Volume 2 - Management Proposal

Solicitation No.: QTA0015THA3003

Date: November 4, 2016

Submitted to: General Services Administration FAS/ITS

Submitted by: Core Technologies, Inc.

Table of Contents

1.0 RESERVED

2.0 MANAGEMENT RESPONSE [RIN: MMC0002-DI]

CTI will meet all of the EIS RFP requirements for Program Management and contract administration that will remain in effect throughout the duration of the contract. CTI's capability to effectively administer the EIS contract assures GSA we will deliver the quality services and products as specified in the RFP and that GSA's Customers will be satisfied with the services, equipment, and labor provided throughout the 15-year and optional periods of performance. For the EIS contract, CTI will focus on the following four major areas of Contract Administration, which will result in GSA:

1. Obtaining quality services, equipment, and labor that meet or exceed contract specifications
2. Achieving scheduled milestones on time
3. Completing the entire program within budget, and
4. Having a problem-free closeout

This Management Volume conforms to the following outline:

5. Section 2.1: Contains CTI's Management Response to requirements for Section G: Contract Administration Data
6. Section 2.2: Contains CTI's Management Response to requirements for Section E: Inspection and Acceptance
7. Section 2.3: Contains CTI's Management Response to requirements for Section J.2 Contractor Data Interaction Plan

CTI has separately addressed each of the Management Volume Documents. The outline for each document is Section 3.#:

1. Program Management Plan (PMP)
2. Supply Chain Risk Management (SCRM) Plan
3. Draft Business Support System (BSS) Verification Test Plan
4. Enterprise Infrastructure Solutions (EIS) Services Verification Test Plan
5. Climate Risk Management Plan
6. Financial Status Management Report (Sample)Plan
7. Business Support System (BSS) Risk Management Framework Plan

8. National Security/Emergency Preparedness (NS/EP) Functional Requirements Implementation Plan

2.1 MANAGEMENT RESPONSE TO REQUIREMENTS FOR SECTION G: CONTRACT ADMINISTRATION DATA (L.30(1), L.30.1.1)

This section provides CTI's proposal response to RFP Section G – Contract Administration Data.

2.1.1 MANAGEMENT APPROACH, TECHNIQUES, AND TOOLS TO MEET RFP SECTION G REQUIREMENTS - CONTRACT ADMINISTRATION DATA (L.30)

CTI's approach to ensuring that we meet the Contract Administration Data requirements is to: (1) ensure that roles, responsibilities, interfaces, and communications paths are clearly defined and agreed upon, (2) clearly define services, performance metrics, and associated deliverables required of each Team member and document those requirements in subcontractor agreements, (3) monitor and track Team performance levels and metrics to ensure that the services provided by the Team comply with the contract requirements, and (4) ensure each Team Member has a good understanding and knowledge of current and future customer needs.

[redacted]

CTI will leverage our current BSS/OSS tools to capture, process, and report EIS contract administration data related to functional areas that include: Ordering, Billing, Business Support Systems, Customer Support Office and Technical Support, Trouble Ticket Management, Inventory Management, Service Level Management, and Training. The techniques CTI will employ to meet Contract Administration Data requirements include applying document management principles, developing effective management reporting procedures, and interpreting the data to identify continuous improvement opportunities.

Document Management Principles, which at a minimum involve: (1) identifying all relevant documentation including contract clauses and schedules, SLAs, procedures manuals; (2) implementing change control procedures, and ensuring no changes are made without appropriate authorization; (3) recording the status of documents (current/historic, draft/final); and (4) ensuring consistency across documents.

Management Reporting Procedures, which at a minimum involve: (1) identifying when 'Exception Reporting' procedures are sufficient or when more detailed performance data

should be retained to facilitate trend analysis and problem investigations; (2) designing the format, layout, and content of management reports; (3) identifying the recipients of the management reports and their frequency of issuance; and (4) ensuring all information flows between the provider and the customer organization, and between various internal groups, are identified and tested.

2.1.1.1 Management Tools to Meet RFP Section G Requirements (L.30)

The requirements for the collection, processing, and reporting of data for contract administration purposes involve the use of different support systems, tools, and interfaces. These tools help to ensure data accuracy and overall transparency in the reporting of contract performance metrics. In the rare event of accessibility issues, Internet connectivity problems, or other situations that prevent the use of our business tools in theater, CTI relies on hard-copy forms, tools, and methods to ensure contract support is uninterrupted. For EIS, CTI will make use of our existing in-house business support systems (BSS) and tools to automate the aspects of the EIS program that are needed to meet the Contract Administration Data requirements. [redacted]

2.1.2 Approach and Capability to Provide User-Friendly, Compliant, and Efficient Support Systems (L.30.1(1a)); M.2.2(1))

CTI will support GSA and its end-user customers on EIS with an integrated set of compliant and efficient tools and professional services to meet the management and contract administration requirements for the contract including service ordering, operational support, billing, inventory, SLA management, trouble handling, training, and customer service. [redacted] The CTI BSS application provides CTI with an all-in-one solution that is a scalable, user-friendly, compliant, efficient, highly

available, platform independent, open, and extensible support system. The system provides features that match the needs of the GSA EIS vehicle. It features a tightly integrated monitoring and billing system that demonstrates specialization in usage-based billing. [redacted]

2.1.3 CAPABILITY TO PROVIDE CUSTOMERS WITH WEB-BASED ACCESS TO SUPPORT SYSTEMS (L.30.1 (1B))

The CTI Team will deliver a Web-based portal and dashboard capability to the EIS end-users providing them with real-time access to network performance data and service level agreement (SLA) information. [redacted]

2.1.3.1 Government Points of Contact (G.2.1)

CTI defines Contract Administration as providing the 'cradle to grave' management and processes that span from contract award to contract completion. Contract completion means the Government accepts the completed work (or the contract was terminated for cause); any disputes are completely resolved, and final payment is made to the vendor. Contract Administration is a process that will require close coordination and clear communications between the CTI and the Government. We acknowledge the administration of this contract will require close coordination and communications between the Government Program Management Office (PMO) and our Customer Service Office (CSO) Points of Contact (POCs).

2.1.3.2 Roles and Responsibilities (G.2.2, G.2.2.1, G.2.2.1.1-2, G.2.2.2, G.2.2.2.1-5)

When handling service orders for equipment, services, or labor CTI will only accept such orders from a warranted contracting officer or other authorized official with authority to obligate funds for the EIS customer agency. The Government official must be one who has been granted a DPA by a GSA CO to be authorized to issue or modify a TO under the EIS contract. CTI will ensure that an OCO or an authorized official (hereinafter referred to as "OCO") has the required DPA prior to processing any Task Order (TO). CTI understands that this information will be available to us via the GSA Systems. CTI complies with and understands the responsibilities and obligations of the various Agency and GSA Officials, as stated in the sub-sections of G.2.2, G.2.2.1 through G.2.2.2.5.

