Key Performance Indicator 27
G.5 Business Support Systems 28
G.5.1 Overview 28
G.5.2 Reserved 28
G.5.3 Technical Requirements 28
G.5.3.1 Web Interface 28

G.5.3.2 Direct Data Exchange 29
G.5.3.3 Role Based Access Control (RBAC) 30
G.5.3.4 Data Detail Level 31
G.5.4 BSS Component Service Requirements 31
G.5.4.1 BSS Component Service Requirements Table 31
G.5.5 BSS Development 31
G.5.5.1 BSS Change Control 32
G.5.6 BSS Security Requirements 33
G.5.6.1 General Security Compliance Requirements 33
G.5.6.2 GSA Security Compliance Requirements 36
G.5.6.3 Security Assessment and Authorization (Security A&A) 37
G.5.6.4 BSS System Security Plan (BSS SSP) 37
G.5.6.5 Reserved 43
G.5.6.6 Additional Security Requirements 43
G.5.7 Data Retention 44
G.6 Service Assurance 45
G.6.1 Customer Support Office 45
G.6.2 Customer Support Office and Technical Support 45
G.6.3 Supply Chain Risk Management 46
G.6.3.1 Plan Submittal and Review 49
G.6.4 Trouble Ticket Management 49
G.6.4.1 Trouble Ticket Management General Requirements 49
G.6.4.2 Reporting Information 49
G.7 Inventory Management 51
G.7.1 Inventory Management Process Definition 51
G.7.1.1 Inventory Management Functional Requirements 51
G.7.1.2 EIS Inventory Maintenance 52
G.7.1.3 EIS Inventory Data Availability 52
G.7.1.4 EIS Inventory Data Discrepancies and Accuracy 53

G.7.1.5 EIS Inventory Reconciliation 54
G.8 Service Level Management 55
G.8.1 Overview 55
G.8.2 Service Level Agreement Tables 55
G.8.2.1 Service Performance SLAs 56
G.8.2.2 Service Provisioning SLAs 60
G.8.2.3 Billing Accuracy SLA 64
G.8.3 Service Level General Requirements 64
G.8.3.1 Measurement 64
G.8.3.2 Reporting 64
G.8.3.3 Credits and Adjustments 64
G.8.4 SLA Credit Management Methodology 65
G.8.4.1 Credit Management 65
G.8.5 Service Level Reporting Requirements 65
G.8.5.1 Report Submission 65
G.8.5.2 Report Definitions 66
G.9 Program Management 67
G.9.1 Contractor Program Management Functions 67
G.9.2 Performance Measurement and Contract Compliance 67
G.9.3 Coordination and Communication 67
G.9.4 Program Management Plan 69
G.9.5 Financial Management 71
G.9.6 Program Reviews 71
G.9.6.1 Quarterly Program Status Reports 71
G.10 Training 73
G.10.1 Training Curriculum 74
G.10.2 Training Evaluation 74
G.11 National Security and Emergency Preparedness 75
G.11.1 Basic Functional Requirements 75

G.11.2 Protection of Classified and Sensitive Information 77
G.11.3 Department of Homeland Security Office of Emergency Communications Priority Telecommunications Services 77
G.11.3.1 Government Emergency Telecommunications Service 77
G.11.3.2 Wireless Priority Service 78
G.11.3.3 Telecommunication Service Priority 78
G.12 Requirements for Climate Change Adaptation, Sustainability and Green Initiatives 80
G.12.1 Climate Change Adaptation 80
G.12.2 Sustainability and Green Initiatives 81
G.12.2.1 Electronic Product Environmental Assessment Tool 82
G.12.2.2 Energy Efficient Products 82
G.12.2.3 Data Centers and Cloud Services 83

G.1 Introduction

This section provides management and operational requirements for the Enterprise Infrastructure Solutions (EIS) contract. The functional areas covered include:

- Contract Administration
- Ordering
- Billing
- Business Support Systems
- Service Assurance
- Inventory Management
- Service Level Management
- Program Management
- Training
- National Security and Emergency Preparedness
- Requirements for Climate Change Adaptation, Sustainability and Green Initiatives

Additional requirements associated with this section related to data interchange, including deliverables and the data dictionary, are further defined in Section J.2 Contractor Data Interaction Plan.

For the purposes of this contract, all days are CALENDAR days unless otherwise specified.

G.2 Contract Administration

G.2.1 Government Points of Contact

The administration of this contract will require coordination between the government and the contractor. The following sections describe the roles and responsibilities of individuals who will be the points of contact for the government and the contractor on matters concerning contract administration.

G.2.2 Roles and Responsibilities

G.2.2.1 Agency Role

With regard to task orders (TOs), service orders and billing for services, agencies are responsible for:

1. Placing TOs according to FAR Subpart 16.505, and service orders in accordance with the terms and conditions of the contract.
2. Accepting or rejecting the services rendered by the contractor under TOs and service orders in accordance with Section E.2.2 EIS Services Verification Testing, and coordinating corrective actions with the contractor and GSA if required.
3. Coordinating resources and service providers to facilitate scheduling and communications for implementing and maintaining service. This includes:
    a) Identifying the agency's Local Government Contacts (LGCs) for each location involved in a particular project or other TO or service order activity, if possible.
    b) Monitoring and facilitating coordination between the contractor and LGC and other agency vendors and service providers as appropriate.
    c) Coordinating with users, and with other contractor(s) that are providing the location with telephone switching or other telecommunications facilities, upon notification by the contractor of changes regarding the date of scheduled activities or site requirements.
4. Paying the contractor for services provided.
5. Notifying the contractor of billing errors and facilitating the resolution thereof.
6. Additional roles and responsibilities contained in any Delegation of Procurement Authority (DPA) issued by a GSA Contracting Officer (GSA CO) to a warranted agency Ordering Contracting Officer or authorized official.
7. Additional roles and responsibilities contained in any Contracting Officer's Representative (COR) Designation Letter.

G.2.2.1.1 Task Order Authority / OCO

As described in Section G.3 Ordering, only a warranted contracting officer or other authorized official with authority to obligate funds for the agency (or tribe, or other entity authorized to use the contract per OGP 4800.2I) and who has been granted DPA by a GSA CO may issue or modify a TO under the contract. The contractor shall ensure that an OCO or an authorized official (hereinafter referred to as "OCO") has the required DPA prior to processing TOs; this information will be available to the contractor in GSA Systems.

G.2.2.1.2 OCO Duties

The OCO duties include, but are not limited to, those specified in the DPA in Attachment J.3 Delegation of Procurement Authority. The OCO for each TO may designate COR(s) authorized to place service orders specified in the TO.

Appointment and Training: The COR is a federal employee with Federal Acquisition Certification – Contracting Officer's Representative (FAC-COR) certification and complete contractor-provided training related to placement of service orders. If the agency does not use the FAC-COR certification process, the OCO may appoint an individual who is responsible for these duties. The COR will be delegated limited TO contract administration authority through a COR appointment letter by the OCO with DPA.

The COR duties may include, but are not limited to, the following tasks:

1. Understanding the contractor's service order procedures and being fully aware of the requirements and limits delegated by the OCO.
2. Placing service orders under a TO using the appropriate billing codes.
3. Accepting services ordered and verifying that services meet technical requirements.
4. Confirming funding availability prior to service ordering.
5. Coordinating with the appropriate budget and finance offices and the OCO to execute processes and internal controls to support funding availability and to comply with the Antideficiency Act (31. U.S.C 1341) and/or other applicable laws regarding funding.
6. Executing other duties related to ordering (e.g., billing disputes), as defined by the OCO.

G.2.2.2 GSA Role

GSA's primary role is contract administration. GSA is responsible for administering this contract and will modify the contract as necessary. In addition, GSA will:

1. Ensure compliance with contract requirements.
2. Delegate procurement authority to agencies to authorize OCOs to place TOs.
3. Place TOs on the agency's behalf, if so requested.
4. Assist in resolving conflicts between the contractor and the agency if necessary.

G.2.2.2.1 GSA Contracting Officer

The GSA CO has overall responsibility for administering the contract. The right to issue contract modifications, change the terms and conditions of the contract, terminate the contract, exercise option renewals, and approve subcontractors is reserved solely for the GSA CO unless otherwise delegated in writing. The GSA CO will be identified upon award.

The GSA CO is:

Joseph Brozi

Phone: 703-859-4603

joseph.brozi@gsa.gov

G.2.2.2.2 GSA Program Manager

The GSA Program Manager will provide central technical oversight and management regarding this contract to the contractor, GSA, and agency customers.

G.2.2.2.3 GSA Contracting Officer's Representative (COR)

A GSA COR will be designated by the GSA CO to monitor certain technical aspects of the contract. Actions within the purview of the GSA COR's authority include:

1. Ensuring that the contractor performs the technical requirements of the contract.
2. Performing or directing the inspections necessary to verify and validate service delivery specified under the contract.
3. Monitoring the contractor's performance under the contract, including SLA compliance, and notifying the contractor and the CO of any deficiencies observed.

A letter of delegation will be issued by the GSA CO to the GSA COR, with a copy supplied to the contractor, stating the COR's responsibilities and limitations.

The COR's authority does not include the ability to authorize work not already in the contract or to modify the terms and conditions of the contract.

The GSA COR is:

Trung Ngo

Phone: 703-306-6345

Email: trung.ngo@gsa.gov

G.2.2.2.4 GSA Customer Service Representative

The customer service representative for GSA is the Technology Service Manager (TSM), who works with agencies to inform them of contractor service offerings. The TSM's authority does not include the ability to authorize work not already in the contract or to modify the terms and conditions of the contract. The TSM assigned to an agency account provides customer support to ensure the agency's satisfaction with delivery, operation, maintenance, and billing of services.

G.2.2.2.5 Delegation of Procurement Authority

GSA establishes a DPA from the GSA CO to the OCO, and complies with the Office of Management and Budget's (OMB) Executive Agent designation to GSA. See Section J.3.

G.2.3 BSS Final Contract Acceptance

The contractor shall complete and pass the BSS validation testing, as stated in the contract, within 12 months from the acceptance of the BSS Verification Test Plan (see Section E.2.1). For the purposes of this section (G.2.3), BSS validation testing does not include completion of Assessment and Authorization (A&A) as referenced in Section E.2.1.2.2, Test Scenario BSS-TS13. If the contractor does not pass the BSS testing in the 12-month period, the government shall cancel the contract; however, the contractor will receive additional time due to delays caused by the government. The contractor shall not receive the Minimum Revenue Guarantee (MRG) stated in Clause H.3 if its contract is cancelled in accordance with this clause. The government shall not entertain any financial claim or settlement submitted by the contractor as a result of the contract being cancelled.

G.2.4 Contract Modification

A contract modification may be requested by GSA, the contractor, or an agency as described in Section J.4 Guidelines for Modifications to EIS Program Contracts.

G.2.5 Contract Closeout

Contract closeout will be accomplished within the guidelines set forth in:

- FAR Part 4.804 Closeout of Contract Files
- GSAM Subpart 504.804-5 Procedures for closing out contract files

G.2.6 Past Performance

In accordance with FAR 42.15 Contractor Performance Information, and individual agency policy, the OCO will prepare an evaluation of the contractor's performance for each TO that exceeds the simplified acquisition threshold of $250,000 using the Contractor Performance Assessment Reporting System (CPARS). CPARS allows the contractor to view and comment on the government's evaluation of the contractor's performance before it is finalized. Once the contractor's past performance evaluation is finalized in CPARS, it will be transmitted into the Past Performance Information Retrieval System (PPIRS) at http://www.ppirs.gov/.

G.3 Ordering

This section applies to all orders (services, equipment, and labor) under the contract. The contractor may only accept orders from entities listed in OGP 4800.2I Eligibility to use GSA Sources of Supply and Services.

The following steps are a high-level summary of the ordering process:

1. GSA establishes a DPA from the GSA CO to the OCO.
2. The OCO completes the fair opportunity process.
3. The OCO issues a TO that complies with FAR 16.505.
4. The OCO may appoint a COR(s) or other authorized ordering official on the TO to assist with the administration and placing of service orders.
5. Once the TO is awarded, the OCO completes account registration with the contractor.
6. Government may place service orders against the TO.

G.3.1 Fair Opportunity Process

Fair opportunity will be accomplished through an RFQ (Request for Quotation) or RFP (Request for Proposal). The RFQ/RFP can be as complex as an entire agency network or as simple as a comparison of existing priced CLINs.

The OCO will follow the fair opportunity procedures and exceptions specified in FAR 16.505, including but not limited to the following:

1. The OCO must provide each awardee a fair opportunity to be considered for each TO exceeding $3,500 unless one of the exceptions in FAR 16.505(b)(2) applies.
2. For fair opportunity for TOs from $3.5K - $250K, the OCO must provide each awardee a fair opportunity to be considered for each TO. If the order does not exceed the simplified acquisition threshold, the OCO need not contact each of the multiple awardees under the contract before selecting a TO awardee if the OCO has information available to ensure that each awardee is provided a fair opportunity to be considered for each TO.
3. For fair opportunity for TOs exceeding the simplified acquisition threshold (more than $250K and less than $5.5M), each TO shall be placed on a competitive basis in accordance with the following.
    a) Provide a fair notice of the intent to make a purchase, including a clear description of the supplies to be delivered or the services to be performed and

the basis upon which the selection will be made to all contractors offering the required supplies or services under the contract.

b) Afford all contractors responding to the notice a fair opportunity to submit an offer and have that offer fairly considered.

4. For fair opportunity for TOs exceeding $5.5 million, the contracting officer shall provide at a minimum:

   a) A notice of the TO that includes a clear statement of the agency's requirements.

   b) A reasonable response period (as defined by the OCO on the TO).

   c) Disclosure of the significant factors and sub-factors the agency expects to consider in evaluating proposals, including cost or price, and their relative importance.

   d) If award is made on a best value basis, a written statement documenting the basis for award and the relative importance of quality and cost or price.

   e) An opportunity for a post-award debriefing.

The OCO will include the evaluation procedures in the RFQ/RFP and establish the timeframe for responding, giving the contractor a reasonable proposal preparation time while taking into account any unique requirements and circumstances. All costs associated with the preparation, presentation, and discussion of the contractor's proposal in response will be at the contractor's sole and exclusive expense.

G.3.1.1 eBuy

The government may issue solicitations via GSA's eBuy (https://www.ebuy.gsa.gov). EBuy is an online RFQ/RFP tool designed to facilitate offerings for a wide range of supplies and services. EBuy allows the government to post requirements and obtain quotes/proposals. Posting on eBuy satisfies all requirements for providing fair opportunity notice to potential offerors, even if fewer than three offers are received. Use of the eBuy system fulfills the notification requirements in FAR 16.505.

Registration in eBuy is required to view and respond to solicitations in eBuy. After registration, the contractor is strongly encouraged to monitor eBuy frequently for opportunities. Industry partners will receive notices regarding opportunities in eBuy at their registered e-mail addresses. Contractors shall respond in the manner prescribed in the request. To respond to opportunities in eBuy, use https://www.ebuy.gsa.gov.

G.3.2 Task Orders

TOs will identify the services required and will provide specific technical details and scope of work required, including the schedule for all deliverables and the identification of any applicable equipment and labor categories, and service level performance. A TO

will still be required for low-value orders that are under the fair opportunity threshold (see Section G.3.1).

TOs may contain a combination of priced CLINs, Task Order Unique CLINs (TUCs), and Individual Case Basis (ICB) CLINs depending on agency-specific requirements for services, features, and performance. Agencies may require services that, although within the scope of the contract, are not available to order with priced CLINs.

TUCs are defined in Section B.1.2.2 and may be used to assist in defining special requirements for ordering and billing purposes or to combine multiple CLINs under a single overarching CLIN. TUC pricing submission details are described in Section J.4.1.

ICB CLINs are defined in Section B.1.2.14 and may be used to provide unique identifiers for services that are yet to be fully defined for a particular service under a specific TO. ICB CLINs are defined for various services on the contract (e.g., an OC-12 Access Arrangement) but require additional information to determine the price for the individual case and TO.