2.1.3.3 BSS Final Contract Acceptance (G.2.3)

CTI will complete and pass the BSS validation testing, as stated in Section E.2.1 of the RFP (contract), within 12 months from the acceptance of the BSS Verification Test Plan. We acknowledge and agree that, if we do not pass the BSS testing in the 12-month period, the Government will cancel the contract. CTI will however, receive additional time if any delays are caused by the Government. CTI further acknowledges we will not receive the Minimum Revenue Guarantee (MRG) as stated in RFP Section H.3 if the Government cancels our contract in accordance with this clause. We understand and agree that the Government will not entertain any financial claim or settlement submitted by the contractor as a result of contract cancellation.

2.1.3.4 Contract Modication (G.2.4)

CTI acknowledges the presence of this data transaction code.

2.1.3.5 Contract Closeout (G.2.5)

CTI acknowledges the presence of this data transaction code.

2.1.3.6 Past Performance (G.2.6)

CTI acknowledges the presence of this data transaction code.

2.1.4 ORDERING (G.3)

CTI will comply with RFP Section G.3 that applies to all orders (services, equipment and labor) under the EIS contract. CTI will only accept orders from entities listed in ADM 4800.2H Eligibility to use GSA Sources of Supply and Services. CTI will follow the steps as outlined below which 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 CTI.
6. Government may place service orders against the TO.

2.1.4.1 Fair Opportunity Process (G.3.1)

CTI accepts the Government's use of the Fair Opportunity Process when issuing an RFQ (Request for Quotation) or RFP. 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 include the evaluation procedures in the RFQ/RFP and establish the timeframe for responding, giving CTI a reasonable proposal preparation time while taking into account any unique requirements and circumstances. We understand and accept that all costs associated with the preparation, presentation, and discussion proposals in response will be at CTI's sole and exclusive expense.

2.1.4.1.1 eBuy (G.3.1.1)

CTI will register in eBuy to view and respond to RFQ/RFP solicitations. After registration, CTI will monitor eBuy frequently for opportunities. We acknowledge we will receive notices regarding opportunities in eBuy at CTI's registered e-mail address. When responding to a RFQ/RFP, CTI will respond in the manner specified in the RFQ/RFP solicitation.

2.1.4.2 Task Orders (TOs) (G.3.2)

CTI will not accept a TO or bill the Government for TOs or service orders received from an unauthorized person. When a TO modification is necessary during the TO period of performance, CTI acknowledges it will be the OCO that will administer the modification. CTI will submit TO summary data and pricing tables, and we will forward copies of the complete TO as described in RFP Section J.2.3 - Task Order Data Management. We affirm we will meet and comply with the processes, data, and systems requirements to support and maintain TOs as described in RFP Section J.2.3.

2.1.4.2.1 Task Order Award (G.3.2.1)

CTI acknowledges that all TOs awarded will be placed directly by the OCO and once awarded, the TO cannot be modified except by a TO modification.

2.1.4.2.2 Task Order Modification (G.3.2.2)

CTI will report TO modifications to GSA as described in RFP Section J.2.3 – Task Order Data Management.

2.1.4.2.3 Protests and Complaints (G.3.2.3)

CTI acknowledges the FAR 16.505 (a)(9)(i) exceptions to unauthorized protests in connection with the issuance or proposed issuance of an order under a TO contract.

2.1.4.2.3.1 Fair Opportunity Notice of Protest (G.3.2.3.1) [RIN: MMR0002-DN, MMR0004-DN]

CTI as per Section G.3.2.3.1 will provide a full un-redacted copy of that protest to the GSA CO within three (3) business days of the protest date. For all FOIA requests, CTI, as per the requirements in Section G.3.2.3.1, will provide a redacted copy of the FOIA to the GSA CO.

2.1.4.2.4 Customer of Record (G.3.2.4)

CTI will support the following options the Government may choose to place orders under the EIS contract: (1) GSA acting as customer of record on behalf of another agency; (2) the agency itself acting as customer of record; or (3) GSA acting as an OCO for an agency with the agency remaining as the customer of record.

2.1.4.2.5 Authorization of Orders (G.3.2.5)

CTI's proposal submission does include pricing for all mandatory services in each of the 100 top CONSU CBSAs. Therefore, if an agency issues a solicitation for a requirement in any CONUS CBSA, CTI can accept a TO or service order to provision the mandatory services for a given CBSA. If CTI is missing a CBSA, then CTI may respond to a solicitation and then submit a modification for the missing CBSA in accordance with clause H.30 Expansion of CTI Based Statistical Areas. If CTI does not have a particular optional service on its contract, and an agency issues a solicitation including that service as a requirement, CTI acknowledges we may submit a proposal or quote for the requirement provided we: (1) also submit a modification proposal to GSA to add the necessary services to its contract; and (2) we indicate we will submit a modification proposal in the TO solicitation.

As per the requirements in Section G.3.2.5, CTI shall not accept any TO or service order or provision any catalog items until the items have adequately been added to the catalog.

2.1.4.3 Ordering Services – Placement, Acceptance, and Handling (G.3.3)

CTI will accept orders for service incorporated directly within a 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 RFP Section G.3.2, CTI will accept the supplemental information to complete the order. CTI's primary objective for Service Ordering is to issue all orders accurately and on-time. Achieving this objective is extremely important to CTI because accurate service orders result in on-time delivery and installation of services and products; avoids the need for billing adjustments because the billing is accurate, thereby leaving a very positive initial impression with customer. For our EIS Customers, CTI will continuously strive to meet our service ordering objective and to provide the processes and tools that are easy-to-use, improve the delivery of existing services, simplify the delivery of new services, and improve all quality performance metrics for service ordering.

2.1.4.3.1 General Requirements for Ordering Services (G.3.3.1)

2.1.4.3.1.1 Agency Hierarchy Code (AHC) (G.3.3.1.1)

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

2.1.4.3.1.2 Auto-Sold CLINs (G.3.3.1.2) [RIN: MMR0013-DN]

CTI'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, CTI shall include those CLINs in the proposal or quote as though they had been expressly requested and ensure they are on the TO. As per Section G.3.3.1.2, all auto-sold CLINs shall be listed in all notifications and deliverables associated with an order. If new auto-sold CLINs are added through a TO modification, CTI shall issue new Service Order Completion Notices (SOCNs) for all applicable previously provisioned orders under that TO. In compliance with Section G.3.3.1.2 all newly added auto-sold CLINs shall not be applicable to any previously issued TO unless specifically added via TO modification.