For each TO, the OCO is the sole and exclusive government official with authority to take actions that may bind the government. The OCO will have a DPA issued by GSA (see G.2.2.1.1 for the contractor's responsibilities regarding the DPA). The OCO may designate a COR or authorized ordering official to assist the OCO with administering the TO. The contractor shall not accept or bill the government for TOs or service orders from an unauthorized person.

TO modifications may be necessary during the TO period to address requirements or administrative changes. The OCO for each TO will administer the modifications for that TO. The contractor shall submit TO summary data and pricing tables, and shall forward copies of the complete TO as described in Section J.2.3 Task Order Data Management.

The contractor shall meet and comply with the processes, data and systems requirements to support and maintain TOs as described in Section J.2.3.

G.3.2.1 Task Order Award

All TOs awarded shall be placed directly by the OCO. Once awarded, the TO cannot be modified except by a TO modification.

G.3.2.2 Task Order Modification

Agencies that are subject to the federal acquisition regulation shall execute TO modifications in accordance with FAR Part 43.

The contractor shall report TO modifications to GSA as described in Section J.2.3 Task Order Data Management.

G.3.2.3 Protests and Complaints

Pursuant to FAR 16.505 (a)(9)(i) no protest is authorized in connection with the issuance or proposed issuance of an order under a TO contract, except for:

1. A protest on the grounds that the order increases the scope, period of performance, or maximum value of the contract.
2. A protest of an order valued in excess of $10 million.

G.3.2.3.1 Fair Opportunity Notice of Protest

Upon protesting a fair opportunity decision to the GAO, the agency, or an order ombudsman, the contractor shall provide a full un-redacted copy of that protest to the GSA CO within three (3) business days of the protest date. For FOIA requests the contractor shall provide a redacted copy to the GSA CO.

G.3.2.3.2 Task-Order and Delivery-Order Ombudsman Alt I

52.216-32 Task-Order and Delivery-Order Ombudsman (Sept 2019)

(a) In accordance with 41 U.S.C. 4106(g), the Agency has designated the following task-order and delivery-order Ombudsman for this contract. The Ombudsman must review complaints from the Contractor concerning all task-order and delivery-order actions for this contract and ensure the Contractor is afforded a fair opportunity for consideration in the award of orders, consistent with the procedures in the contract.

Maria Swaby

GSA Ombudsman

1800 F St NW, 2nd Floor

Washington, D.C. 20405

GSAOmbudsman@gsa.gov

202-208-0291

(b) Consulting an ombudsman does not alter or postpone the timeline for any other process (e.g., protests).

(c) Before consulting with the Ombudsman, the Contractor is encouraged to first address complaints with the Contracting Officer for resolution. When requested by the Contractor, the Ombudsman may keep the identity of the concerned party or entity confidential, unless prohibited by law or agency procedure.

(d) Contracts used by multiple agencies.

(1) This is a contract that is used by multiple agencies. Complaints from Contractors concerning orders placed under contracts used by multiple agencies are primarily reviewed by the task-order and delivery-order Ombudsman for the ordering activity.

(2) The ordering activity has designated the following task-order and delivery-order Ombudsman for this order:

[The ordering activity's contracting officer to insert the name, address, telephone number, and email address for the ordering activity's Ombudsman or provide the URL address where this information may be found.]

(3) Before consulting with the task-order and delivery-order Ombudsman for the ordering activity, the Contractor is encouraged to first address complaints with the ordering activity's Contracting Officer for resolution. When requested by the Contractor, the task-order and delivery-order Ombudsman for the ordering activity may keep the identity of the concerned party or entity confidential, unless prohibited by law or agency procedure.

G.3.2.4 Customer of Record

The government may place orders under this contract with:

1. GSA acting as customer of record on behalf of another agency
2. The agency itself acting as customer of record

3. GSA acting as an OCO for an agency with the agency remaining as the customer of record

The contractor shall support all options.

G.3.2.5 Authorization of Orders

A contractor may not accept, and the Government may not award, a task order until the apparent awardee has added all of the CLINs and prices at all locations requested in the agency's solicitation to their contract via fully executed modifications. Any task order issued prior to the execution of all aforementioned modifications will result in the OCO's DPA being revoked.

If a contractor does not have all mandatory services priced for a CBSA on its contract, and an agency issues a solicitation for a requirement in that CBSA, the contractor may not accept a TO or service order or provision services until all mandatory services for that CBSA have been added to its contract. If a contractor is missing a CBSA, the contractor may respond to a solicitation and then submit a modification for the missing CBSA in accordance with clause H.30 Expansion of Core Based Statistical Areas.

In addition to the CBSA requirement, if a contractor does not have a particular optional service on its contract, and an agency issues a solicitation including that service as a requirement, the contractor may submit a proposal or quote for the requirement provided it also submits a modification proposal to GSA to add the necessary services to its contract and so indicates in the solicitation. The contractor shall not accept a TO or service order or provision services not on its contract.

In both cases (a missing CBSA or missing service), the contractor shall include a clear notice of the pending modification in its response to the solicitation.

For catalog items, if the contractor requires a new discount class as defined in B.1.3.1, it must submit a modification proposal to GSA to add the necessary discount class. If an agency issues a solicitation including an item that the contractor has identified as requiring a new discount class, the contractor may submit a proposal or quote for the requirement provided it also submits the modification proposal to GSA to add the necessary discount class to its contract and so indicates the required modification in the solicitation. The contractor shall not accept a TO or service order or provision catalog items until the discount class has been added to the contract.

If a contractor does not have a particular item on its catalog and an agency issues a solicitation including that item as a requirement, the contractor may submit a proposal or

quote for the requirement. The contractor shall not accept a TO or service order or provision catalog items until the items have been added to the catalog.

G.3.3 Ordering Services

Within the limitations of the TO and the contract, the contractor shall accept orders for service incorporated directly within the TO or placed separately after the issuance of the TO. If an order for service incorporated directly within the TO is missing required data, with the exception of the data required in the TO as specified in Section G.3.2, the contractor shall accept supplemental information to complete the order.

This section describes the requirements for the placement, acceptance, and handling of all orders for service regardless of whether such orders are incorporated into the TO or placed separately after the issuance of the TO. In addition, process, data, and systems requirements for ordering service are described in Section J.2.4 Ordering.

Unless otherwise specified, all references to “orders” within this section refer to orders for service.

G.3.3.1 General Requirements for Ordering Services

G.3.3.1.1 Agency Hierarchy Code (AHC)

Orders submitted by the government will contain one or more Agency Hierarchy Codes (AHCs). The contractor shall reject any order submitted without an AHC for each line item. The contractor shall meet and comply with the AHC requirements as described in Section J.2.4.1.2 Agency Hierarchy Code.

G.3.3.1.2 Auto-Sold CLINs

If the contractor’s solution to an agency requirement includes services with one or more auto-sold CLINs, as described in Section B.1.2.11 Auto-Sold CLINs, the contractor shall include those CLINs in the proposal or quote as though they had been expressly requested and ensure they are on the TO. All auto-sold CLINs shall be listed in all notifications and deliverables associated with an order. The contractor may add new auto-sold CLINs to the contract with GSA approval via a contract modification. Such newly added auto-sold CLINs shall not be applicable to any previously issued TO unless specifically added via TO modification. If a TO modification is issued to add a new auto-sold CLIN, the contractor shall issue new Service Order Completion Notices (SOCNs) for all applicable previously provisioned orders under that TO.

G.3.3.1.3 Customer Want Date

The order for services may include a Customer Want Date (CWD), which indicates the customer's desired install date. The contractor shall make reasonable effort to accommodate the CWD. If the order includes a CWD, the following requirements apply:

1. The contractor shall not issue the SOCN nor begin billing prior to the CWD unless the order specifies that early installation is acceptable.
2. If the time between the order and the CWD is greater than the defined provisioning interval for the service as described in Section G.8.2.2, the service provisioning SLA is waived for that service on that order.

NOTE: CWD specifications do not apply to rapid provisioning orders as described in Section G.3.3.3.2.

G.3.3.1.4 Service Order Completion Notification (SOCN)

After completion of each service provisioning the contractor shall submit a SOCN as described in Section J.2.4. After an order has been provisioned and a SOCN submitted and accepted, no revisions to the SOCN are permitted unless one of the following applies: the customer submits an administrative change order, to correct an erroneous submission with the prior approval of the COR, or to add or remove an auto-sold CLIN.

G.3.3.2 Order Types

G.3.3.2.1 Orders for New Services

Orders for new services are defined as orders for services (CLINs) that are not currently being provided.

G.3.3.2.2 Orders to Change Existing Services

G.3.3.2.2.1 Move Orders

Move orders are defined as orders that require the removal of an existing service and/or Service Related Equipment (SRE) from one location and the re-installation of the identical service and/or SRE at another location.

G.3.3.2.2.2 Feature Change Orders

Feature change orders are defined as orders that require changes to the features of an existing service as described in Section B. They fall into two categories:

- Feature changes that require a change to the CLIN being billed
- Feature changes that do not require a change to the CLIN being billed

G.3.3.2.2.3 Disconnect Orders

Disconnect orders are defined as orders that require the removal of services (CLINs) currently being provided. The contractor shall accept disconnect orders from agencies at any time. Billing for the disconnected services shall stop on the completion date in the SOCN and within the provisioning intervals for disconnects as specified in Section G.8 Service Level Management.

Disconnect orders will include the customer's desired disconnect date. If the time between the order and the customer's desired disconnect date is greater than the defined provisioning interval for the service as described in Section G.8.2.2, the service provisioning SLA will be waived for that service on that order.

The government will automatically stop payment on these orders based on the stated disconnect date.

Equipment related to disconnect orders shall be removed within 45 days after the termination of services. For equipment sanitization, see Section C.1.8.7.1.

If a disconnect order includes the disconnection of services that appear to leave other services effectively unusable (e.g., disconnecting a circuit but not the associated equipment), the contractor shall notify the customer of the full list of associated Unique Billing Identifiers (UBIs). The contractor shall request clarification of the customer's intent to only disconnect the specified service. If the customer provides instructions indicating that the list, in whole or in part, is intended for disconnect, the contractor shall accept this as an order update.

G.3.3.2.2.4 Administrative Change Orders

The contractor shall accept administrative changes to previously provisioned orders. After updating its system, the contractor shall provide the updated information to GSA as described in Section J.2.4.

Changes to administrative data associated with existing services can only occur based on an administrative change order. Administrative data is limited to data provided by the government that does not impact service delivery or pricing.

G.3.3.2.3 Updates to In-Progress Orders

Within the limitations defined in the subsections below, order line items that have not completed the provisioning process may be updated by the government to accommodate the following situations:

- Cancel the Order
- Change Service Delivery Location

- Change Service Features
- Change the Customer Want Date (CWD)
- Change in Administrative Data

G.3.3.2.3.1 Cancel Orders

The contractor shall accept an order from an agency to cancel a pending order at any step of the order process prior to SOCN.

If a cancel order includes the cancellation of services that appear to leave other services effectively unusable (e.g., canceling a circuit but not the associated equipment), the contractor shall notify the customer of the full list of order line items that are associated. The contractor shall request clarification of the customer's intent to only cancel the specified order line items. If the customer provides instructions indicating that the list, in whole or in part, is intended for cancellation, the contractor shall accept this as an order update.

The contractor shall not charge the ordering agency for network access orders if the cancellation order was placed 30 or more days before the later of:

1. The CWD in the initial order, or
2. The firm order commitment date.

If the government's cancellation request does not meet the timeframe and requirements above, then the government shall pay the non-recurring charge (NRC) for the associated access arrangements using the cancellation CLIN described in Section B.4.1.13, even if it was previously waived by the contractor.

G.3.3.2.3.2 Location Change Updates

Location change updates are defined as order updates that change the service delivery location from that specified in the original order. They fall into two categories:

- Changes in service delivery location that impact LEC provisioning.
- Changes in service delivery location that do not impact LEC provisioning.

G.3.3.2.3.3 Feature Change Updates

Feature change updates are defined as order updates that require changes to the features of an existing service. They fall into two categories:

- Feature changes that require a change to the CLIN originally ordered.
- Feature changes that do not require a change to the CLIN originally ordered.

G.3.3.2.3.4 Customer Want Date Change Updates

Customer Want Date (CWD) updates are defined as order updates that change the customer want date from that specified in the original order. If the agency delays the CWD prior to receiving the Firm Order Commitment Notice (FOCN), the contractor shall not issue the SOCN and begin billing prior to the new CWD, unless the change requested is less than14 days before the CWD of the initial order.

G.3.3.2.3.5 Administrative Data Change Updates

The contractor shall accept administrative changes to in-progress orders.

Administrative data is limited to data provided by the government that does not impact service delivery or pricing.

G.3.3.3 Special Order Handling

G.3.3.3.1 Telecommunications Service Priority (TSP) Orders

1. The contractor shall meet and comply with the requirements for Telecommunications Service Priority (TSP) orders (see Section G.11 National Security and Emergency Preparedness).
2. When TSP is specified in the order, the contractor shall provide the service in accordance with the following telecommunication service priority levels:
   a) PROVISIONING PRIORITY (5, 4, 3, 2, 1, or E),
   b) RESTORATION PRIORITY (5, 4, 3, 2, or 1), or
   c) BOTH for both provisioning and restoration as specified in the order from Service Delivery Point to Service Delivery Point (SDP).
3. Restoration of service shall be in accordance with the TSP priority levels designated for the transmission service and in accordance with NCS Directive (NCSD) 3-1, TSP System for NS/EP and NCS Manual 3-1-1, “Service User Manual for the TSP System.”
4. Expedited service:
   a) The contractor shall provide expedited service implementation when the ordering agency requires priority provisioning for NS/EP circumstances or other circumstances in which the TSP system is invoked.
   b) The contractor shall make best effort to implement the ordered service(s) by the CWD, based on essential priorities as set certified by the DHS Program.

G.3.3.3.2 Rapid Provisioning Orders

Certain services, including self-provisioned services, lend themselves to rapid provisioning, which streamlines the provisioning process and only requires the Service Order Acknowledgement (SOA) and SOCN. If the contractor completes the provisioning process and issues a SOCN within twenty-four (24) hours of order submission, the SOA is not required.

An order is subject to rapid provisioning if all the following conditions apply:

1. The service ordered is specified as subject to rapid provisioning in the contract or the TO.
2. The order does not contain a TSP (see Section G.3.3.3.1).
3. The order does not contain an Administrative Change Order (see Section G.3.3.2.3.5).

As part of its proposal, the contractor shall specify which services it is offering as subject to rapid provisioning and the defined provisioning interval for each such service. The following restrictions apply to the contractor-defined provisioning intervals for rapid provisioning:

1. The provisioning interval shall not exceed 48 continuous hours.
2. The proposed provisioning interval shall be used to calculate SLA compliance as described in Section G.8.2.2.
3. Any CWD (see Section G.3.3.1.3) specified in the order does not apply, and early installation is acceptable.

G.3.3.3.3 Task Order Projects

The agency will indicate in the TO requirements whether the service orders under that TO are to be managed as a Task Order Project.

At the agency's discretion, upon award of the TO, the contractor shall prepare a Task Order Project Plan (TOPP). This plan identifies the contractor's project management processes, scheduling, procedures, tools, and implementation of the TO on the contractor's network. The contractor shall deliver the TOPP to the OCO of the TO (or service order) for approval and signature; the OCO's signature indicates agreement to the implementation schedule and as-of billing date for each item in the TO.

For each Task Order Project, the contractor shall provide the OCO with a single point of contact for service implementation. The contractor shall ensure that the point of contact or the designated alternate is accessible by telephone (office or mobile) or pager during the time periods when service implementation activities are taking place. The contractor shall coordinate with the OCO, customers, subcontractors, vendors, and other service providers during the service implementation. The contractor shall inform the OCO and

the LGC on the order when activities, including installation and cutover testing, are scheduled at a building. If the contractor changes the installation or activation date, the contractor shall notify the OCO and provide a revised date.

Unless the OCO requests an alternative outline, the contractor shall include in the TOPP at a minimum the following information, and any additional information the contractor deems appropriate:

1. Name and information for the contractor's primary point of contact for implementing the plan and coordinating with the agency as well as escalation contacts.
2. Name of the OCO who awarded the TO.
3. The TO number.
4. Description of the specific activities required by all parties, including the contractor, the agency, vendors, and the incumbent service provider, to implement the project.
5. Specification of government equipment (hardware/software) required by location for this project.
6. Key areas of risk for the specific project, the contractor's processes and procedures to minimize risk, and the contingency plan to fallback to previous services, if any, in the event of failure of newly installed services.
7. Comprehensive inventory of services to be implemented along with SDP, proposed activation date, as-of billing date, testing and acceptance timeframes by the contractor and by the customer, and approach to implementation, such as hot-cutover or parallel operation.
8. Installation and service implementation schedule and as-of billing dates.
9. If applicable, interconnectivity or network gateways required for the implementation.
10. Any special technical requirements.
11. A site-specific design plan to include:
    a) Site preparation and implementation requirements for each building. Identify where site surveys will be required, whether surveys will be conducted via physical site visits, telephonically, or other means, and what information will be collected. Indicate what the ordering agency's responsibilities will be for site surveys.
    b) Interim and final configuration to include hardware (type, manufacturer, model), software, special circuit arrangements, environmental and electrical

requirements, equipment room layouts, Main/Intermediate Distribution Frame / riser cable diagrams (if needed), and any special design requirements.

c) Numbering plan and dialing plan. Identify blocks of telephone numbers, if any, that will have to change.

d) Interface equipment for CPE, including identification and location of special systems integration requirements.

e) A site-specific cutover test plan that describes the contractor's general approach to cutover testing and pass/fail criteria for each service during service implementation as described here and in Section E Inspection and Acceptance.

G.3.4 Testing and Acceptance of Services Ordered

The contractor shall meet and comply with the requirements for the verification testing of all associated EIS services based on the methodology defined in Section E.2.2 EIS Services Verification Testing. The contractor shall also meet and comply with the criteria for acceptance testing defined by the agency on the TO.

G.3.5 Performance Management

For completion timeframes associated with orders for services as defined in Section G.3.3 Ordering Services, the contractor shall meet and comply with requirements for service provisioning intervals as defined in Section G.8 Service Level Management.

G.4 Billing

This section describes the billing process, which includes:

1. Submission of billing invoice data by the contractor (see FAR 2.101 for the definition of "invoice").
2. Verification and validation of billing by the government.
3. Resolution of any billing disputes and adjustments.

In addition to the billing functional requirements described herein, the contractor shall meet and comply with the processes, data, and systems interface requirements described in Section J.2.5 Billing.

G.4.1 Billing Prerequisites

The following information must be taken into consideration by the contractor to process and deliver billing details and adjustments.

G.4.1.1 Billing Cycle

The contractor shall comply with the government's billing period, which runs from the first through the last day of the calendar month. The contractor shall bill the government in arrears at the end of every month after providing services. All billing shall be rendered based on calendar month cycles.

G.4.1.2 Billing Start Date and End Date

The contractor shall submit the SOCN to the government prior to billing for the associated service. The SOCN contains the order completion date:

- For new services, this date is the billing start date
- For disconnected services, this date is the billing end date

Unless otherwise specified in the TO, the NRC price billed shall be that which was in effect at the time the service order was placed and the MRC shall be that which is in effect for the billing month.

The contractor shall begin billing both NRC and MRC on the billing start date with the following exceptions:

- The contractor shall not begin billing for services if the government rejects the services within three (3) days of receipt of the SOCN. A longer period for test and acceptance may be specified in the TO. If the SOCN is rejected, the contractor shall issue a new SOCN for services, with an updated order completion date, after correcting the reasons for rejection.
- A TO may also specify alternate billing start date requirements provided the adjustment does not violate the 90-day billing requirement described in Section G.4.1.3. In such cases, the contractor shall comply with the billing start date requirements specified in the TO.

G.4.1.3 90-Day Billing Requirement

The contractor shall submit a proper Billing Invoice (BI) deliverable (see Section J.2.5 Billing) for all services and SREs up to 90 days after issuance of the SOCN. The contractor shall not receive payment for a single billing charge or portion of a billing charge invoiced after 90 days. The OCO may waive this 90-day billing requirement on a case-by-case basis. This 90-day requirement applies to both initial invoicing and all billing adjustments.

G.4.1.4 Unique Billing Identifier

As described in Section J.2.5, the Unique Billing Identifier (UBI) shall be included on all billing. The contractor shall create and assign a UBI for each billed record and provide it

with each of the component(s) associated with the record to identify all components of a billed service.

G.4.1.5 Agency Hierarchy Code

Orders submitted by the government will contain an AHC as described in Section G.3 Ordering. The contractor shall include the AHC for each line item in all billing. The contractor shall meet and comply with the AHC requirements as described in Section J.2.4. The government will not pay the contractor for any order billed without an AHC for each line item.

G.4.1.6 Agency Service Request Number

Orders submitted by the government may contain one or two Agency Service Request Numbers (ASRNs). If provided by the government, the contractor shall include ASRN data in billing records throughout the service lifecycle as described in Section J.2.4.

G.4.1.7 Electronic Billing

The government intends to use electronic invoicing for all TOs. In addition to the billing deliverables described in Section J.2.5, the contractor shall input invoice summary data into a designated government system. The contractor shall support input into any of the following systems as specified by the GSA CO:

- WebVendor
- Vendor and Customer Self Service (VCSS) system
- Invoice Processing Platform (IPP)
- Other systems as specified in the TO

The contractor shall not submit and the government will not accept paper invoices except as authorized by the OCO.

G.4.2 Direct Billing

The contractor shall bill the agency directly for all charges incurred by the agency and its sub-agencies in accordance with the TO. The contractor will be paid directly by the agency.

The contractor shall be responsible for collecting the AGF and remittance of the total AGF amount collected for the month to GSA by electronic funds transfer (EFT).

G.4.3 Billing Functional Requirements

In addition to the functional requirements below, the contractor shall comply with the processes, deliverables and data exchange requirements for billing as defined in Section J.2.5 Billing.

The contractor shall respond within seven (7) days to a billing inquiry.

G.4.3.1 Adjustments

In the event it is necessary to adjust a bill, the contractor shall follow the adjustment process described in Section J.2.5 Billing. The contractor shall apply the adjustment to the next available bill. In the event of a dispute, the Billing Disputes process shall apply (see Section G.4.4).

G.4.3.2 Monthly Billing Informational Memorandum

The contractor shall provide, as needed, a Monthly Billing Informational Memorandum to coincide with the monthly delivery of billing files. The Monthly Billing Informational Memorandum is a list of information that includes, but is not limited to, items that explain changes in billing, changes to data formats, and new services added to the billing, and issues pertaining to balancing charges.

G.4.4 Disputes

The dispute process shall apply under any of the following conditions:

1. The government disputes the content of a BI submitted by the contractor.
2. The government disputes the content of an Inventory Reconciliation (IR) submitted by the contractor.
3. The government disputes a SLACR response submitted by the contractor.

The GSA CO, OCO, or authorized ordering official may submit to the contractor a dispute notice as defined in Section J.2.6 Billing & Inventory Disputes. The GSA CO or the OCO may designate additional personnel or systems authorized to submit a dispute notice.

The contractor shall accept and process the government's disputes. The contractor shall comply with the processes, deliverables, and data exchange requirements described in Section J.2.6 Billing & Inventory Disputes. The contractor shall resolve all disputes within 180 days of the dispute notice. The government reserves the right not to make payment for disputes that have not been resolved within 180 days.

The following section describes the billing dispute process.

G.4.4.1 Billing Disputes Resolution

Billing disputes begin with the initial submission of the dispute and end with the mutually agreeable resolution of the dispute. Payment adjustments will be applied on the next available bill. The government may reject a bill in whole or in part within seven (7) days of receipt. If only part of an invoice is in dispute, the government will pay the remainder of the bill and withhold only the disputed amount. Upon dispute resolution, the contractor shall submit corrected billing on the next available bill. For more information, see Section H.32 Payments and Incorrectly Invoiced Items and Prompt Payment Clause 52.232-25. The following requirements apply to billing dispute resolution:

1. The contractor shall resolve billing disputes with the agency that submitted the dispute.
2. The contractor shall work to resolve disputes within 180 days of the dispute notice.
3. In cases where a complete resolution is not forthcoming, the contractor may submit partial resolutions (less than the total amount in dispute) to the agency for acceptance or rejection. Accordingly, the OCO will respond within fourteen (14) days to the contractor's proposed resolution. Either party may escalate the dispute at any time to the OCO. In cases where the contractor and government agree on a portion of a dispute, the parties may make an adjustment to resolve the agreed-to portion(s) pending resolution of the remainder of the dispute.
4. Disputes that are not resolved within 180 days of the dispute notice or the approved extension time shall be escalated to the OCO.
5. Disputes escalated to an OCO will be resolved in accordance with FAR 52.233-1 (Disputes).
6. Once a dispute is resolved, the contractor shall process the associated adjustment ensuring that the debit or credit and the associated billing dispute identifier are clearly documented according to Section J.2.6 Billing & Inventory Disputes.
7. The contractor shall provide a monthly Dispute Report (DR) in accordance with Section J.2.6 Billing & Inventory Disputes.

G.4.5 Payment of a Bill by the Government

The contractor will be paid only for items and services that are issued, delivered, and accepted in accordance with this contract's ordering, billing, and payment procedures (see Section H.32 Payments and Incorrectly Invoiced Items).

Conditions of the government's acceptance of services are described in Section E.2.2 EIS Service Verification Testing. Billing shall be submitted monthly in accordance with Section G.4.1.7 Electronic Billing and Section J.2.5 Billing.

Upon the expiration of the contract or TO, the contractor shall submit a final billing invoice within 90 days unless the contractor requests and is granted an extension by the OCO in writing.

The government will start the Prompt Payment clock according to FAR Clause 52.232-25 when the detail billing has been delivered to the government (See Section G.4.2 Direct Billing).

G.4.6 Associated Government Fee

The contractor shall collect the AGF from customer agencies on a monthly basis throughout the life of the contract. The total amount of AGF collected for each month shall be remitted to GSA via EFT no later than 15th business day of the following month. See Section J.2.5 Billing for details including calculation methodology.

G.4.7 Electronic Funds Transfer

The contractor shall accept payment of bills via EFT. The contractor shall provide information required to receive payment via EFT.

G.4.8 Government Purchase Card Payments

The contractor shall accept payment via Government Purchase Card when authorized by the government for telecommunications purchases under this contract.

The contractor shall coordinate with its bank to obtain the appropriate Standard Industrial Classification code for the services provided under the contract and establish its Government Purchase Card financial procedures with its financial institution to ensure acceptance of such payments for billing.

G.4.9 Rounding of Charges for Billing and AGF

The contractor shall round billing in accordance with Section J.2.5.1.6 Rounding.

G.4.10 Proration of Monthly Charges

The contractor shall prorate billing based on the number of days that the service is provided during the billing period in accordance with Section J.2.5.1.5 Proration.

G.4.11 Taxes, Fees and Surcharges

G.4.11.1 Separate Billing of Taxes, Fees and Surcharges

The contractor shall separate billing amounts for taxes, fees and surcharges. Taxes, fees and surcharges shall be provided as individual components or amounts on the BI, whether they are part of an original charge or an adjustment.

The agency may elect to request prices that include all taxes, fees and surcharges in its solicitation (see Sections H.14 and H.23 for specific guidance). In this case, the contractor shall bill the prices that were proposed, accepted and included in the TO.

G.4.11.2 Aggregated Taxes

The contractor shall include the aggregated tax for each line item in the billing invoice and shall also provide the detailed composition of the aggregated tax in the tax detail deliverable (see Section J.2.5.1.7 Taxes, Fees and Surcharges).

G.4.12 Billing Performance Objectives

The contractor shall submit accurate billing that meets the following performance objectives for billing data accuracy and billing charge accuracy:

1. All applicable data elements shall be included on the BI in accordance with Section J.2.10 Data Dictionary.
2. The BI shall have an associated SOCN for each order.
3. The information on the BI shall be consistent with that on the SOCN.
4. There shall be no duplicate records within the BI.
5. There shall be no records within the BI that represent charges being billed more than 90 days after the issuance of the SOCN unless waived as described in G.4.1.3 (Note: this requirement applies to both initial invoicing and all billing adjustments).
6. The price shall match the price(s) on the contract or TO.

G.4.12.1 Billing Data Accuracy Key Performance Indicator

The Billing Data Accuracy Key Performance Indicator (KPI) measures the accuracy of the data submitted in the BI deliverable and is based on the accuracy standards listed above. KPI calculation is done on billing invoice after a six-month holding period to allow for resolution of any disputes. In the calculation below, “billing data submission” refers to an entire BI submission.

Billing Data Accuracy KPI is calculated in two steps:

1. Count the number of line items in the billing data submission that meet the above criteria.
2. Divide the result from Step 1 by the total number of line items in the billing data submission, and express the answer as a percentage.

The Acceptable Quality Level (AQL) is 95%.

G.4.12.2 Billing Charges Accuracy Key Performance Indicator

The Billing Charges Accuracy KPI measures the accuracy of the charges (prices) submitted in the BI deliverable. KPI calculation is done on billing invoice after a six-month holding period to allow for resolution of any disputes. In the calculation below, "billing data submission" refers to an entire BI submission.

Billing Charges Accuracy KPI is calculated in three steps:

1. For each line in the billing data submission, calculate the absolute value of the difference between the correct charge (C) and the submitted charge (S): |C – S|.
2. Calculate the sum of the individual line results from Step 1.
3. Divide the result from Step 2 by the absolute value of the total of the correct charges in the billing data submission, subtract from 1, and express the answer as a percentage.

The AQL is 95%.

G.5 Business Support Systems

G.5.1 Overview

To support this contract, the contractor shall have and maintain Business Support Systems (BSS). The contractor is encouraged to leverage its commercial systems to meet the BSS requirements. This requirement can be met by a single, integrated BSS or a combination of BSSs that meets the requirements specified in this section. The functions described below are the minimum that will require automation to meet the government's requirements for this contract.

G.5.2 Reserved

G.5.3 Technical Requirements

G.5.3.1 Web Interface

The contractor's BSS shall include a secure, user-friendly web interface suitable for human interaction with appropriate training as defined in Section G.10 Training. As noted in Section G.5.1 above, this requirement can be met with multiple web interfaces.

G.5.3.1.1 Web Interface Functions

At a minimum this interface shall support the following functions (see Section G.5.4 BSS Component Service Requirements for function explanations and references):

- Order Submission including Pricing Catalog.
- Trouble Ticketing.
- Inventory Management.
- Billing and Payment Management.

All other functions included in Section G.5.4 BSS Component Service Requirements are highly desired but not required.

G.5.3.1.2 Technology Standards

To the extent practical, the government desires a web interface solution that adheres to common industry standards. To that end, the web interface shall not require special software or plug-ins beyond standard web browsers with default built-in functionality. At a minimum, the following web browsers in their current and immediate previous versions (N-1) as well as any successor products shall be supported for all functions:

- Microsoft Edge (desktop and mobile).
- Google Chrome (desktop and mobile).
- Mozilla Firefox (desktop and mobile).

- Apple Safari (desktop and mobile).

G.5.3.1.3 Accessibility

The contractor's BSS supplied under this contract constitutes Electronic and Information Technology (EIT), as defined in FAR 2.101, and must conform to the Standards for Section 508 of the Rehabilitation Act at 36 C.F.R. § 1194.1 and Appendices A, C and D to Part 1194.

The contractor shall have readily available a comprehensive list of all offered EIT products (supplies and services) that fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Standards for Section 508 of the Rehabilitation Act at 36 C.F.R. § 1194.1 and Appendices A, C and D to Part 1194.The contractor shall also identify the technical standards applicable to all products proposed. In addition, the contractor shall clearly indicate where this list with full details of compliance can be found (e.g., an exact web page location). The contractor shall ensure that the list is available on the contractor's website(s) within 30 days of Notice to Proceed (NTP).

The contractor shall ensure that all EIT products that are less than fully compliant are offered pursuant to extensive market research, which ensures that they are the most compliant products available to satisfy the solicitation's requirements.