2.1.4.3.1.3 Customer Want Date (G.3.3.1.3) [RIN: MMR0022-DN]

In compliance with Section G.3.3.1.3, CTI, shall make a reasonable effort to accommodate the CWD. As per Section G.3.3.1.3, CTI shall not issue the SOCN nor begin billing prior to the CWD unless the order specifies that early installation is acceptable.

2.1.4.3.1.4 Service Order Completion Notification (SOCN) (G.3.3.1.4) [RIN: MMR0025-DN]

In compliance with Section G.3.3.1.4, after completion of each service provisioning, CTI will submit a SOCN as described in Section J.2.4.

2.1.4.3.2 Order Types (G.3.3.2)

2.1.4.3.2.1 Orders to Change Existing Services (G.3.3.2.2)

2.1.4.3.2.1.1 Disconnect Orders (G.3.3.2.2.3) [RIN: MMR0028-DN, MMR0030-DN, MMR0032-DN, MMR0033-DN, MMR0034-DN]

With regard to Section G.3.3.2.2.3, CTI shall accept disconnect orders from agencies at any time. Per Section G.3.3.2.2.3, all 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. With respect to Section G.3.3.2.2.3, 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), then CTI shall notify the customer of the full list of associated Unique Billing Identifiers (UBIs). CTI per Section G.3.3.2.2.3, shall request clarification of the customer's intent to only disconnect the specified service. In compliance with Section G.3.3.2.2.3, if the customer provides instructions indicating that the list, in whole or in part, is intended for disconnect, CTI shall accept this as an order update.

2.1.4.3.2.1.2 Administrative Change Orders (G.3.3.2.2.4) [RIN: MMR0035-DN]

With regards to Section G.3.3.2.2.4, CTI shall accept administrative changes to previously provisioned orders.

2.1.4.3.2.2 Updates to In-progress Orders (G.3.3.2.3)

2.1.4.3.2.2.1 Cancel Orders (G.3.3.2.3.1) [RIN: MMR0036-DN, MMR0037-DN, MMR0038-DN, MMR0039-DN, MMR0040-DN]

In compliance with Section G.3.3.2.3.1, CTI shall accept an order from any agency to cancel a pending order at any step of the order process prior to SOCN. As per Section G.3.3.2.3.1, 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), CTI shall notify the customer of the full list of order line items that are associated. In compliance with Section G.3.3.2.3.1 CTI 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, as per Section G.3.3.2.3.1, CTI shall accept this as an order update. With respect to the Section G.3.3.2.3.1, CTI 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) CWD in the initial order or (2) the firm order commitment date.

2.1.4.3.2.2.2 Location Change Updates (G.3.3.2.3.2)

CTI acknowledges the presence of this data transaction code.

2.1.4.3.2.2.3 Feature Change Updates (G.3.3.2.3.3)

CTI acknowledges the presence of this data transaction code.

2.1.4.3.2.2.4 Customer Want Date Change Updates (G.3.3.2.3.4) [RIN: MMR0041-DN]

As per Section G.3.3.2.3.4, if the agency delays the CWD prior to receiving the Firm Order Commitment Notice (FOCN), CTI 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.

2.1.4.3.2.2.5 Administrative Data Chnge Updates (G.3.3.2.3.5) [RIN: MMR0042-DN]

CTI per Section G.3.3.2.3.5, shall accept administrative changes to in-progress orders. All administrative data is limited to data provided by the government that does not impact service delivery or pricing.

2.1.4.3.3 Special Order Handling (G.3.3.3)

2.1.4.3.3.1 Telecommunications Service Priority (TSP) Orders (G.3.3.3.1)

CTI will comply with the requirements for Telecommunications Service Priority (TSP) as stated in RFP Sections G.3.3.3.1 and G.11.3.3. A TSP assignment ensures that a service will receive priority attention by CTI before any non-TSP service. Agencies must request and obtain an Authorization Code through the NCS office prior to placing a TSP service order with CTI. There cannot be any sharing of TSP codes by multiple circuits. CTI will reject Agency TSP order requests for multiple circuits if there is only one TSP code. The authorization code is composed of 12 characters as shown in the table below.
When an Agency specifies TSP in the order, CTI will provide the service in accordance with the following telecommunications five levels of service priority, with 1 being the highest priority and 5 the lowest priority:

a) Provisioning Priorities are: E, 1, 2, 3, 4, 5 or 0 (Zero) is acceptable
b) Restoration Priorities 1, 2, 3, 4, 5 or 0 (Zero) is acceptable or
c) Both for provisioning and restoration as specified and required in the order from the Service Delivery Point to Service Delivery Point (SDP).

The TSP provisioning categories are as follows:

Emergency TSP Service: CTI notes that Emergency ("E") authorization codes apply only to service provisioning and they are applicable to certified, newly ordered services that the requesting Agency defines as critical. These services require provisioning at the earliest possible date and may incur an expedite charge.

Essential TSP Services: It will be CTI's responsibility to designate which Agency circuit will have the TSP applied to it. CTI will 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. CTI will make its best effort to implement the ordered services by the CWD, based on essential priorities as certified by the DHS Program.

CTI understands that if the Government submits a Telecommunications Service Priority (TSP) order the standard ordering process as described in the RFP Section J.2.4.2.1) will apply with the following caveats:

1. CTI will follow the prioritizations applicable to TSP orders as noted in RFP, Section G.3.3.3.1 - Telecommunications Service Priority Orders and/or Section G.11- National Security and Emergency Preparedness.
2. CTI will not delay the delivery of services in any way based on the need to submit deliverables specified in this process.

CTI will 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. Should CTI's network experience significant degradation or failure, we will 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.

2.1.4.3.3.2 Rapid Provisioning Orders (G.3.3.3.2) [RIN: MMR0043-DN, MMR0044-DN]

As per Section G.3.3.3.2 CTI agrees to specify which services it is offering that is subject to rapid provisioning and the defined provisioning interval for each such service. For Rapid provisioning, the provisioning interval shall not exceed 48 continuous hours.

With compliance to Section G.3.3.3.2, CTI agrees that the proposed provisioning interval shall be used to calculate SLA compliance as described in Section G.8.2.2.

2.1.4.3.3.3 Task Order Projects (G.3.3.3.3) [RIN: MMR0045-DN, MMR0046-DN, MMR0047-DN, MMR0048-DN, MMR0049-DN, MMR0050-DN, MMR0051-DN]

Section G.3.3.3.3 states that CTI 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, as per Section G.3.3.3.3, CTI shall provide the OCO with a single point of contact for the service implementation. As stated in Section G.3.3.3.3, CTI, 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. As per section G.3.3.3.3, CTI shall coordinate with the OCO, customers, subcontractors, vendors, and other service providers during the service implementation. In compliance with Section G.3.3.3.3, CTI shall inform the OCO and the LGC on the order when activities, including installation and cutover testing, are scheduled at a building. Section G.3.3.3.3 states that if CTI changes the installation or activation date, CTI shall notify the OCO and provide a revised date. As per Section G.3.3.3.3, unless the OCO requests an alternative outline, CTI shall include in the TOPP at a minimum the following information, and any additional information that CTI deems appropriate:

1. Name and information for CTI‘s primary point of contact.
2. Name of the OCO who awarded the TO.
3. The TO number.
4. Description of the specific activities required by all parties.
5. Specification of government equipment (hardware/software).
6. Key areas of risk for the specific project.
7. Comprehensive inventory of services to be implemented along with SDP.
8. Installation and service implementation schedule and as-of billing dates.
9. If applicable, interconnectivity or network gateways required.
10. Any special technical requirements.
11. A site-specific design plan.

2.1.4.4 Testing and Acceptance of Services Ordered (G.3.4)

CTI will meet and comply with the requirements for the verification testing of all associated EIS services based on the methodology defined in the RFP Section E.2.2 (test scenarios, test cases, test data sets, acceptance criteria) in response to the EIS Services Verification Testing. CTI shall also meet and comply with the criteria for acceptance testing defined by the agency on the TO.

2.1.4.5 Performance Management (G.3.5) [RIN: MMR0052-DN]

CTI will meet the completion timeframes associated with orders for services as defined in RFP Section G.3.3 - Ordering Services. We will also meet and comply with requirements for service provisioning intervals as defined in RFP Section G.8 - Service Level Management. CTI will comply with Service Level Agreements (SLAs) using a Methodological approach to managing those metrics and SLA reporting requirements. CTI will be responsible for services provided by our team partners and other providers that CTI will use to provide and deliver EIS services. In compliance with Section G.3.5 the completion timeframes associated with orders for services as defined in Section G.3.3 Ordering Services, CTI shall meet and comply with requirements for service provisioning intervals as defined in Section G.8 Service Level Management.

2.1.5 BILLING METHODOLOGY (G.4)

The billing process for each Task Order (TO) begins with the GSA's acceptance of the delivered services and equipment as specified in the TO and ends with the contract termination and close-out. The billing process CTI will implement for the EIS program will include the: (1) submission of billing invoice data by the contractor in accordance with the FAR 2.101 definition of "invoice"; (2) verification and validation of billing by the government; and (3) resolution of any billing disputes and adjustments.

CTI's EIS billing process will meet and comply with the processes, data, and systems interface requirements as described in RFP Section J.2.5 Billing.

2.1.5.1 Billing Prerequisites (G.4.1)

2.1.5.1.1 Billing Cycle (G.4.1.1)

CTI will comply with the Government's billing cycle. We acknowledge the billing cycle will run from the first day through the last day of the calendar month and we will base all billing on calendar month cycles. CTI will bill the Government in arrears at the end of every month after providing services.

2.1.5.1.2 Billing Start Date and End Date (G.4.1.2)

CTI will submit the SOCN to the Government prior to billing for the associated service. The SOCN contains the order completion date, which for new services is the billing start date and for disconnected services, this is the billing end date. Unless otherwise specified in the TO, the NRC price billed will be that which was in effect at the time the service order was placed and the MRC will be that which is in effect for the billing month.

2.1.5.1.3 90-Day Billing Requirement (G.4.1.3)

CTI will 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. We acknowledge that payment will not be received for a single billing charge or portion of a billing charge invoiced after 90 days. CTI further acknowledges that 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.

2.1.5.1.4 Unique Billing Identifier (G.4.1.4)

As defined in Section J.2.5, the Unique Billing Identifier (UBI) will be included on all billing. CTI will 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.

2.1.5.1.5 Agency Hierarchy Code (G.4.1.5)

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

2.1.5.1.6 Agency Service Request Number (G.4.1.6)

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

2.1.5.1.7 Electronic Billing (G.4.1.7)

The government intends to use electronic invoicing for all TOs. In addition to the billing deliverables described in Section J.2.4, CTI will input invoice summary data into the designated Government system. We will also 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), and other systems as specified in the TO.

CTI affirms we will not submit and the Government will not accept paper invoices except as authorized by the OCO.

2.1.5.2 Direct Billing (G.4.2)

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

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

2.1.5.3 Billing Functional Requirements (G.4.3)

In addition to the billing functional requirements specified in the sections that follow, CTI will comply with the processes, deliverables and data exchange requirements for billing as defined in RFP Section J.2.5 Billing. CTI will respond within seven (7) days to a billing inquiry and we will handle Government requests for Billing Adjustments and Monthly Billing Informational Memorandum.

2.1.5.3.1 Adjustments (G.4.3.1)

In the event it is necessary to adjust a bill, CTI will follow the adjustment process described in Section J.2.5 Billing. We will apply the adjustment to the next available bill. In the event of a dispute, the Billing Disputes process specified in RFP Section G.4.4 will apply.

2.1.5.3.2 Monthly Billing Informational Memorandum (G.4.3.2)

CTI will create and deliver a Monthly Billing Informational Memorandum to coincide with the monthly delivery of billing files. The Monthly Billing Informational Memorandum will list information that includes, but is not limited to, items that explain changes in billing, changes to data formats, new services added to the billing, and issues pertaining to balancing charges. Figure 1.4.1.2-1 shows the format CTI will use for the Monthly Billing Informational Memorandum.

2.1.5.4 Billing Disputes (G.4.4)

The CTI personnel, who will research Government billing inquiries, are those who are fully trained and knowledgeable regarding our billing system configuration and the procedures implemented specifically in support Government billing. CTI will accept billing inquiries during normal business hours. We will inform our EIS Customers that

billing inquiries/disputes must be accompanied with a complete description of the issue(s) and include the invoice number, date of invoice, CTI billing account number, and other billing dispute requirements as specified in RFP Section J.2.6. The name of the person making the inquiry and preferred method of communication, date of inquiry, and contact information will also be included. CTI will maintain a record of all inquiries made by GSA and its EIS customers including informal phone calls to CTI's CSO.
CTI will resolve all disputes within 180 days of the dispute notice and we acknowledge that the government reserves the right not to make payment for disputes that have not been resolved within 180 days.