If any EIT product proposed is not fully compliant with all the standards, the contractor shall specify each specific standard that is not met, provide a detailed description as to how the EIT product does not comply with the identified standard(s), and indicate the degree of compliance.

The contractor shall make the BSS Voluntary Product Accessibility Template (VPAT) available on its website (See http://www.itic.org/policy/accessibility) and shall directly address compliance with Section 508 in the following deliverables:

- BSS Development and Implementation Plan

G.5.3.2 BSS Verification Test Plan Direct Data Exchange

The contractor's BSS shall include secure, automated mechanisms for direct transfer of detailed transaction data to the GSA Conexus. This data shall cover all elements detailed in Section G.5.4 BSS Component Service Requirements.

G.5.3.2.1 Direct Data Exchange Methods

The contractor's BSS shall initiate and process bidirectional automated exchange of management and operations data using the following methods:

- Web Services: Transactions over HTTPS via contractor Business to Business (B2B) Application Program Interfaces (APIs) for system-to-system data exchange between government and contractor systems. The contractor shall support XML over HTTPS using SOAP as the web services exchange mechanism. The transactions will be bi-directional. GSA Conexus will utilize X.509-based digital certificates to support mutual authentication and encryption, and HTTPS as the protocol for secure web services between contractor systems and GSA Conexus, observing the National Institute of Standards and Technology (NIST) SP 800-95 Guide to Secure Web Services as well as other references identified in NIST SP 800-53 R4 and GSA Web Application Security Guide 07-35.
- Secure File Transport Protocol (SFTP) Services: Transactions for file-based data exchange between government and contractor systems using government provided FTP service. The transactions will include transfer of data from the government to the contractor and from the contractor to the government.

Additional detail about the data exchange methods is specified in Section J.2.9.

G.5.3.2.2 Direct Data Exchange Formats

The contractor's BSS shall accept data transfers from the government and submit data to the government in the formats specified in Section J.2.9.

G.5.3.2.3 Direct Data Exchange Governance

GSA shall maintain and manage all approved data exchange format specifications, data schemas, and method descriptions. The government customer may specify additional data exchange requirements in the TO. Any changes or updates, to include timeframes for implementation, will be coordinated and negotiated between the government and the contractor.

Once the BSS is operational, the contractor shall not make any changes to the data exchange formats or methods without government approval via the established change control process (see Section G.5.5.1 BSS Change Control).

G.5.3.3 Role Based Access Control (RBAC)

The contractor shall collect user registration and RBAC information from the government customer. The contractor shall use this information to setup access control on its BSS as described in Section J.2.3.

G.5.3.4 Data Detail Level

The data provided by the BSS shall be sufficiently detailed to provide all data elements relating to the services listed in Section G.5.4 BSS Component Service Requirements as addressed in Section J.2.

As indicated in Section J.2, all BSS deliverables and reports shall be submitted in at least the following formats:

1. Human-Readable (see to J.2.9 for required file types) – made available via the web interface (Section G.5.3.1 Web Interface) unless otherwise specified in the TO.
2. Machine-Readable (see to J.2.9 for required file types) – as part of the direct data exchange described in Section G.5.3.2 Direct Data Exchange.

G.5.4 BSS Component Service Requirements

G.5.4.1 BSS Component Service Requirements Table

Service	Minimum Functionality	Specified in Section(s)
Customer Management	• User Training • Trouble Management	• Section G.10 Training • Section G.6.4.1 Trouble Ticket Management General Requirements
Financial Management	• Billing Management • Disputes • SLA Credit Management • Payment Management	• Section G.4 Billing • Section G.8 Service Level Management
Order Management	• Order Submission • Order Tracking	• Section G.3 Ordering
Inventory Management	• Inventory Management	• Section G.7 Inventory Management
Service Management	• Service Assurance • SLA Management	• Section G.6 Service Assurance • Section G.8 Service Level Management
Program Management	• Administration • Project Management • Reporting • Service Catalog	• Section G.9 Program Management • Section B.1.3 Catalog Pricing Requirements - General

G.5.5 BSS Development

The contractor shall submit a BSS Development and Implementation Plan with its proposal. This plan shall detail how the BSS to support the contract will be architected

and supported to meet GSA's requirements including the development timeline (if applicable).

Although the BSS is required to support this contract, the government will not pay for or otherwise finance the development or maintenance of the BSS. The contractor shall be solely responsible for all development, testing, and maintenance including, but not limited to, security validation, functional testing, and configuration control.

The contractor shall provide upgrades to its BSS at no additional cost to the government, as these upgrades become available to its commercial customers. BSS functional testing requirements are defined in Section E.2.1. BSS security testing requirements are defined in Section G.5.6.

G.5.5.1 BSS Change Control

A change to the BSS is subject to change control, as defined in this section, if it has an impact on any of the following:

- Web interface user experience that impacts Section 508 compliance (see Section G.5.3.1.3)
- Web interface user experience that requires additional training of government personnel
- Direct data exchange (see Section G.5.3.2.1)
- Ability of BSS to meet any specified requirements including those specified in a TO award
- System security

The contractor shall provide a BSS Change Control Notification to the government at least 30 days prior to all BSS changes regardless of their impact. In the event of an emergency change, the contractor shall notify the government as soon the contractor discovers that a change is required.

For those changes that meet the standard for being subject to change control, the contractor shall:

1. Obtain government approval before implementing the change.
2. Use industry-standard change control procedures.
3. Train government personnel if required.
4. Retest with the government to ensure functionality continues to meet requirements. Relevant BSS testing must be successfully completed for any new functionality that impacts GSA Conexus before it becomes operational.

5. Update all relevant service documents and information posted on the contractor's website(s) as necessary, at no additional cost to the government and within seven (7) days of completing the change.

G.5.6 BSS Security Requirements

The contractor shall ensure security requirements are met for the BSS as defined in the BSS System Security Plan (BSS SSP) (see Section G.5.6.4), at a Moderate impact level and shall support government security and authorization efforts. The contractor shall also support the government's efforts to verify that these standards are being met.

G.5.6.1 General Security Compliance Requirements

In providing services under this contract, the contractor shall be subject to all current applicable federal and agency-specific IT security directives, standards, policies, and reporting requirements. The contractor shall comply with Federal Information Security Management Act (FISMA) guidance and directives to include Federal Information Processing Standards (FIPS), NIST Special Publication (SP) 800 series guidelines (see http://csrc.nist.gov/), GSA IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of government IT. Compliance references shall include:

- Federal Information Security Management Act (FISMA) of 2002, available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.) available at: https://www.congress.gov/113/bills/s2521/BILLS-113s2521es.pdf.
- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996," available at: https://www.fismacenter.com/clinger%20cohen.pdf.
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and contractors," August 27, 2004; available at: http://www.idmanagement.gov/.
- OMB Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/.
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies." (Available at: http://www.whitehouse.gov/omb/memoranda_2004).

- OMB Memorandum M-05-24, “Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors.” (Available at https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf.)
- OMB Memorandum M-11-11, “Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors.” (Available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.)
- OMB Memorandum M-14-03, “Enhancing the Security of Federal Information and Information Systems.” (Available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.)
- 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 140-2, “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 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.”
- NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View.”
- NIST SP 800-41, Revision 1, “Guidelines on Firewalls and Firewall Policy.”
- NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems.”
- NIST SP 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations.”

- NIST SP 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.”
- NIST SP 800-61, Revision 2, “Computer Security Incident Handling Guide.”
- NIST SP 800-88, Revision 1, “Guidelines for Media Sanitization.”
- NIST SP 800-128, “Guide for Security-Focused Configuration Management of Information Systems.”
- NIST SP 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations.”
- NIST SP 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.”
- “IT Security Procedural Guide: External Information System Monitoring CIO-IT Security-19-101”

In addition to complying with the requirements identified in the government policies, directives and guides specified above, the contractor shall comply with the current GSA policies, directives and guides listed below (the current documents are referenced within the GSA IT Security Policy and are available upon request submitted to the GSA CO*)*:

- GSA Information Technology (IT) Security Policy, CIO P 2100.1M.
- GSA Order CIO P 2181.1 “GSA HSPD-12 Personal Identity Verification and Credentialing Handbook.”
- GSA Order CIO 2104.1, “GSA Information Technology (IT) General Rules of Behavior.”
- GSA Order CPO 1878.1, “GSA Privacy Act Program.”
- GSA IT Security Procedural Guide 01-01, “Identification and Authentication.”
- GSA IT Security Procedural Guide 01-02, “Incident Response.”
- GSA IT Security Procedural Guide 01-05, “Configuration Management.”
- GSA IT Security Procedural Guide 01-07, “Access Control.”
- GSA IT Security Procedural Guide 01-08, “Audit and Accountability Guide.”
- GSA IT Security Procedural Guide 05-29, “IT Security Training and Awareness Program.”

- GSA IT Security Procedural Guide 06-29, “Contingency Planning Guide.”
- GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.”
- GSA IT Security Procedural Guide 06-32, “Media Protection Guide.”
- GSA IT Security Procedural Guide 07-35, “Web Application Security Guide.”
- GSA IT Security Procedural Guide 08-39, “FY 2014 IT Security Program Management Implementation Plan.”
- GSA IT Security Procedural Guide 10-50, “Maintenance Guide.”
- GSA IT Security Procedural Guide 11-51, “Conducting Penetration Test Exercise Guide.”
- GSA IT Security Procedural Guide 12-63, “GSA’s System and Information Integrity.”
- GSA IT Security Procedural Guide 12-64, “Physical and Environmental Protection.”
- GSA IT Security Procedural Guide 12-66, “Continuous Monitoring Program.”
- GSA IT Security Procedural Guide 12-67, “Securing Mobile Devices and Applications Guide.”
- GSA IT Security Procedural Guide 14-69, “SSL / TLS Implementation Guide.”
- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing December 2011.
- The Committee on National Security Systems Instruction (CNSSI) No. 5000, “Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony,” October 17, 2016.

G.5.6.2 GSA Security Compliance Requirements

FIPS 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 eighteen security-related areas. Contractor systems supporting GSA must meet the minimum security requirements through the use of the security controls in accordance with NIST SP 800-53 R4.

To comply with the federal standard, GSA has determined the security category of the information and information system in accordance with FIPS 199, “Standards for Security Categorization of Federal Information and Information Systems,” to be

established at the Moderate Impact Level and baseline security controls must be established as identified in NIST SP 800-53 R4 and other associated directives and guides identified and/or provided by GSA. The contractor shall submit a Risk Management Framework Plan describing its approach for BSS security compliance. This plan shall be submitted with the proposal in accordance with NIST SP 800-37. (Reference: NIST SP 800-37 R1, and NIST SP 800-53 R4: SA-3, RA-3).

G.5.6.3 Security Assessment and Authorization (Security A&A)

The implementation of an IT system to process federal government data requires a formal approval process known as Assessment and Authorization (A&A). NIST SP 800-37, Revision 1 (hereinafter listed as NIST SP 800-37) and GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk," provides guidance for performing the security A&A process. The contractor's system must have a valid security A&A prior to being placed into operation and processing government information. Failure to maintain a valid security A&A will be grounds for termination of the contract. The system must have a new security A&A conducted at least every three (3) years, or when there is a significant change that impacts the system's security posture.

G.5.6.4 BSS System Security Plan (BSS SSP)

The contractor shall comply with all security A&A requirements as mandated by federal laws, directives and policies, including making available any documentation, physical access, and logical access needed to support this requirement. The level of effort for the security A&A is based on the system's NIST FIPS Publication 199 categorization. The BSS SSP shall be completed in accordance with NIST SP 800-18, Revision 1 (hereinafter listed as NIST SP 800-18) and other relevant guidelines. The BSS SSP for the information system shall initially be completed and submitted within 30 days of the NTP to include annual updates (Reference: NIST SP 800-53 R4: PL-2). At a minimum, the contractor shall create, maintain and update the following security A&A documentation:

1. The contractor shall develop and maintain a Security Assessment Boundary and Scope Document (BSD) as identified in NIST SP 800-37. This document will be used to determine the actual security assessment boundary. The set of information resources allocated to an information system defines the boundary for that system. These resources support the same mission/business objectives or functions. Generally the set of information resources is located within the same operating environment; however, distributed systems can reside in various locations with similar operating environments. Establishing and/or changing information system security boundaries is a cooperative effort between the federal government and the contractor. A template is available in Section J.8.

The BSD for the information system shall intially be completed and submitted within 15 days of the NTP to include annual updates. (Reference: NIST SP 800-37 R1).

2. The contractor shall develop and maintain Interconnection Security Agreements (ISA) developed in accordance with NIST SP 800-47. The contractor shall provide any ISAs for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CA-3).
3. The contractor shall develop and maintain a GSA NIST SP 800-53 R4 Control Tailoring Workbook as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” A template is included in Section J.8. Column E of the workbook titled “Contractor Implemented Settings” shall document all contractor-implemented settings that are different from GSA-defined settings, and where GSA-defined settings allow a contractor to deviate. The contractor shall provide a Control Tailoring Workbook for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: AC-1).
4. The contractor shall develop and maintain a GSA Control Summary Table for a Moderate Impact Baseline as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” A template is provided in Section J.8. The contractor shall provide a GSA NIST SP 800-53 R4 Control Summary Table for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: AC-1).
5. The contractor shall develop and maintain a Rules of Behavior (RoB) for information system users as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk” and GSA Order CIO 2104.1, “GSA IT General Rules of Behavior.” The contractor shall provide an RoB for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: PL-4).
6. The contractor shall develop and maintain a System Inventory that includes hardware, software and related information as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” The contractor shall provide a System Inventory for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CM-8).
7. The contractor shall develop and maintain a Contingency Plan (CP) including Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA) completed in agreement with NIST SP 800-34. The contractor shall provide a

CP, DRP, and BIA for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CP-2).

8. The contractor shall develop and maintain a Contingency Plan Test Plan (CPTP) completed in agreement with GSA IT Security Procedural Guide 06-29, “Contingency Planning Guide.” The contractor shall provide an CPTP for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CP-4).
9. The contractor shall test the CP and document the results in a Contigency Plan Test Report (CPTR), in agreement with GSA IT Security Procedural Guide 06-29, “Contingency Planning Guide.” The contractor shall provide a CPTR for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CP-4).
10. The contractor shall perform a Privacy Threshold Assessment (PTA)/Privacy Impact Analysis (PIA) completed as identified in GSA IT Security Procedural Guide 06-30, Managing Enterprise Risk. The contractor shall provide a PTA/PIA for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: AR-2, AR-3 and AR-4).
11. The contractor shall develop and maintain a Configuration Management Plan (CMP) (Reference: NIST SP 800-53 R4 control CM-9; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall provide a CMP for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: CM-9).
12. The contractor shall develop and maintain a System(s) Baseline Configuration Standard Document (Reference: NIST SP 800-53 R4 control CM-2; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall provide a well defined, documented, and up-to-date specification to which the information system is built. The contractor shall provide the System Baseline Configuration for the information system as a part of the CMP and shall be submitted with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CM-9).
13. The contractor shall develop and maintain System Configuration Settings (Reference: NIST SP 800-53 R4 control CM-6; NIST SP 800-128; GSA CIO-IT Security 01-05). The contractor shall 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 shall be configured in accordance with GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines (Level 1), or industry best practices in hardening systems, as deemed appropriate by the AO. System configuration settings shall be included as part of the Configuration Management plan and shall be updated and/or reviewed on an annual basis. (Reference: NIST SP 800-53 R4: CM-9).