2.1.5.4.1 Billing Disputes Resolution (G.4.4.1)

Billing disputes begin with the initial submission of the dispute and end with the mutually agreeable resolution of the dispute. When disputes are resolved in agreement with the customer, CTI will issue a Payment Adjustment on the next available bill.
The government may reject a bill in whole or in part within seven (7) days of receipt. 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.

2.1.5.5 Payment of a Bill by the Government (G.4.5) [RIN: MMR0007-DN]

CTI acknowledges the Government will pay only for items and services that we issue, deliver, and the Government accepts in accordance with this contract's ordering, billing, and payment procedures as stated in Section H.32 - Payments and Incorrectly Invoiced Items. CTI will submit billing 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, CTI will submit a final billing invoice within 90 days unless CTI requests and is granted an extension by the OCO in writing. We acknowledge that the government will start the Prompt Payment clock according to FAR Clause 52.232-25 upon delivery of detail billing to the government. (See Section G.4.2 Direct Billing).

2.1.5.6 Associated Government Fee (G.4.6)

CTI will collect the AGF from customer agencies on a monthly basis throughout the life of the contract and we will remit the total amount of AGF collected to GSA via EFT.

2.1.5.7 Electronic Funds Transfer (G.4.7)

CTI will accept payment of bills via EFT and we will provide the GSA with the information required to receive payment via EFT.

2.1.5.8 Government Purchase Card Payments (G.4.8)

CTI will accept payment via Government Purchase Card when authorized by the Government for telecommunications purchases under this contract. We will coordinate with our bank to obtain the appropriate Standard Industrial Classification code for the services provided under the contract and establish the Government Purchase Card financial procedures with our financial institution to ensure acceptance of such payments for billing.

2.1.5.9 Rounding of Charges for Billing and AGF (G.4.9)

CTI will use the rounding rules for billing as specified in RFP Section J.2.5.1.6 - Rounding.

2.1.5.10 Proration of Monthly Charges (G.4.10)

CTI will prorate billing based on the number of days we provide service during the billing period in accordance with RFP Section J.2.5.1.5 Proration.

2.1.5.11 Taxes, Fees and Surcharges (G.4.11)

2.1.5.11.2 Separate Billing of Taxes, Fees and Surcharges (G.4.11.1)

CTI will separate billing amounts for taxes, fees and surcharges, which we will provide as individual components or amounts on the Billing Invoice (BI), whether they are part of an original charge or an adjustment. When an Agency elects to request prices that include all taxes, fees and surcharges in its solicitation, CTI will bill the prices that were proposed, accepted, and included in the TO.

2.1.5.11.1 Aggregated Taxes (G.4.11.2)

CTI will include the aggregated tax for each line item in the billing invoice and will also provide the detailed composition of the aggregated tax in the tax detail deliverable.

2.1.5.12 Billing Performance Objectives (G.4.12)

CTI will submit accurate billing that meets the following performance objectives for billing data accuracy and billing charge accuracy:

1. All applicable data elements will be included on the BI in accordance with RFP Section J.2.10 Data Dictionary.
2. The BI will have an associated SOCN for each order.
3. The information on the BI will be consistent with that on the SOCN.
4. There will be no duplicate records within the BI.

5. There will 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 RFP Section G.4.1.3. CTI acknowledges this requirement applies to both initial invoicing and all billing adjustments.
6. The price will match the price(s) on the contract or TO.

2.1.6 BUSINESS SUPPORT SYSTEMS (G.5)

2.1.6.1 Overview (G.5.1)

CTI currently has and maintains our Business Support Systems (BSS). CTI will leverage our commercial systems to meet the BSS requirements. [redacted] The functions described in this section are the minimum that CTI will automate to meet the Government's requirements for this contract.

2.1.6.2 Technical Requirements (G.5.3)

CTI will comply with the technical requirements as stated in RFP Section G.5.3.1 through G.5.3.1.3. These requirements consist of Web Interface Functions, Technology Standards, and Accessibility.

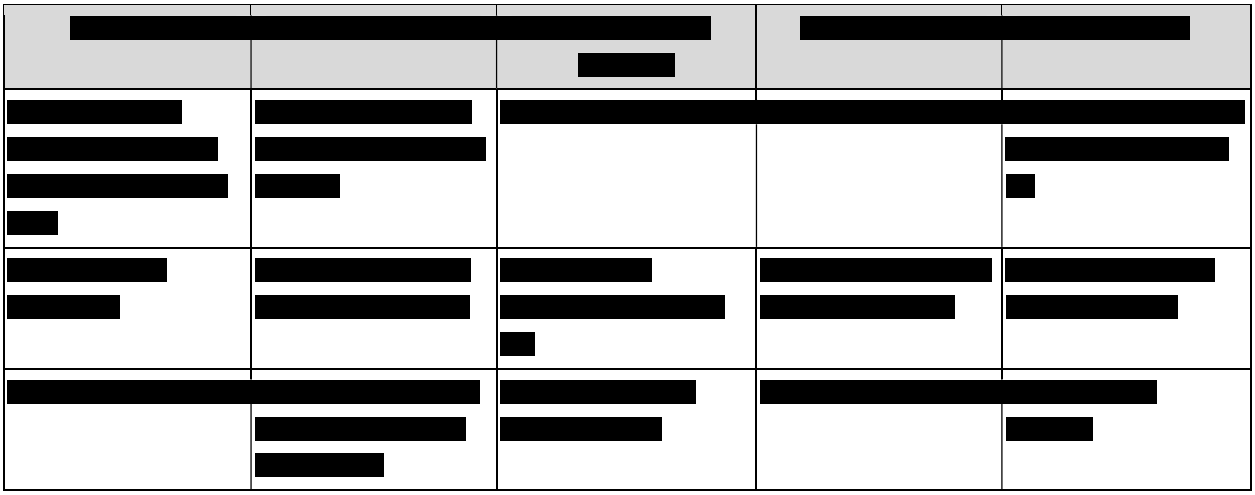
2.1.6.2.1 Web Interface (L.30.1(1a)); M.2.2(2); G.5.3.1)

[redacted] CTI's EIS web-based portal will provide end-users with online, near real-time visibility, management, and control of their communications services. EIS Customers will be capable of accessing and viewing information related to the following:

- Current and past billing information
- Trouble reporting status and incident/problem resolution,
- Change/configuration management activities throughout the Traffic Order's lifecycle
- Overall network performance based on objective Network Performance KPIs and SLAs
- Service inventory reports by account, location name, address, product, service ID, carrier

- Order tracking by date, order number, ID, status, billing and service telephone number
- Trouble Ticket Submission and Tracking by date, ticket number, your internal ticket number, service ID and status

The table below lists the attributes, features, and capabilities available from our web-based portal.