14. The contractor shall develop and maintain an Incident Response Plan (IRP) (Reference: NIST SP 800-53 R4 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”). The contractor shall provide an IRP for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: IR-8).
15. The contractor shall test the IRP and document the results in an Incident Response Test Report (IRTR) (Reference: NIST SP 800-53 R4 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”). The contractor shall provide an IRTR for the information system with the initial security A&A package to include annual updates. (Reference: NIST SP 800-53 R4: IR-3).
16. Maintenance of the system security will be through continuous monitoring of security controls of the contractor’s system and its environment of operation to determine if the security controls in the information system continue to be effective over time and as changes occur in the system and environment. The contractor shall develop and maintain a Continuous Monitoring Plan to document how continuous monitoring of information system will be accomplished. Through continuous monitoring, security controls and supporting deliverables shall be updated and submitted to GSA per the schedules below. The submitted deliverables provide a current understanding of the security state and risk posture of the information systems. They allow GSA authorizing officials to make credible risk-based decisions regarding the continued operations of the information systems and initiate appropriate responses as needed when changes occur.
17. The contractor shall develop and maintain a Plan of Action and Milestones completed in agreement with GSA IT Security Procedural Guide 06-30, “Plan of Action and Milestones (POA&M).” All scans associated with the POA&M shall be performed as an authenticated user with elevated privileges. Vulnerability scanning results shall be managed and mitigated in the POA&M and submitted together with the quarterly POA&M submission. (Reference: NIST SP 800-53 R4; RA-5 and GSA CIO-IT Security Guide 06-30). Scans shall include all networking components that fall within the security accreditation boundary. The appropriate

vulnerability scans are also submitted with the initial security A&A package. An annual information system User Certification/Authorization Review must be annotated on the POA&M. A POA&M template is provided in Section J8. The contractor shall provide a POA&M for the information system as part of the initial security A&A package followed by quarterly updates. (Reference: NIST SP 800-53 R4; CA-5).

18. All FIPS 199 Low, Moderate and High impact information systems must complete an independent internal and external penetration test and provide an Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities with the security assessment package and on an annual basis in accordance with GSA CIO-IT Security Guide 11-51. GSA will provide for the scheduling and performance of these penetration tests. All penetration test exercises must be coordinated through the GSA Office of the Chief Information Security Officer (OSISO) Security Engineering (ISE) division at itsecurity@gsa.gov per GSA CIO-IT Security Guide 11-51. (Reference: NIST SP 800-53 R4; CA-5 and RA-5).
19. All FIPS 199 Low, Moderate, and High impact information systems must conduct code analysis reviews in accordance with GSA CIO Security Procedural Guide 12-66 using the appropriate automated tools (e.g., Fortify, Veracode, etc.) to examine for common flaws, and document results in a Code Review Report to be submitted prior to placing system into production, when there are changes to code and on an annual basis. Applicable NIST SP 800-53 R4 Control is SA-11. References: GSA CIO Security Procedural Guides 06-30, “Managing Enterprise Risk” and GSA CIO Security Procedural Guide 12-66, “Continuous Monitoring Program.” If applicable, a Code Review Report shall be submitted as an initial deliverable prior to placing the information system into production, when there are changes to code and on an annual basis. (Reference: NIST SP 800-53 R4: SA-11).
20. The government is responsible for providing the Security/Risk Assessment and Penetration Tests. The contractor shall allow GSA employees (or GSA-designated third-party contractors) to conduct security A&A activities to include control reviews in accordance with NIST SP 800-53 R4 / NIST SP 800-53A R4 and GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” 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 government information. This includes the general support system infrastructure. All scans must be performed as an authenticated user with elevated privileges.

21. All identified gaps between required 800-53 R4 controls and the contractor's implementation as documented in the Security/Risk Assessment Report (SAR) shall be tracked by the contractor for mitigation in a POA&M document completed in accordance with GSA IT Security Procedural Guide 09-44, "Plan of Action and Milestones (POA&M)."
22. The contractor shall mitigate all security risks found during the security A&A and continuous monitoring activities. All critical and high-risk vulnerabilities shall be mitigated within 30 days and all moderate risk vulnerabilities shall be mitigated within 90 days from the date vulnerabilities are formally identified. The government will determine the risk rating of vulnerabilities. Updates shall be provided on a monthly basis on the status of all critical and high vulnerabilities that have not been closed within 30 days.
23. The contractor shall deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, "FISMA Implementation." Each fiscal year the annual assessment will be completed in accordance with instructions provided by GSA. (Reference: NIST SP 800-53 R4: CA-2).
24. The contractor shall develop and keep current all policy and procedures documents, as outlined in the specified NIST documents as well as appropriate GSA IT Security Procedural Guides . The following documents shall be verified and reviewed during the initial security assessment and updates provided to the GSA COR/ISSO/ISSM biennially:
    a) Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1).
    b) Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1).
    c) Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1).
    d) Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1).
    e) Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1).
    f) Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1).
    g) Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1).
    h) Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1).
    i) System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1).
    j) Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1).

k) Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1).
l) Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1).
m) Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1).
n) Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1).
o) Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 R4: SA-1).
p) System and Communication Protection Policy and Procedures (NIST SP 800-53 R4: SC-1).
q) System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1).

G.5.6.5 Reserved

G.5.6.6 Additional Security Requirements

The contractor shall ensure that proper privacy and security safeguards are adhered to in accordance with the FAR Part 52.239-1, see Section I.

The deliverables identified in Section G.5.6.4 shall be labeled “CONTROLLED UNCLASSIFIED INFORMATION” (CUI) or contractor-selected designation per document sensitivity. External transmission/dissemination of Controlled Unclassified Information (CUI) data to or from a GSA computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, “*Security Requirements for Cryptographic Modules.*”

Where appropriate, the contractor shall ensure implementation of the requirements identified in the FAR (see Section I, 52.224-1, “*Privacy Act Notification*” and FAR 52.224-2, “*Privacy Act*.”)

The contractor shall cooperate in good faith in defining non-disclosure agreements 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 contractor’s IT environment being used to provide or facilitate services for the government. In accordance with the FAR (see Section I, 52.239-1) the contractor shall be responsible for the following privacy and security safeguards:

1. The contractor shall not publish or disclose in any manner, without the CO’s written consent, the details of any safeguards either designed or developed by the contractor under this contract or otherwise provided by the government (except for disclosure to a consumer agency for purposes of security A&A verification).

2. To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public government data collected and stored by the contractor, the contractor shall provide the government logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods:
    - Authenticated and unauthenticated operating system/network vulnerability scans
    - Authenticated and unauthenticated web application vulnerability scans
    - Authenticated and unauthenticated database application vulnerability scans
    - Internal and external penetration testing
3. 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 contractor 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 (See GSA Security Guide 6-30 "Managing Enterprise Risk" for acceptance criteria). In these cases, scanning tools and their configurations shall be approved by the government. In addition, the results of contractor-conducted scans shall be provided, in full, to the government.

G.5.6.6.1 Personnel Security Suitability

The contractor shall perform personnel security/suitability in accordance with FAR Part 52.204-9, see Section I.

All contractor personnel with access to government information that is within the security A&A scope must successfully complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12), OMB guidance M-05-24, M-11-11 and as specified in GSA CIO Order 2100.1J and GSA Directive 9732.1D Suitability and Personnel Security.

The government shall be responsible for the cost of such background investigations.

G.5.7 Data Retention

The contractor shall comply with FAR Subpart 4.7 (48 CFR 4.7), to maintain an archive of all records for three (3) years after final payment under the contract.

G.6 Service Assurance

This section describes the requirements for the following Service Assurance functions:

- Customer support
- Supply Chain Risk Management (SCRM)
- Trouble ticket management

G.6.1 Customer Support Office

The contractor's Customer Support Office (CSO) will be the primary interface between the contractor and government entities interested in or using the contract. The contractor shall identify the structure of the CSO to the government in the contract. The CSO shall support the contractor's sales, service and implementation activities with the government. The CSO will be set up to communicate with government users of the contract around the world using common means of communications including toll-free number, email, and collaboration tools.

The CSO shall assist users experiencing difficulty and shall provide training as required. The contractor shall also make Customer Service Representatives (CSRs) available to users for requirements planning or billing reconciliation.

G.6.2 Customer Support Office and Technical Support

The contractor's CSO shall be located at premises provided by the contractor and shall provide basic operation at contract award, with a main toll-free telephone number and primary email address. The contractor shall have all functional areas of the CSO fully operational within 30 days of NTP. The contractor's CSO shall:

1. Facilitate the government's use of the contract.
2. Provide contact information for each functional area of the CSO.
3. Respond to general inquiries.
4. Provide information regarding available products and services, respond to service inquiries, and accept orders.
5. Provide training registration and scheduling information.
6. Respond to inquiries via the same method the user used to access the CSO, unless otherwise specified by the user.
7. Provide a main US toll-free telephone number through which all CSO functional areas can be accessed.

8. Provide the capability for non-domestic users to contact the CSO without incurring international charges and minimize, to the extent possible, the different CSO contact numbers required to support non-domestic users.
9. Provide hot-links from the contractor's public EIS website(s) to CSO functional area email addresses.
10. Provide Telecommunications Device for the Deaf (TDD) access to the CSO for government representatives who are hearing impaired or have speech disabilities.
11. Deal effectively with the geographical distribution of EIS subscribing agencies, GSA's Program Management Offices (PMOs) in the GSA regions, and GSA international activities.
12. Provide responses to user inquiries of a general nature such as the contractor's established administrative and operational procedures, contractor points of contact, and user forum information.
13. Provide information on available training classes as well as guidance and assistance with registration for training classes. Training requirements are described in G.10 Training.
14. Provide technical support to agencies and the PMO regarding the services the contractor delivers to the government. Technical support shall include, but not be limited to:
    a) Answering questions related to how users can obtain the functions designed into the services the contractor provides via the contract
    b) Advising users on the capabilities incorporated into service features
    c) Providing technical support to assist either the contractor technicians or the agencies or other organizations or personnel in the timely resolution of troubles
    d) Notifying users of new services and features that are planned or that have recently been added to the contract
    e) Providing ordering and tracking support services
    f) Providing support to help resolve billing issues
    g) Providing inventory management support

G.6.3 Supply Chain Risk Management

The contractor shall include a SCRM Plan with its proposal that addresses counterfeit and illegally modified products. The SCRM plan shall describe the contractor's

approach to SCRM and demonstrate how the contractor's approach will reduce and mitigate supply chain risks.

The contractor shall provide a SCRM plan to manage supply chain risk throughout each of the five (5) supply chain phases specified in its proposal: 1) design and engineering, 2) manufacturing and assembly, 3) distribution and warehousing, 4) operations and support, and 5) disposal and return. In addition to the components and processes for which the contractor is directly responsible, and as feasible, the contractor shall identify "specified supporting infrastructure beyond the system boundary" and where appropriate, include such infrastructure in its SCRM Plan.

The SCRM Plan shall address at a minimum, but not be limited to, the following:

1. How the contractor ensures that requirements for genuine Information Technology Tools (ITT) are imposed upon its direct suppliers, whether the direct supplier is a systems integrator, reseller or OEM. The requirements for assurance and supporting evidence must include:
    a) The contractor performs reasonable steps to ensure its SCRM Plan is performed for ITT in its delivered and installed configuration.
    b) Equipment resellers from whom the contractor purchases ITT have valid licenses for OEM equipment and software.
    c) The ITT OEM exercises strict quality control to ensure that counterfeit or illegally modified hardware or software components are not incorporated into the OEM product.
    d) The contractor ensures traceability of assurance and evidence of genuineness of ITT back to the licensed product and component OEMs.
2. The contractor's use of system security engineering processes in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities.
3. The contractor's strategy for implementing SCRM security requirements throughout the life of the contract. The SCRM plan shall address the security controls described in NIST SP 800-53 R4 or the latest publication. Implementation of the controls shall be tailored in scope to the effort and the specific information.
4. The criticality analysis (CA) process used by the contractor to determine Mission Critical Functions and the protection techniques (countermeasures and sub-countermeasures) used to achieve system protection and mission effectiveness. The CA shall describe the contractor's supply chain for all critical hardware and software components (and material included in products), key suppliers, and

include proof of company ownership and location (on-shore or off-shore) for key suppliers and component manufacturers.

5. How the contractor will ensure that products and components are not repaired and shipped as new products and components provided to the government.
6. How the contractor will ensure that supply channels are monitored for counterfeit products throughout the product life cycle to include maintenance and repair.
7. How the contractor's physical and logical delivery mechanisms will protect against unauthorized access, exposure of system components, information misuse, unauthorized modification, or redirection.
8. How the contractor's operational processes (during maintenance, upgrade, patching, element replacement, or other sustainment activities) and disposal processes will limit opportunities for knowledge exposure, data release, or system compromise.
9. Which of the following identifies the relationship between the contractor and the manufacturer: 1) OEM, 2) authorized reseller, 3) authorized partner/distributor, or 4) unknown/unidentified source.
10. The contractor's expressed warranty that the software shall be free from all computer viruses, worms, trojans, time-outs, time bombs, back doors, disabling devices and other harmful or malicious code intended to or which may damage, disrupt, inconvenience or permit access to the software user's or another's software, hardware, networks, data or information. The government will only accept standard commerical warranties for Commerical-Off-the-Shelf (COTS) components only if they are consistent wtih clause 52.246.17. In the case of standard commerical warranties that exceed one year, the government shall receive the additional term(s) of the commerical warranty.
11. How the contractor will ensure independent verification and validation of assurances, and provide supporting evidence as required.

The contractor shall incorporate the substance of this clause in subcontracts at all tiers where a subcontractor provides personnel, components, or processes identified as 1) a critical component, or 2) part of the contractor's supporting infrastructure. All subcontractors providing critical components or services shall be identified and required to provide all necessary information to complete the SCRM Plan in association with the contractor. Suppliers of COTS components are considered subcontractors for this contract.

The contractor shall comply with NIST SP 800-161 Supply Chain Risk Management (SCRM) Practices. The offeror shall update its SCRM Plan to include any future

changes to the NIST SCRM Guidelines and all such modifications to the Plan shall be made at no cost to the government.

G.6.3.1 Plan Submittal and Review

The plan shall be submitted with the contractor's proposal. Updates shall be submitted on an annual basis to the CO and COR. All information included will be treated as Controlled Unclassified Information pursuant to Executive Order 13556, shared only with government agencies, and used solely for the purposes of mission essential risk management. All reviews shall be completed within a 45-day time period.

G.6.4 Trouble Ticket Management

The contractor shall perform trouble ticket management in accordance with commercial best practices, and shall meet the government's requirements specified below.

G.6.4.1 Trouble Ticket Management General Requirements

The contractor shall create a trouble ticket for any reported and discovered service issues, provide status updates, provide online real-time access to trouble ticketing and system status information, update open trouble tickets and escalate as needed, and report the resolution to the initiator.

The contractor shall establish and implement procedures and systems for 24x7x365 trouble ticket and complaint collection, entry, tracking, analysis, priority classification, and escalation for all services to ensure that problems are resolved within the timeframes specified in Section G.8 Service Level Management.

As the first priority, the contractor shall restore any TSP restoration coded service, as quickly as possible, using best effort.

The contractor shall escalate issues according to the contractor's Program Management Plan (PMP) as described in Section G.9.4 Program Management Plan.

G.6.4.2 Reporting Information

The contractor shall provide the government with the capability to query, sort, export, and save in formats such as PDF/CSV or standard/structured file formats trouble and complaint records by any field or combination of formatted (that is, not free-form text) fields in each record.

The contractor shall process any credits applicable to the service outage based on this record of information. SLAs and credits are defined in Section G.8 Service Level Management.

The contractor shall, upon request from the PMO and agencies, deliver archived trouble and complaint report data within five (5) days of the request for such information.

G.7 Inventory Management

G.7.1 Inventory Management Process Definition

The contractor shall establish, and keep current a complete and accurate inventory of EIS services provided to agencies. The contractor shall provide a secure web interface to allow the government to access the data, make queries, obtain reports and perform periodic downloads as needed for audits, billing verification, and other government program management purposes. The technical details for this interface are defined in Section G.5.3.1 Web Interface.

The key tasks associated with inventory management are defined below:

1. GSA identifies the minimum inventory data elements required by service as part of the Inventory Reconciliation (IR) deliverable and specified in Section J.2.7 Inventory Management.
2. As new or enhanced services are added by contract modification, additional inventory data elements will be added to the IR deliverable.
3. The government audits the EIS inventory data provided and advises the contractor of discrepancies noted in the EIS inventory data.
4. The contractor shall investigate EIS inventory data discrepancies reported by the government and works with the government to resolve them.
5. The contractor shall make corrections to the EIS inventory as needed to maintain its accuracy and completeness and issues corrected SOCNs or billing as needed.
6. The contractor shall meet the inventory requirements for transition as defined in Section C.3 Transition.

G.7.1.1 Inventory Management Functional Requirements

The key functional requirements related to Inventory Management are described below:

1. The contractor shall fully populate the EIS Inventory with the data elements of the IR as defined in Section J.2.7 Inventory Management.
2. The contractor shall initially populate records of EIS services in the EIS inventory within one (1) business day of the issuance of SOCNs for EIS services delivered to customers.
    a) The contractor shall establish an inventory for all EIS services provided to its customers.

b) The contractor shall maintain and update the EIS inventory for all EIS services provided to its customers.

c) The contractor shall make the EIS inventory data available to the government.

3. The contractor shall deliver IR deliverable each month as defined in Section J.2.7 Inventory Management.

G.7.1.2 EIS Inventory Maintenance

1. The contractor shall maintain and update the EIS Inventory for all EIS services provided to its customers.
2. The contractor shall update the EIS inventory current view to reflect all additions, deletions, or changes to the EIS services being provided within one (1) business day of the issuance of the SOCN for every addition, deletion, or change.

G.7.1.3 EIS Inventory Data Availability

The contractor shall:

1. Provide to government users secure electronic access to the current view and to the monthly snapshots of EIS services in the contractor-maintained EIS inventory.
2. For secure web-based queries against the contractor-maintained EIS inventory, the contractor shall, as a minimum:

   a) Provide government users the option to select a user choice of online viewing, data file downloading.

   b) Provide and maintain on its EIS BSS web interface a link for secure, electronic access to the contractor-maintained EIS inventory information.

3. For data export or data file delivery in response to a secure query against the contractor-maintained EIS inventory, the contractor shall, at a minimum:

   a) Support common industry standard formats and file structures

   b) Impose no limit on the number of records that is less than the limit imposed by the file format specification

4. Make older monthly snapshots of the EIS inventory that have been archived available for query access, within five (5) days of a government request.
5. Retain the monthly snapshots of the EIS inventory and provide them to the government as requested for three (3) years following the expiration or termination of the contract.

6. Meet or exceed the access security and performance requirements specified in Section G.5.6 BSS Security Requirements for the system used for the EIS inventory.
7. If requested by the government, the contractor shall, at no additional expense to the government, provide a copy of the records, in the format requested by the government, with data field labels, in the current EIS inventory or any of the monthly snapshots either in their entirety or for a subset specified in the government's request.
8. If requested by the government, the contractor shall, at no additional expense to the government, provide a copy of the records in the current EIS inventory, in the format requested by the government, in their entirety of for a subset specified in the government's request.
9. The contractor shall not restrict the use by the government of any and all EIS inventory data related to this contract during the contract and for three (3) years following the expiration or termination of the contract.

G.7.1.4 EIS Inventory Data Discrepancies and Accuracy

G.7.1.4.1 EIS Inventory Data Discrepancies

1. The contractor shall investigate EIS inventory data discrepancies reported by the government. If the contractor agrees to a correction, it shall correct the data discrepancies within ten (10) days.
2. If the contractor does not agree to a correction, it shall advise the government and work with the government to resolve the issue.
3. If the discrepancy is escalated to the CO for resolution, the contractor shall work with the CO to resolve the issue to the government's satisfaction.

G.7.1.4.2 EIS Inventory Data Accuracy

1. The contractor shall institute internal verification and audit procedures to ensure that the EIS inventory is complete and correct.
2. When the contractor discovers an EIS inventory data discrepancy, agrees with a government report of a discrepancy, or is directed to do so by the CO, the contractor shall correct its EIS inventory at no additional cost to the government.
3. When the contractor discovers an EIS inventory data discrepancy, agrees with a government report of an EIS inventory data discrepancy, or is directed to do so by the CO as a result of formal discrepancy resolution, the contractor shall also

investigate whether or not the EIS inventory data elements in the SOCN or Billing Detail (BD) deliverable issued to the government were correct or in error.

4. If the EIS inventory data elements in the SOCN issued to the government were in error, the contractor shall issue, at no additional cost to the government, a corrected SOCN or a new correct SOCN that clearly references the original error.
5. If the EIS inventory data elements result in a billing error in the BD deliverable issued to the government, the contractor shall issue, at no additional cost to the government, a Billing Adjustment (BA) deliverable.
6. The contractor shall correct data discrepancies as they occur and as designated by the government within ten (10) days.

G.7.1.5 EIS Inventory Reconciliation

The contractor shall provide the monthly IR deliverable as defined in Section J.2.7 Inventory Management.

G.8 Service Level Management

This section defines the approach to Service Level Management to be used under the contract. This section specifically addresses the following:

- Service Level Agreements (SLAs)
- Methodological approach to managing those metrics
- SLA reporting requirements

The contractor is responsible for services provided by its subcontractors and any other providers that the contractor uses to deliver EIS services.

G.8.1 Overview

An SLA is an agreement between the government and the contractor to provide a service at a performance level that meets or exceeds the specified performance objective(s). The contract has specific KPIs for nearly all services. If a contractor does offer a service, it must comply with those KPIs. For each KPI, the contractor shall meet specified AQLs. Certain services deemed essential to government operations also require mandatory SLAs. If the specified service levels are not met, then the contractor shall issue specified credits.

This section contains the following major components:

- Service Level Agreement Tables (all SLAs under the contract)
- Service Level General Requirements
- SLA Credit Management Methodology
- Service Level Reporting Requirements

G.8.2 Service Level Agreement Tables

This section contains all standard SLAs. If the contractor offers a service, or if a service is included on a TO, the following SLAs shall apply.

The SLAs in this document represent a minimum level of service acceptable to the government unless otherwise specified at the TO level. Agencies may define additional or different SLAs, KPIs and AQLs during the TO process. These TO-specific SLAs are equally binding, and the contractor is subject to the terms and conditions stated after agreeing to the measurement and price.

G.8.2.1 Service Performance SLAs

G.8.2.1.1 Service-Specific SLAs

Service-specific SLAs are performance measures demonstrating the overall performance of a single TO service. The following table lists each service SLA and a reference to the appropriate location in Section C Technical Requirements. The referenced portion of Section C contains the associated KPIs, their definitions, measurement methodologies, and AQLs. The SLA is defined by all KPIs listed for the service in Section C except those for Time-to-Restore which are addressed in Section G.8.2.1.2. For each service SLA the contractor is required to meet the AQL associated with each KPI listed. The KPIs shall be measured and reported for each unique instance of a service which is defined at the most granular level to which the KPI is applicable but never at a level higher than that defined by the UBI service grouping (see Section J.2.10.1.1.2).

Failure to meet the AQL for any KPI within an SLA constitutes failing that SLA.

G.8.2.1.1.1 Service-Specific SLA Table

Service	Service ID		Section C Reference
Virtual Private Network Service	VPNS	•	C.2.1.1.4
Ethernet Transport Service	ETS	•	C.2.1.2.4
Optical Wavelength Service	OWS	•	C.2.1.3.4
Private Line Service	PLS	•	C.2.1.4.4
Synchronized Optical Network Service	SONETS	•	C.2.1.5.4
Dark Fiber Service	DFS		C.2.1.6.4
Internet Protocol Service	IPS	•	C.2.1.7.4
Broadband Internet Service	BIS	•	C.2.1.8.4
Internet Protocol Voice Service	IPVS	•	C.2.2.1.4
Circuit Switched Voice Service	CSVS	•	C.2.2.2.4
Toll Free Service	TFS	•	C.2.2.3.4
Circuit Switched Data Service	CSDS	•	C.2.2.4.4

Service	Service ID		Section C Reference
Contact Center Service	CCS	•	C.2.3.1.7
Co-located Hosting Center Service	CHS	•	C.2.4.5.1
Infrastructure as a Service	IaaS	•	C.2.5.1.4
Platform as a Service	PaaS		C.2.5.2.4
Software as a Service	SaaS	•	C.2.5.3.4
Content Delivery Network Service	CDNS	•	C.2.5.4.4
Wireless Service	MWS	•	C.2.6.4.1
Commercial Mobile Satellite Service	CMSS	•	C.2.7.3
Commercial Fixed Satellite Service	CFSS	•	C.2.7.3
Managed Network Service	MNS	•	C.2.8.1.4
Web Conferencing Service	WCS	•	C.2.8.2.4
Unified Communications Service	UCS	•	C.2.8.3.4
Managed Trusted Internet Protocol Service – Trusted Internet Connection Portal	MTIPS-TIC	•	C.2.8.4.4
Managed Trusted Internet Protocol Service – Transport Collection and Distribution	MTIPS	•	C.2.8.4.4
Managed Security Service	MSS	•	C.2.8.5.4
Managed Mobility Service	MMS	•	C.2.8.6.4
Audio Conferencing Service	ACS	•	C.2.8.7.4
Video Teleconferencing Service	VTS	•	C.2.8.8.4
DHS Intrusion Prevention Security Service	DIPSS	•	C.2.8.9.4
Software Defined Wide Area Network Service	SDWANS	•	C.2.8.10.4

Note: The government considers the above table and all associated references to be its Quality Assurance Surveillance Plan (QASP) in accordance with FAR 46.401.

G.8.2.1.1.2 Service-Specific SLA Credit Formulas

For each failed SLA, the contractor shall apply the associated credit in accordance with Section G.8.4 SLA Credit Management Methodology. The credit shall be calculated based on the number of times a particular SLA is failed during a rolling six-month window from service acceptance using the following formulas:

- For the first month missing a particular SLA during the six-month window:
  - Service-Specific Credit = 12.5% of the Monthly Charge for a service. This Monthly Charge is either the Monthly Recurring Charge (MRC) for the affected service or the Usage Charge for usage-based services.
- For the second month missing the same SLA during the six-month window:
  - Service-Specific Credit = 25% of the Monthly Charge for the affected service. This Monthly Charge is either the Monthly Recurring Charge (MRC) for the affected service or the Usage Charge for usage-based services.
- For the third (or any subsequent) month missing the same SLA during the six-month window:
  - Service-Specific Credit = 50% of Monthly Charge for the affected service. This Monthly Charge is either the Monthly Recurring Charge (MRC) for the affected service or the Usage Charge for usage based services.
  - The agency may also choose to cancel the affected service without penalty.

G.8.2.1.2 Incident-Based Service SLAs

The Time to Restore (TTR) SLA measures contractor performance on a per-incident basis. The contractor shall calculate the TTR using the following method:

1. Find the elapsed time between the time a service outage is recorded in the trouble ticketing system and the time the service is restored.
2. Subtract time for any scheduled network configuration change or planned maintenance.
3. Subtract time, as agreed to by the government, that the service restoration of the service cannot be worked on due to government-caused delays. Examples of government-caused delays include:

   a) The customer was not available to allow the contractor to access the Service Delivery Point or other customer-controlled space or interface
   b) The customer failed to inform the contractor that a security clearance was required to access the SDP or customer-controlled space
   c) The government required service at a remote site and agreed that a longer transit time was required

For each Incident-based SLA, the contractor shall meet the AQL for the matching KPI associated with the service affected by the incident. The KPIs and associated AQLs for each service are defined in the sections referenced in the table below. Failure to meet the AQL for an individual incident constitutes failing the SLA for that incident unless due to documented delays caused by the customer.

G.8.2.1.2.1 Incident-Based Service SLA References

Service	Service ID	Section C Reference
Virtual Private Network Service	VPNS	C.2.1.1.4
Ethernet Transport Service	ETS	C.2.1.2.4
Optical Wavelength Service	OWS	C.2.1.3.4
Private Line Service	PLS	C.2.1.4.4
Synchronized Optical Network Service	SONETS	C.2.1.5.4
Dark Fiber Service	DFS	C.2.1.6.4
Internet Protocol Service	IPS	C.2.1.7.4
Internet Protocol Voice Service	IPVS	C.2.2.1.4
Broadband Internet Service	BIS	C.2.1.8.4
Circuit Switched Voice Service	CSVS	C.2.2.2.4
Toll Free Service	TFS	C.2.2.3.4
Circuit Switched Data Service	CSDS	C.2.2.4.4
Contact Center Service	CCS	C.2.3.1.4
Colocated Hosting Service	CHS	C.2.4.5.1
Infrastructure as a Service	IaaS	C.2.5.1.4
Platform as a Service	PaaS	C.2.5.2.4
Software as a Service	SaaS	C.2.5.3.4
Content Delivery Network Service	CDNS	C.2.5.4.4
Wireless Service	MWS	C.2.6.4.1
Managed Network Service	MNS	C.2.8.1.3

Service	Service ID	Section C Reference
Web Conferencing Service	WCS	C.2.8.2.4
Unified Communications Service	UCS	C.2.8.3.4
Managed Trusted Internet Protocol Service – Transport Collection and Distribution	MTIPS	C.2.8.4.4
Managed Security Service	MSS	C.2.8.5.4
Audio Conferencing Service	ACS	C.2.8.7.4
Video Teleconferencing Service	VTS	C.2.8.8.4
DHS Intrusion Prevention Security Service	DIPSS	C.2.8.9.4
Software Defined Wide Area Network Service	SDWANS	C.2.8.10.4

G.8.2.1.2.2 Incident-Based Service SLA Credit Formula

For each failed SLA, the contractor shall apply the associated credit in accordance with Section G.8.4 SLA Credit Management Methodology using one of the following formulas based on the nature of the service in question:

- Routine Service Time to Restore (TTR) Credit = 50% of the Monthly Recurring Charge (MRC) for the affected service
- Critical Service Time to Restore (TTR) Credit = 100% of the MRC for the affected service

G.8.2.1.3 Service-Related Labor SLAs

The types of labor services to be delivered will vary widely by TO; as a result, KPIs and SLAs will be specific to and defined in each TO. Similarly, measurement methods, SLA credit formulations, and tracking methodology shall be defined in the TO, see C.2.11 Service-Related Labor for additional information.

G.8.2.2 Service Provisioning SLAs

The SLAs for the provisioning of services under the contract are defined in the subsections below:

- Standard Provisioning SLAs
- ICB Provisioning SLAs
- Project Provisioning SLAs

The provisioning interval for orders shall be measured in days from the TO submission date if no service orders are used, or else from the service order date to the completion date in the SOCN in accordance with Section J.2.4 Ordering:

- Interval = number of days from the service order to the SOCN Completion Date

For associated services ordered together and assigned UBIs with the same service group ID, the SLA shall be governed by the longest provisioning interval.

As described in Section G.3.3.1.3, if the time between the service order and the CWD is greater than the defined provisioning interval for the service as described in the subsections below, the service provisioning SLA is waived for that service on that order.

G.8.2.2.1 Standard Provisioning SLAs

The contractor shall complete orders within the provisioning intervals defined in the table below.

Failure to complete the provisioning of service within the specified timeframes shall constitute a failure to meet the SLA for that provisioning incident.

Note: For orders with non-CONUS delivery locations, these services have individual case basis (ICB) provisioning intervals and follow the requirements described in Section G.8.2.2.2 Individual Case Basis Provisioning SLAs.

G.8.2.2.1.1 Standard Service Provisioning Intervals

Service	Orders SLA (Days)
Disconnect (all services)	30
Circuit Switched Data Service (CSDS)	23
Toll-Free Service (TFS)	45
Private Line Service (PLS):	
PLS ≤ DS1	45
DS1 < PLS ≤ DS3	85
DS3 < PLS ≤ OC3	120
VPN Service (VPNS)	45

G.8.2.2.2 Individual Case Basis Provisioning SLAs

Certain service provisioning tasks do not have predefined provisioning intervals (see the table below for a complete list). For these services, the performance objective shall be

defined on an individual case basis (ICB) with the required delivery schedule established in the TO.

Failure to complete the provisioning of service within the timeframe specified in the TO shall constitute a failure to meet the SLA for that provisioning incident.