2.1.6.2.1.1 Web Interface Functions (G.5.3.1.1)

Service	Desired but no Required Functionality
Customer Management	User Training
Financial Management	Disputes & SLA Credit Management
Order Management	Order Tracking
Service Management	Service Assurance & SLA Management
Program Management	Contract Administration, Project Management, & Reporting

2.1.6.2.1.2 Technology Standards (G.5.3.1.2) [RIN:]

CTI's BSS web interface solution is easily accessible on both desktop and mobile devices through the standard web browsers in their current and immediate previous versions (N-1) as well as any successor products, including:

Miscrosoft Internet Explorer/Microsoft Edge	**Desktop & Mobile**
Google Chrome	Desktop & Mobile
Mozilla Firefox	Desktop & Mobile
Apple Safari	Desktop & Mobile

CTI's BSS solution does not require "special software or plug-ins" when using the default capabilities provided using the above mentioned web browsers.

2.1.6.2.1.3 Accessibility (G.5.3.1.3) [RIN: MMR0055-DN, MMR0056-DN, MMR0057-DN]

CTI's BSS supplied under this contract constitutes Electronic and Information Technology (EIT), as defined in FAR 2.101, and must conform to the Architectural and Transportation Barriers Compliance Board Electronic and Information Technology Accessibility Standards (36 CFR Part 1194), parts B, C and D as amended. CTI 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 Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR 1194. CTI shall also identify the technical standards applicable to all products proposed. In addition, CTI shall clearly indicate where this list with full details of compliance can be found (e.g., an exact web page location). CTI shall ensure that the list is available on CTI's website(s) within 30 days of Notice to Proceed (NTP). CTI will ensure that all EIT products, in compliance with section G.5.3.1.3, that are less than fully compliant that are offered are subjected to extensive market research, which ensures that they are the most compliant products available to satisfy the solicitation's requirements. As per Section G.5.3.1.3, if any EIT product proposed is not fully compliant with all the standards, CTI 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. CTI shall make the BSS Voluntary Product Accessibility Template (VPAT) available on its website www.coretechinc.com (See http://www.itic.org/policy/accessibility) and shall directly address compliance with Section 508 in the following deliverables: BSS Development and Implementation Plan, BSS Verification Test Plan, and BSS Verification Test Results.

2.1.6.2.2 Direct Data Exchange (G.5.3.2)

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

2.1.6.2.2.1 Direct Data Exchange Methods (G.5.3.2.1)

2.1.6.2.2.2 Direct Data Exchange Formats (G.5.3.2.2)

CTI's BSS will accept data transfers from the government and submit data to the Government in the formats specified in RFP Section J.2.9.

2.1.6.2.2.3 Direct Data Exchange Governance (G.5.3.2.3)

CTI accepts that GSA will maintain and manage all approved data exchange format specifications, data schemas, and method descriptions. We acknowledge that the Government Customer may also specify additional data exchange requirements in the TO. The Government and CTI will coordinate and negotiate any changes or updates, to include timeframes for implementation. Once the BSS is operational, CTI will not make any changes to the data exchange formats or methods without Government approval via the established change control process as specified in RFP Section G.5.5.1 – BSS Change Control.

2.1.6.2.3 Role Based Access Control (RBAC) (G.5.3.3)

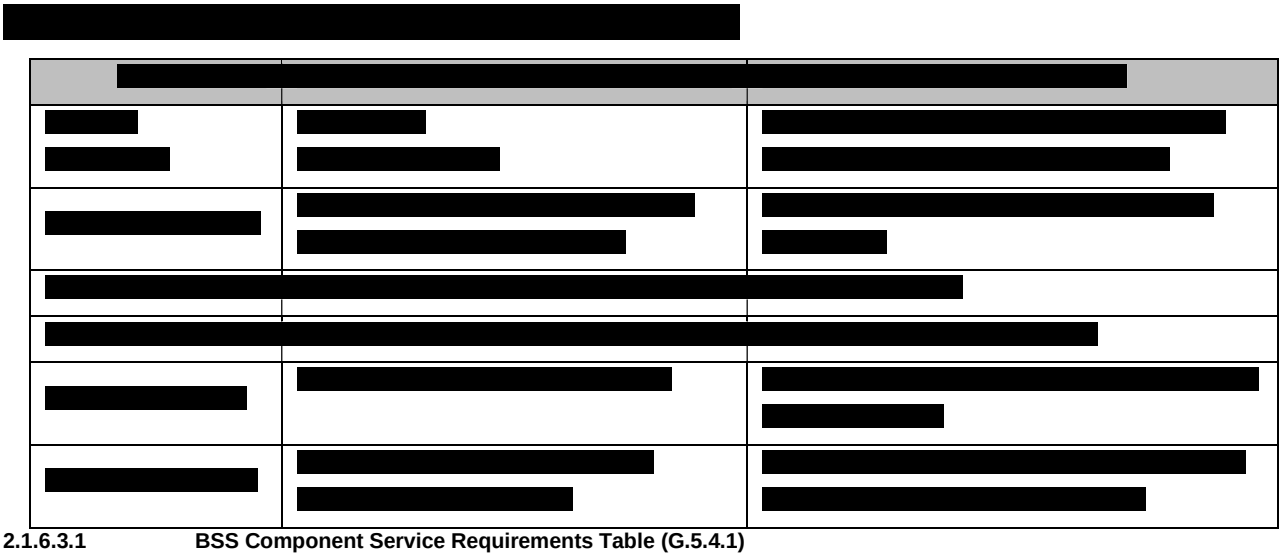
Role-based Access Control (RBAC) is a control considered to be most appropriate and central to the secure processing needs within civilian Government agencies. CTI will apply RBAC to allow access and assigned permission to our Business Support Systems (BSS) from only authorized Government customers. [redacted]

RBAC contains a list of defined business roles. The Administrator assigns each user added to the system to one or more roles. The Administrator then grants permissions and privileges to each role, and users receive them via their membership in the role, which is very much equivalent to a group. The BSS applications using RBAC will test the user for membership in a specific role, and grant or deny access based on that. The main benefit of RBAC is ease of management because, in principle, there are very few roles that are centrally administered, no matter how many users; CTI knows, however, we must assign each user the correct role. CTI will add new users within seven (7) days of receiving an Agency customer request. CTI's objective will be to arrange for the immediate removal of users who no longer have access authorization to our BSS and we affirm all removals will occur within one (1) business day.

2.1.6.2.4 Data Detail Level (G.5.3.4)

The data provided by the BSS will be in sufficient detail to provide all data elements relating to the services listed in RFP Section G.5.4 BSS Component Service Requirements. As required in RFP Section J.2, CTI will submit all BSS deliverables and reports in at least the following formats: (1) Human-Readable made available via the web interface unless otherwise specified in the TO; (2) Machine-Readable using the file types specified in RFP Section J.2.9 as part of the direct data exchange as described in Section G.5.3.2 – Direct Data Exchange.

2.1.6.3 BSS Component Service Requirements (G.5.4)



2.1.6.3.1 BSS Component Service Requirements Table (G.5.4.1)

2.1.6.4 BSS Development (G.5.5) [RIN: MMR0061-DN]

As per the requirement in Section G.5.5, CTI shall be solely responsible for all development, testing, and maintenance including, but not limited to, security validation, functional testing, and configuration control. CTI's BSS Development and Implementation Plan is submitted within the Program Management Plan in section 3.1 of this Management volume. This plan details how the BSS supporting this contract will be architected and supported to meet GSA's requirements including the development timeline. 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. CTI shall be solely responsible for all development, testing, and maintenance including, but not limited to, security validation, functional testing, and configuration control.
CTI shall provide, as per Section G.5.5, upgrades to its BSS at no additional cost to the government, as these upgrades become available to its commercial customers.

2.1.6.4.1 BSS Change Control (G.5.5.1)

CTI will 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, we will notify the government as soon we discover that a change is required. For those changes that meet the standard for being subject to change control, CTI will:

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.
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.

2.1.6.5 BSS Security Requirements (G.5.6) [RIN: MMR0062-DN]

With respect to Section G.5.6, CTI shall also support the government‘s efforts to verify that these specific standards are being met.

2.1.6.5.1 General Security Compliance Requirements (G.5.6.1)

See Section 3.7.1.1 of this Management volume, within the BSS Risk Management Framework Plan.

2.1.6.5.2 GSA Security Compliance Requirements (G.5.6.2) [RIN: MMR0064-DN]

CTI's Risk Management Framework Plan describing our approach for BSS security compliance is submitted with this proposal in accordance with NIST SP800-37. This plan is submitted in section 3.7 of this Management volume.

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

See Section 3.7.1.3 of this Management volume, within the BSS Risk Management Framework Plan.

2.1.6.5.4 BSS System Security Plan (BSS SSP) (G.5.6.4) [RIN: MMR0067-DN, MMR0068-DN, MMR0070-DN]

CTI will 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. CTI will complete the BSS SSP 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 will 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 will create, maintain and update the security A&A documentation as specified in RFP Section 5.6.4(1) through 5.6.4(24q). In accordance with the GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines (Level 1), and industry best practices in hardening systems, the systems will be configured as deemed appropriate by the AO. CTI will develop and maintain a Plan of Action and Milestones (POA&M), which will be completed in agreement with the GSA IT Security Procedural Guide 06-30. All scans associated with this POA&M will be performed as an authenticated user with elevated priviledges. In accordance with NIST SP 800-53 R4 / NIST SP 800-53A R4 and the GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk", CTI will allow GSA employees (or GSA-designated third-party contractors) to conduct security A&A activities to include control reviews.

2.1.6.5.5 CTI's BSS Security Focus

CTI's BSS has introduced a program that ensures our systems undergo Privacy and Security Assessments on a regular basis. These assessments are also entrenched in the "technical security" and "data protection" aspects early on in our system development processes. Security is a top priority at CTI and we consider it to be a

system design factor because it's about ensuring our company's future and sustainability.Reserved (G.5.6.5)

2.1.6.5.6 Additional Security Requirements (G.5.6.6)

Where appropriate, CTI will 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."). We will cooperate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the Federal Government's agent.

CTI acknowledges and accepts 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) CTI will be responsible for the following privacy and security safeguards:

1. CTI will 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. As required to safeguard against threats and hazards to the security, integrity, and confidentiality of non-public Government data that CTI collect and stores, we will provide the Government with logical and physical access to our facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits will include, but are not limited to, the following methods:
    d) Authenticated and unauthenticated operating system/network vulnerability scans
    e) Authenticated and unauthenticated web application vulnerability scans
    f) Authenticated and unauthenticated database application vulnerability scans
    g) Internal and external penetration testing
3. Government personnel can perform automated scans, or agents acting on behalf of the government, using government operated equipment, and government specified tools. When CTI runs its own automated scans or audits, results from

these scans the Government may, at its discretion, accept those scans in lieu of government performed vulnerability scans. In these cases, CTI acknowledges the Government will approve the scanning tools and their configurations and CTI will provide the results of the scans, in full, to the Government.

2.1.6.5.6.1 Personnel Security Suitability (G.5.6.6.1)

CTI will perform personnel security/suitability in accordance with FAR Part 52.204-9, Section I. Prior to any CTI personnel having access to Government information that is within the security A&A scope, they will have to undergo a successful 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 2100.1I and GSA Directive 9732.1D Suitability and Personnel Security. CTI acknowledges that the Government will be responsible for the cost of such background investigations.

2.1.6.6 Data Retention (G.5.7)

Data Retention is important to CTI, and we understand and will 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 EIS contract.

2.1.7 SERVICE ASSURANCE (G.6)

2.1.7.1 Customer Support Office (G.6.1)

CTI will establish a Customer Support Office (CSO), which will be the primary interface between CTI and Government entities that are interested in or using the EIS contract.

[redacted]

2.1.7.2 Customer Support Office and Technical Support (G.6.2) [RIN: MMR0072-DI]

[redacted]When customers call the toll-free number, they will

speak with a single Point of Contact (POC) who will be individuals dedicated to specific agencies. [redacted] CTI's Program Manager, who will act as the primary interface to the GSA's EIS Contracting Officer Technical Representative (COTR), will direct the PMO. For each Task Order (or multiple Task Orders depending on the size and complexity), we will assign a thoroughly trained and professional Task Leader who will be responsible to the Project Manager for ensuring successful performance on their assigned tasks. The Tasks Leaders will be assigned based upon their knowledge and ability to manage a specific task, and may be assigned from any of the CTI Team members. [redacted]

CTI will provide technical support to agencies and the PMO regarding the services CTI will deliver to the government. Technical support will 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

2.1.7.3 Supply Chain Risk Management (G.6.3)

CTI's Supply Chain Risk Management Plan is submitted within Section 3.2 of this Management volume.

2.1.7.3.1 Plan Submittal and Review (G.6.3.1)

CTI agrees and will comply with the requirements in the RFP Section G.6.3.1 for SCRM Plan Submittal and Review, CTI will submit this plan with our EIS proposal. CTI will submit updates on an annual basis to the Contracting Officer (CO) and Contracting Officer Representative (COR).We will treat all SCRM Plan information as Controlled Unclassified Information pursuant to Executive Order 13556, and we will share it only with Government agencies, and we will use the information solely for the purposes of mission essential risk management. We acknowledge the Government will complete all reviews within a 45 – day time period.