Notes:

1. For Ethernet Transport Services, see also Section G.8.2.2.4.2 Bandwidth-on-Demand

2. For Cloud Services; including IaaS, PaaS, SaaS, and CDNS; the ICB provisioning interval must be no greater than the provisioning interval proposed as specified in Section G.8.2.2.4

3. For any services proposed under rapid provisioning that also appear on this list, the ICB provisioning intervals must be no greater than the provisioning interval proposed as specified in Section G.8.2.2.4

G.8.2.2.2.1 Services Subject to ICB Provisioning Intervals

Service
• Audio Conferencing Service (ACS) • Cloud Infrastructure as a Service (IaaS) • Cloud Platform as a Service (PaaS) • Cloud Software as a Service (SaaS) • Cloud Content Delivery Network Service (CDNS) • Co-located Hosting Service (CHS) • Commercial Satellite Communications Services (CMSS, CFSS) • Contact Center Service (CCS) • Dark Fiber Service (DFS) • Ethernet Transport Service (ETS) • Internet Protocol Service (IPS) • Broadband Internet Service (BIS) • Managed Network Service (MNS) • Managed Security Service (MSS) • Managed Trusted Internet Protocol Service (MTIPS) • Managed Mobility Service (MMS) • Optical Wavelength Service (OWS) • Unified Communications Service (UCS) • Video Teleconferencing Service (VTS) • Voice Services (IPVS, CSVS) • Web Conferencing Service (WCS)

G.8.2.2.3 Project Provisioning SLAs

For project orders (orders that require special treatment by the contractor due to the size, complexity, or importance of the services ordered), the performance objective shall be based on the baseline completion dates in the Task Order Project Plan (TOPP) agreed upon and documented by the government and the contractor at the time orders are placed and confirmed by the contractor. For these services, the performance objective shall be defined on an individual case basis (ICB) with the required delivery schedule established in the TO.

Failure to complete the provisioning of service within the timeframes specified in the TOPP shall constitute a failure to meet the SLA. In the event that timeframes are not specified in the TOPP, the standard provisioning SLAs and intervals are defined in Section G.8.2.2 Service Provisioning SLAs.

G.8.2.2.4 Rapidly Provisioned Services

G.8.2.2.4.1 Cloud Service Provisioning

Within the criteria of rapid and elastic provisioning for cloud services as defined by NIST, and as referenced in Section C.2.5 Cloud Service, the contractor shall provide a means of electronically tracking the ordering, confirmation, and provisioning of cloud services such that the intervals between each can be accurately tracked as described in Section G.3.3.3.2 Rapid Provisioning Orders. If the contractor is proposing cloud services, they shall also propose the associated provisioning KPIs and SLAs.

G.8.2.2.4.2 Bandwidth-on-Demand

As described in Section C.2.1.2 Ethernet Transport Services, the contractor shall support bandwidth increments and decrements on demand, as agreed between the contractor and the agency. Unless otherwise agreed by the agency and contractor on a case-by-case basis, provisioning time for this feature shall meet the standard below, measured from the service order to the SOCN.

Service	Provisioning SLA
Ethernet Transport Services: Bandwidth-on-Demand Changes	24 Hours

G.8.2.2.4.3 Other Services Subject to Rapid Provisioning

Consistent with the requirements in Section G.3.3.3.2 Rapid Provisioning Orders, if the contractor is proposing specific services for rapid provisioning, they shall also propose associated KPIs and SLAs.

G.8.2.2.5 Service Provisioning SLA Credit Formulas

For each failed SLA, the contractor shall apply the associated credit in accordance with Section G.8.4 SLA Credit Management Methodology using the following formulas:

- **Default Provisioning Credit** = the larger of:
  - 50% of the Non-Recurring Charge (NRC), or
  - 50% of the Monthly Recurring Charge (MRC).

G.8.2.3 Billing Accuracy SLA

The contractor shall submit accurate billing that meets the performance standards for Billing Accuracy for each TO as defined in Section G.4 Billing. Failure to meet the accuracy standards defined in that section shall constitute failing to meet the Billing Accuracy SLA. If this SLA is failed, the contractor shall apply the associated credit in accordance with Section G.8.4 SLA Credit Management Methodology using the following formula:

- **Billing Accuracy Credit** = 1% of contractor's Total Billed Revenue on the applicable TO for the month.

G.8.3 Service Level General Requirements

The contractor shall be responsible for meeting all SLA requirements as defined in Section G.8.2 Service Level Agreement Tables. This includes delivering the service, maintaining the service at specified AQLs, measuring the KPIs, reporting on compliance, and issuing the specified credit when performance fails to meet the performance objective.

G.8.3.1 Measurement

The contractor shall measure each SLA in accordance with its definition provided in Section G.8.2 Service Level Agreement Tables. Procedures for measuring and sampling shall be described in the quality assurance section of the Program Management Plan, which is described in Section G.9.4 Program Management Plan.

G.8.3.2 Reporting

The contractor shall provide service level management reports as detailed in Section G.8.5 Service Level Reporting Requirements.

G.8.3.3 Credits and Adjustments

In cases where the contractor does not meet the defined contractual or TO SLA, the contractor shall provide credits and/or adjustments to the government agency of record

or GSA. This process is further detailed in Section G.8.4 SLA Credit Management Methodology.

G.8.4 SLA Credit Management Methodology

If the contractor fails to meet the performance objectives specified in the SLAs defined above, the government is entitled to receive credit within two billing cycles. The amount of credit shall be calculated as specified in the applicable portion of Section G.8.2 Service Level Agreement Tables.

In cases where multiple SLAs credits are triggered, all credits are paid with the limitation that the total maximum penalty on a service in a given month shall not exceed the total billed cost for that service.

The government may grant a waiver from all or part of a credit if exceptional circumstances warrant.

The TO on the bill defines the customer that will receive the credit and may grant a waiver for all SLAs.

G.8.4.1 Credit Management

The GSA CO, OCO, or authorized ordering official may submit to the contractor an SLA Credit Request (SLACR) as defined in Section J.2.8. In addition, the GSA CO or OCO may designate, in writing, additional personnel or systems authorized to submit SLACRs to the contractor. Additional credit management requirements may be defined in the TO.

The government reserves the right to submit a SLACR at any time within six (6) months of the original SLA failure. For the billing accuracy SLA, defined in Section G.8.2.3, the six-month window for SLACR submission shall begin at the end of the six-month holding period included in the underlying KPI definitions (see Sections G.4.12.1 and G.4.12.2). The contractor shall respond to the request within 30 days by submitting a SLACR response and issue the credit within two billing cycles of this response unless it chooses to reject the request.

The contractor shall work with the government to resolve any disputes and agree on an appropriate credit award in accordance with Section G.4.4 Billing Disputes.

G.8.5 Service Level Reporting Requirements

G.8.5.1 Report Submission

Unless otherwise specified, each report shall be TO-specific and address only those actions and metrics applicable to the TO in question. As specified in Section G.5

Business Support Systems, reports shall be submitted electronically via the contractor's web interface and via direct data exchange.

G.8.5.2 Report Definitions

G.8.5.2.1 Service Level Agreement Report

The Service Level Agreement Report (SLAR) shall document monthly SLA performance covering all aspects of service including incident-based SLAs, service-specific SLAs, and service provisioning SLAs, and billing accuracy SLAs. Report contents are defined in Section J.2.8. The contractor shall deliver this report on the 15th day of each month.

G.8.5.2.2 SLA Credit Request (SLACR) Response

The SLA Credit Request (SLACR) response shall document the contractor's response to a government request for SLA credits (See Section G.8.4.1 Credit Management). Response contents are defined in Section J.2.10. The contractor shall deliver this response within 30 days after the receipt of an SLACR.

G.8.5.2.3 Trouble Management Performance Summary Report

This report shall document trouble management performance by summarizing the number of trouble reports opened and resolved during the reporting period. Unless otherwise specified by the TO, the contractor may use its standard commercial report format for this report provided that it contains the information specified. The contractor shall deliver this report within 14 days after the end of each FY quarter.

G.8.5.2.4 Trouble Management Incident Performance Report

This report shall document trouble management incident-level performance by describing each trouble report issued during the reporting period by contractor trouble report number, agency and AHC, UBI, time opened and time resolved. Unless otherwise specified by the TO, the contractor may use its standard commercial report format for this report provided that it contains the information specified. The contractor shall deliver this report within 14 days after the end of each FY quarter.

G.9 Program Management

This section describes the contractor's requirements for program management, which shall remain in effect through the duration of the contract.

The contractor shall communicate directly with agencies and with GSA. GSA will be accountable for the contractor's technical performance.

G.9.1 Contractor Program Management Functions

The contractor shall effectively and responsively plan, control, and execute against this contract. The contractor shall provide the following program management functions including but not limited to: program control, planning at the program level, planning at the agency level, contractor performance, resource management, revenue management, reporting and reviews, and senior-level communications.

G.9.2 Performance Measurement and Contract Compliance

The contractor's performance shall be measured against the set of SLAs established by the contract. The contractor shall:

1. Submit all SLA data for performance monitoring and reporting to enable an accurate assessment of performance against SLAs as defined in Section G.8.
2. Monitor and manage the contractor's performance against all contract performance requirements.
3. Designate a single interface point for SLA information or issues.
4. Resolve all issues concerning SLAs, including those that pertain to subcontractors. These include, but are not limited to, missing data, data reported in the wrong format or units, late submission from subcontractors, etc.

G.9.3 Coordination and Communication

1. The contractor shall implement consistent and effective communications between management and technical personnel as indicated below in Section G.9.4 Program Management Plan.
2. The contractor shall manage the customer relationship, including, but not limited to:
   a) Government-contractor communications
   b) Resolving trouble reports and complaints
   c) Resolving issue calls
   d) Resolving billing disputes and inquiries
   e) Resolving schedule issues

f) Resolving reporting discrepancies

3. The contractor shall provide technical expertise across all services.
4. The contractor shall answer questions and address issues from the EIS PMO regarding the contractor's network management activities, particularly those that have not been resolved to the government's satisfaction through the standard trouble handling process described in Section G.6.4.1 Trouble Ticket Management General Requirements.
5. The contractor shall provide the escalation procedure for the government to escalate issues to appropriate levels of the contractor's management to resolve disputes and issues.
6. At a minimum, the contractor shall have the capability and authority to:
   a) Support disaster recovery planning and execution
   b) Resolve interoperability problems
   c) Respond to escalation of service concerns
   d) Participate in contract performance reviews
   e) Participate in contract modification negotiations
   f) Perform basic network management functions in support of the government's requirements as described in Section G.8 Service Level Management
   g) Help resolve billing queries and reconciliation issues
   h) Support NS/EP requirements
   i) Provide the EIS PMO with information on customer requirements and customer demographics
7. Within 30 days of the Notice to Proceed, the contractor shall provide and maintain a Contractor Points of Contact List that provides contact information for, at a minimum, the functions that follow:
   a) Provisioning orders
   b) Identifying and resolving service troubles and complaints
   c) Providing customers with status of troubles and resolution
   d) Developing and delivering training
   e) Conducting billing inquiries
   f) Transition project management
   g) Finance
   h) Contracting

i) Account Management (business development and sales)

j) Security

k) NS/EP

8. The contractor shall identify its:

   a) Security POCs who will be processing background investigations and security clearances at the appropriate levels as identified in Section C.1.8.7.7 Personnel Background Investigation Requirements and Section G.5.6 BSS Security Requirements.

   b) POCs that have passed national agency checks or background investigations, and the security clearance levels held by these individuals as defined in Section G.5.6 BSS Security Requirements.

GSA will provide the contractor with contact information (names, phone numbers, and email addresses) for the CO, PM, COR, TSMs and for contacts within the PMO.

G.9.4 Program Management Plan

The contractor shall submit with its proposal a Program Management Plan (PMP) that describes its program management method and implementation plan at a level of detail sufficient to give the government an understanding of the program management approach. The PMP shall address, at a minimum, but is not limited to the following:

1. Summary of contract management requirements, including government dependencies and assumptions regarding government services, facilities, and personnel.
2. Summary Description of the service solution, including the methodologies used to comply with Service Ordering, Billing, Inventory Management, and Service Management requirements.
3. Draft program management schedule.
4. Draft transition management approach. The contractor shall describe its approach to the project management of transition, including the contractor's project management process, procedures, and tools to meet the transition requirements of Section C.3. The Transition section shall address the following areas as well as additional areas proposed by the contractor:

   a) Transition Project Management. The contractor shall address the billing, service ordering, trouble reporting, and customer service processes unique to transitioning onto and off from EIS, specifically including a discussion of how the contractor will expedite transition when it is also the incumbent service provider. The contractor shall describe how it will coordinate with other incumbent providers to ensure a smooth, successful, and timely transition.

The contractor shall identify and assess the major transition risks and propose a response to each.

b) Agency Solicitations. The offeror shall describe its approach to assisting agencies with selecting new or enhanced services to replace services on expiring contracts. The offeror shall identify in the PMP the Transition Management Approach incentives, if any, it will offer agencies to expedite transition.

c) Customer Support during Transition. The contractor shall describe and provide an outline for any transition handbooks or guides it will make available to customers and indicate the target date for publication.

d) Interconnection Plan. The contractor shall describe the interconnection arrangements between the incumbent contractor's network and the EIS networks during the transition, including the interconnection arrangements with the local exchange network, the IXCs, and government private networks. The contractor shall describe any interconnections with other service providers, including other operating units within the contractor's company such as wholesale services, known or expected to be required to transition services and describe the potential impact to customers' operations.

e) Transition Contingency Plan. The contractor shall describe how service will be restored if unforeseen difficulties are encountered at any stage of the transition.

5. Resource plan, providing a management approach to:

   a) Financial Resources: budgeting, tracking, and controlling costs

   b) Human Resources: identifying and retaining qualified personnel and making effective use of their skills

   c) Equipment: managing hardware and software assets

6. Quality Control Program. Management approach to formulating and enforcing work and quality standards, ensuring compliance with contractual SLAs, reviewing work in progress, and providing customer support services.

7. Key Personnel and Organizational Structure . Management structure, organizations, and roles and responsibilities of each function performing work under this contract, key personnel and corporate structure, and subject matter experts as defined in Section H.10 Key Personnel and Corporate Structure .

8. Risk Management. Process for identifying program risks, including risks identified in this contract, and actions to mitigate them.

9. Information Systems. Description of BSS employed to implement the requirements of the contract consistent with security plans to prevent unauthorized access to the government's data and an agency's access to data

belonging to any other agency. Describe how the contractor shall ensure those systems are available to meet the requirements of Section G.5 Business Support Systems

G.9.5 Financial Management

The contractor shall provide a monthly Financial Status Report to the GSA PMO that shows the total dollar activity for the month, broken down by the service types and services in Table B.1.2.1.1, and including the total billed charges for all agencies during the monthly reporting period.

Note: the contractor shall update the list of service types and services with proposals for new or improved services, or when a contract action deletes services from the list.

G.9.6 Program Reviews

G.9.6.1 Quarterly Program Status Reports

The contractor shall deliver Quarterly Program Status Reports to the GSA PMO and lead Quarterly Program Management Review (QPMR) meetings. The Quarterly Program Status Reports shall include, but are not limited to:

- The status of:
  - Project Plan for program management activities
  - Base contract modifications
  - TOs and modifications
  - Projects
  - Orders entered and completed
  - Backlog
  - Aging
  - Pipeline of orders
- Billing disputes
- Summary of trouble reports
- Issues and resolution
- Root cause analysis:
  - Identification of measures failing SLAs
  - Root cause of the failure
  - Corrective action to remedy

- Technical accomplishments and future plans

G.10 Training

The contractor shall provide training on EIS as described below in Section G.10.1 at no additional cost to government customers, as part of the basic service. An agency may request additional (specialized) training as required in a TO. Training shall include courseware development and instructing customer personnel.

The contractor shall include a draft Customer Training Plan in its proposal. The contractor's Customer Training Plan shall detail the designated training for government users that may include the CO and/or CORs, end-users of services, government trainers, and government executives. This training shall remain available throughout the life of the contract. The Customer Training Plan shall list course curricula that educate the government users on the use of the BSS and the performance of tasks related to billing, pricing, order submission and tracking, network performance, trouble ticketing, and inventory management as described below in Section G.10.1. The government reserves the right to provide comments within 30 days of Notice to Proceed. If comments are provided, the contractor shall incorporate them and deliver the revised Training Plan within 15 days after the comments were received.

As mutually agreed by the government and the contractor, training shall be conducted on government premises or contractor premises within daily commuting distance for the government students, or via training methods that include:

1. Instructor-led classroom training
2. Distance learning
3. Online web-based / self-paced learning
4. Interactive video
5. Other remote training methodologies
6. Other methods specified by the government

When training is conducted at a contractor site, the contractor shall provide an appropriate classroom environment and all necessary equipment and support. When training is conducted at a government site, the government will provide the necessary space, equipment, and environmental support. The government may inspect training facilities and may observe training being performed by the contractor to ensure compliance with the contract.

The contractor shall provide training as requested by the government throughout the life of the contract.

G.10.1 Training Curriculum

The contractor shall train designated COs, authorized ordering officials, OCOs, and CORs to fully understand and use the contractor's BSS. The contractor shall provide training that covers the course curriculum (classroom and laboratory, as required) to ensure each student becomes proficient in performing tasks that include, but are not limited to:

1. Use of the contractor's BSS
2. Obtaining price quotes for services and features
3. Ordering services from the contractor via CLINs or ICBs
4. Placing order electronically to add, change, cancel, or disconnect services
5. Adding or changing the features, calling privileges, telephone number or other line attributes that can be changed via "soft" reconfigurations
6. Accepting or rejecting an order or part of an order
7. Reconciling billing
8. Initiating and tracking billing disputes
9. Initiating the inventory management process
10. Initiating and reconciling performance management (SLA) reports
11. Placing and tracking trouble reports for routine and emergency troubles

G.10.2 Training Evaluation

To measure and improve the student's training experience as well as to ensure that the contractor accomplished its purpose, the contractor will provide an automated/online method at the end of each class for the students to evaluate the instructor, effectiveness, course objectives and applicability of the course material, training facilities/method, and offer written comments.

The contractor will be notified by the CO or the OCO in writing of any training that is deemed unacceptable. This notification will identify the unacceptable portion(s) of the training. The contractor shall be responsible for correcting the unacceptable issue(s).

G.11 National Security and Emergency Preparedness

The concept of a national telecommunications infrastructure is recognized in national policy statements and directives issued under the authority of the Executive Office of the President, Congress, the Department of Homeland Security (including the Office of Emergency Communications), and other entities of the government. This telecommunications infrastructure is required to support the critical needs of the government under conditions of stress that range from crises and natural disasters (e.g., flood, earthquake) through declared conditions of National Security and Emergency Preparedness (NS/EP). Public safety and the economic well-being of the nation also depend upon the availability of reliable and responsive telecommunications services. EIS is a key component of the US national telecommunications infrastructure.

NS/EP requirements for telecommunication services are used to maintain a state of readiness or to respond to and manage any event or crisis that causes or could cause injury or harm to the population or damage to or loss of property or that degrades or threatens the NS/EP posture of the United States.

GSA expects to provide assurance for government users that services and other service elements (technical, management, and operations-related) acquired through EIS are in compliance with national policy throughout the life of the contracts. The contractor shall ensure that services delivered are in compliance with national policy directives that apply to the national telecommunications infrastructure. Specific national policy requirements include, but are not limited to, PL 93-288 (Disaster Preparedness Assistance dated May 22, 1974), PPD-1 (Organization of the National Security Council System dated February 13, 2009), PPD-21 (Critical Infrastructure Security and Resilience, dated February 12, 2013), NSDD-97, NSDD-145 and its successors, and other applicable laws, regulations, and directives. Executive Orders (EO) 12472 and 13618 and its successors shall also be considered in the design and operations of services provided under this contract. The contractor shall provide an NS/EP Functional Requirements Implementation Plan with the proposal that addresses the specifications identified in Sections G.11.1–G.11.3, and update it annually.

The contractor shall notify the government immediately when events arise that may have major consequences to its network. This notification is similar to the “abnormal report” currently furnished to the DHS National Coordinating Center (NCC). The GSA CO will set priorities; however, the contractor shall be solely responsible for network operations.

G.11.1 Basic Functional Requirements

For services and CBSAs awarded, the contractor must support the agency's NS/EP requirements which may include the following 14 basic functional requirements for

NS/EP telecommunications and IT services, as identified by the Department of Homeland Security (DHS) Office of Emergency Communications (OEC) (formerly NCS) and the Office of Science and Technology Policy for NS/EP telecommunications services and are now being endorsed by ANSI T1 and ITU-TSS standard bodies and widely supported by contractor communities:

1. Enhanced Priority Treatment. Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic.
2. Secure Networks. Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
3. Non-Traceability. Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).
4. Restorability. Should a service disruption occur, voice and data services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.
5. International Connectivity. Voice and data services must provide access to and egress from international carriers.
6. Interoperability. Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks which will be identified after contract award.
7. Mobility. The ability of voice and data infrastructure to support transportable, re-deployable, or fully mobile voice and data communications.
8. Coverage. Voice and data services must be readily available to support the national security leadership and inter- and intra- agency emergency operations, wherever they are located.
9. Survivability/Endurability. Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.
10. Voice Band Service. The service must provide voice band service in support of presidential communications.
11. Broadband Service. The service must provide broadband service in support of NS/EP missions (e.g., video, imaging, Web access, multimedia).
12. Scalable Bandwidth. NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.

13. Affordability. The service must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).
14. Reliability/Availability. Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

G.11.2 Protection of Classified and Sensitive Information

NS/EP related information includes, but is not limited to, databases for classified information; critical users' locations, identifications, authorization codes, and call records; and customer profiles. Additionally, the contractor is provided access to certain classified and sensitive materials required for the planning, management, and operations for NS/EP. That information is in various forms, including hardcopy and electronic media. It will be identified as to its classification and shall be protected by the contractor in accordance with applicable industrial security regulations (National Industrial Security Program Operating Manual [NISPOM] and NSA-approved standards as applicable for Safeguarding Classified Information). The level of classification will be up to and including Top Secret / SCI (Sensitive Compartmented Information), and identified by the government.

G.11.3 Department of Homeland Security Office of Emergency Communications Priority Telecommunications Services

The contractor shall fully comply and interoperate with all Department of Homeland Security (DHS) Office of Emergency Communications (OEC) Priority Telecommunications Services including TSP, Government Emergency Telecommunications Service (GETS), Wireless Priority Service (WPS) and, when released, Next Generation Network Priority Services (NGN-PS). OEC's Communications Portfolio Management (CPM) Branch collaborates with the public and private sectors to ensure the NS/EP communications community has access to priority telecommunications and restoration services to communicate under all circumstances.

G.11.3.1 Government Emergency Telecommunications Service

Government Emergency Telecommunications Service (GETS) is a White House-directed emergency telephone service provided by the DHS OEC. During emergencies, the public telephone network can experience congestion due to increased call volumes and/or damage to network facilities, hindering the ability of NS/EP personnel to complete calls. GETS provides NS/EP personnel priority access and prioritized processing in the local and long distance segments of the landline networks, greatly increasing the probability of call completion. GETS is intended to be used in an

emergency or crisis situation when the network is congested and the probability of completing a normal call is reduced. GETS is an easy-to-use calling card program; no special phones are required. There is no cost to enroll in GETS, though usage fees may apply. GETS calls will receive priority over normal calls; however, GETS calls do not preempt calls in progress or deny the general public's use of the telephone network. GETS is in a constant state of readiness. It also provides priority calling to most cell phones on major carrier networks. The contractor shall fully comply and interoperate with the GETS service. For more information, see: http://www.dhs.gov/government-emergency-telecommunications-service-gets.

G.11.3.2 Wireless Priority Service

Wireless Priority Service (WPS) is a White House-directed emergency phone service managed by the DHS OEC. WPS complies with the Federal Communications Commission (FCC) Second Report and Order, FCC 00-242, *Establishment of Rules and Requirements for Priority Access Service*.

During emergencies cellular networks can experience congestion due to increased call volumes and/or damage to network facilities, hindering the ability of NS/EP personnel to complete emergency calls. The WPS provides NS/EP personnel priority access and prioritized processing in all nationwide and several regional cellular networks, greatly increasing the probability of call completion. WPS is intended to be used in an emergency or crisis situation when cellular networks are congested and the probability of completing a normal cellular call is reduced. WPS is an easy-to-use, add-on feature subscribed to on a per-cell phone basis. It is deployed by cellular service providers throughout the United States. WPS calls will receive priority over normal cellular calls; however, WPS calls do not preempt calls in progress or deny the general public's use of cellular networks. WPS is in a constant state of readiness. The contractor shall fully comply and interoperate with the WPS service. For more information, see: https://www.dhs.gov/wireless-priority-service-wps.

G.11.3.3 Telecommunication Service Priority

The Telecommunication Service Priority (TSP) System (FCC 88-341) provides a framework for telecommunications services contractors to initiate, restore, or otherwise act on a priority basis to ensure effective NS/EP telecommunication services. The TSP System applies to common carriers, to government, and to private systems that interconnect with commercially provided services or facilities. The TSP System is intended to apply to all aspects of end-to-end NS/EP telecommunication services. The TSP system allows five (5) levels of priorities for restoration (5, 4, 3, 2, or 1) and provisioning (5, 4, 3, 2, 1, or E).

The contractor shall fully comply and interoperate with the TSP system for priority provisioning (i.e., installation of new circuits), restoration of previously provisioned circuits, and priority level for design change of circuits, including coordination between local access providers and the transport segment. The contractor shall fully comply and interoperate with any future TSP replacement system.

Should the contractor's network experience significant degradation or failure, the contractor shall provide priority restoration of affected services in accordance with the TSP system five levels of priorities. In addition, the contractor shall ensure that the restored circuits retain the property of the original circuits (i.e., TSP levels). [Note that the contractor is only obligated for priority restoration and provisioning of those circuits that agencies have obtained TSP priorities from EOC.

TSP Authorization Codes are active for three (3) years, at which point the service user will need to revalidate them. Service users must request TSP restoration priority **before** a service outage occurs.

G.12 Requirements for Climate Change Adaptation, Sustainability and Green Initiatives

G.12.1 Climate Change Adaptation

EIS seeks to benefit from the use of sustainable management practices by contractors including tracking and seeking continual reductions in energy usage, greenhouse gas (GHG) emissions, water consumption, solid waste and hazardous waste, and other relevant environmental impacts and associated costs. Use of sustainable management practices results in lower environmental impacts of delivered products and services, helping customers meet the GHG emissions reduction, sustainable acquisition, and climate change adaptation requirements under Executive Order 13693, – Planning for Federal Sustainability in the Next Decade, and its precursors, successors and related regulations and guidance.

Public disclosures of environmental impacts and sustainable management practices have been associated with reduced supply chain and other business risks for disclosing companies. Sustainability disclosures can help EIS customers understand the major environmental impacts of procured products and services, familiarize themselves with the available strategies for reducing these impacts, and design projects and TO requirements which incorporate these strategies.

GSA will require corporate sustainability reporting. GSA encourages the contractor to provide the location(s) (Internet URL or URLs) of one or more sources of publicly available information regarding company-wide environmental impacts and sustainable management practices (sustainability disclosures) on the contractor's EIS webpage. In making sustainability disclosures, the contractor is requested to use existing, widely recognized third-party sustainability reporting portals and services such as the Global Reporting Initiative (GRI) Sustainability Disclosure Database (database of corporate social responsibility (CSR) reports) and the Carbon Disclosure Project (CDP) Climate Change and Water Disclosure Questionnaires. All sustainability disclosures shall be kept up-to-date and accurate.

These sustainability-related standards, including estimates of the lifecycle costs and environmental impacts of proposed solutions, shall apply at the TO level.

GSA has a leading role in ensuring that the federal government is better prepared to cope with the consequences of climate change adaptation that presents many serious risks for government operations. These risks include damage to facilities and equipment, and disruptions to communications networks and transportation routes needed to deliver supplies and services. Climate change adaptation aspects shall be considered in the design and operations of services to be provided under this contract.

The contractor shall incorporate climate change adaptation strategies into risk-management programs to reduce property, infrastructure, and supply chain vulnerabilities. This includes identifying mission critical facilities, products and services, evaluating business operations and supply chains that may be vulnerable and anticipating needs that may arise from climate change. The contractor shall comply with the climate change adaptation conditions described in Executive Order 13693, – Planning for Federal Sustainability in the Next Decade, and other applicable laws, regulations, and directives.

Executive Order 13693 – Planning for Federal Sustainability in the Next Decade, requires agencies "To improve environmental performance and Federal sustainability, priority should first be placed on reducing energy use and cost, then on finding renewable or alternative energy solutions. Pursuing clean sources of energy will improve energy and water security, while ensuring that Federal facilities will continue to meet mission requirements and lead by example. Employing this strategy for the next decade calls for expanded and updated Federal environmental performance goals with a clear overarching objective of reducing greenhouse gas emissions across Federal operations and the Federal supply chain." In support of this requirement, contract awardees shall prepare and update as needed Corporate Climate Risk Management Plans that will be made available for agency use to directly support the Agency Adaptation Plans of agencies procuring services through this contract.

Contractors shall conduct corporate sustainability reporting through accredited third parties and provide copies of their reporting to GSA.

The contractor shall deliver a yearly Climate Change Adaptation, Sustainability, and Green Initiatives Report to the GSA CO that highlights any changes made throughout the year to remain fully compliant with the federal directives mentioned above. Section F contains the schedule for all contractual deliverables.

The contractor shall notify the agency and the GSA CO immediately if conditions arise thought to be out of compliance with the aforementioned Executive Orders, laws, regulations, and directives.

G.12.2 Sustainability and Green Initiatives

GSA is committed to environmentally friendly sustainable practices that reduce the federal government's environmental footprint. The contractor shall provide sustainable products and services whenever possible. Both the sustainable acquisition and data center requirements of Executive Order 13693 – Planning for Federal Sustainability in the Next Decade shall be considered in the design and operations of services to be provided under this contract. The contractor shall comply with the climate change

adaptation conditions described in the aforementioned Executive Orders, and other applicable laws, regulations, and directives.

The contractor shall notify the agency and GSA COR immediately if conditions arise thought to be out of compliance with the aforementioned Executive Orders, laws, regulations, and directives.

Commercially available products under this contract may be covered by the Energy Star®, Federal Energy Management Program (FEMP), or Electronic Product Environmental Assessment Tool (EPEAT) programs. For applicable products, the contractor is encouraged to offer Energy Star-qualified/certified products, products meeting FEMP low-standby power levels, and EPEAT-registered products, at the Bronze level or higher. If the contractor opts to offer Energy Star-certified, low standby power, or EPEAT-registered products then they shall identify by model which products offered are Energy Star-qualified/certified, meet FEMP low standby power levels, and/or EPEAT-registered, with EPEAT-registered products broken out by registration level of bronze, silver, or gold. Visit the Green Procurement Compilation at www.sftool.gov/greenprocurement for a complete list of products covered by these programs.

E.O. 13693 requires agencies to improve data center energy efficiency at federal facilities. The E.O. Implementing Instructions encourage agencies to use data center shared service providers and contracted data center services, including cloud services, which are provided through data centers that meet power utilization efficiency targets between 1.2 and 1.4.

G.12.2.1 Electronic Product Environmental Assessment Tool

Under this contract, the contractor shall deliver, furnish for government use, or furnish for contractor use at a federally-controlled facility, equipment that was EPEAT bronze-registered at the bronze level or higher throughout the life of the contract. For all products covered by EPEAT, the contractor shall comply with FAR 23.704.

The contractor shall deliver a yearly Climate Change Adaptation, Sustainability, and Green Initiatives Report to the GSA CO that highlights any changes made throughout the year to remain fully compliant with the federal directives mentioned above. Section F contains the schedule for all contractual deliverables.

G.12.2.2 Energy Efficient Products

The contractor shall ensure that energy-consuming products are energy efficient (e.g., Energy Star-certified products or Federal Energy Management Program (FEMP)-designated products or low standby power products) throughout the life of the contract,

in compliance with FAR Clause 52.223-15 Energy Efficiency in Energy-Consuming Products.

G.12.2.3 Data Centers and Cloud Services

The contractor shall identify which data center or cloud services, if any, will be provided through data centers meeting power utilization efficiencies (PUE) between 1.2 and 1.4. The contractor shall report annually the PUE of data centers used under this contract.