2.1.7.4 Trouble Ticket Management (G.6.4)

CTI will perform trouble ticket management in accordance with commercial best practices, and we will meet the Government's requirements as specified below in RFP Section G.6.4.1 Trouble Ticket Management General Requirements.

2.1.7.4.1 Trouble Ticket Management General Requirements (G.6.4.1)

CTI will 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. CTI will 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 the RFP Section G.8 Service Level Management.
As the first priority, CTI will restore any Telecommunications Service Priority (TSP) restoration coded service, as quickly as possible, using best effort. CTI will escalate issues according to our Program Management Plan (PMP) as described in the RFP Section G.9.4 Program Management Plan.

2.1.7.4.2 Reporting Information (G.6.4.2)

CTI agrees with the Reporting Information in RFP Section G.6.4.2 and will 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. CTI will process any credits applicable to the service outage based on this record of information. The approach we will use for SLAs and credits are as defined in RFP Section G.8 - Service Level Management. CTI will, upon request from the PMO and agencies, deliver archived trouble and complaint report data within five (5) days of the request for such information.

2.1.8 INVENTORY MANAGEMENT (G.7)

CTI will comply with the RFP requirements as stated in RFP Section G.7 - Inventory Management through RFP Section G.7.1.5 EIS - Inventory Reconciliation.

2.1.8.1 Inventory Management Process Definition (G.7.1)

CTI will establish, and keep current a complete and accurate Inventory Management Process of EIS services provided to agencies. CTI will 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. CTI has read and will comply with the technical details for this interface as defined in the RFP Section G.5.3.1 Web Interface [redacted]

CTI will perform the key tasks associated with inventory management as defined below:

1. GSA identifies the minimum inventory data elements required by service as part of the Inventory Reconciliation (IR) deliverable and specified in the RFP 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 will advise CTI of discrepancies noted in the EIS inventory data.
4. CTI will investigate EIS inventory data discrepancies reported by the government and works with the government to resolve them.
5. CTI will make corrections to the EIS inventory as needed to maintain its accuracy and completeness and issues corrected SOCNs or billing as needed.
6. CTI will meet the inventory requirements for transition as defined in the RFP Section C.3 Transition; (Transition Roles and Responsibilities, Transition On, and Transition Off).

2.1.8.1.1 Inventory Management Functional Requirements (G.7.1.1)

CTI will perform the key functional requirements related to Inventory Management as follows:

1. CTI will fully populate the EIS Inventory with the data elements of the IR as defined in the RFP Section J.2.7 Inventory Management.
2. CTI will 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.

    h) CTI will establish an inventory for all EIS services provided to its customers.

    i) CTI will maintain and update the EIS inventory for all EIS services provided to its customers.

    j) CTI will make the EIS inventory data available to the government.

3. CTI will deliver an Inventory Reconciliation (IR) deliverable each month as defined in the RFP Section J.2.7 Inventory Management.

2.1.8.1.2 EIS Inventory Maintenance (G.7.1.2)

CTI agrees and understands the requirements of the RFP Section G.7.1.2 for EIS Inventory Maintenance. CTI will maintain and update the EIS Inventory for all EIS

services provided to its customers. CTI also will 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.

2.1.8.1.3 EIS Inventory Data Availability (G.7.1.3)

CTI will provide the GSA and EIS Agency customers with a web-based interface and access to inventory data. In so doing, CTI will:

1. Provide to Government users secure electronic access to the current view and to the monthly snapshots of EIS services in CTIs maintained EIS inventory
2. For secure web-based queries against CTI's maintained EIS inventory, CTI will, as a minimum: (a) provide Government users the option to select a user choice of online viewing, data file downloading, and (b) provide and maintain on its EIS BSS web interface a link for secure, electronic access to CTIs maintained EIS inventory information.
3. For data export or data file delivery in response to a secure query against CTI's maintained EIS inventory, CTI will, at a minimum: (a) support common industry standard formats and file structures, and (b) impose no limit on the number of records that is less than the limit imposed by the file format specification
4. Make archive older monthly snapshots of the EIS inventory and these archives will be available for Customer 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 the RFP Section G.5.6 - BSS Security Requirements for the system used for the EIS inventory
7. If requested by the Government, and at no additional expense to the Government, provide a copy of the inventory records to the Government, 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, and 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. CTI will 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.

2.1.8.1.4 EIS Inventory Data Discrepancies and Accuracy (G.7.1.4)

2.1.8.1.4.1 EIS Inventory Data Discrepancies (G.7.1.4.1)

CTI will comply with EIS Inventory Data Discrepancies in the RFP for Section G.7.1.4.1. CTI will investigate EIS inventory data discrepancies reported by the government. If CTI agrees to a correction, it will correct the data discrepancies within ten (10) days. If CTI does not agree to a correction, it will advise the Government and work with the Government to resolve the issue. If the discrepancy is escalated to the CO for resolution, CTI will work with the CO to resolve the issue to the government's satisfaction.

2.1.8.1.4.2 EIS Inventory Data Accuracy (G.7.1.4.2)

CTI agrees to the RFP requirements for Section G.7.1.4.2 EIS Inventory Data Accuracy. CTI will institute internal verification and audit procedures to ensure that the EIS inventory is complete and correct. When CTI discovers an EIS inventory data discrepancy, agrees with a government report of a discrepancy, or is directed to do so by the CO, CTI will correct its EIS inventory at no additional cost to the government. When CTI 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, CTI will 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. If the EIS inventory data elements in the SOCN issued to the government were in error, CTI will issue, at no additional cost to the government, a corrected SOCN or a new correct SOCN that clearly references the original error. If the EIS inventory data elements result in a billing error in the BD

deliverable issued to the government, CTI will issue, at no additional cost to the government, a Billing Adjustment (BA) deliverable. CTI will correct data discrepancies as they occur and as designated by the government within ten (10) days.

2.1.8.1.5 EIS Inventory Reconciliation (G.7.1.5)

CTI will provide the monthly Inventory Reconciliation deliverable as required in RFP Section G.7.1.5 and as defined in RFP Section J.2.7 – Inventory Management.

2.1.9 SERVICE LEVEL MANAGEMENT (G.8)

2.1.9.1 Overview (G.8.1)

CTI understands that an SLA is an agreement between the Government and CTI to provide a service at a performance level that meets or exceeds the specified performance objective(s). CTI acknowledges the contract has specific KPIs for nearly all services. If CTI offer's this service, we understand we must comply with those KPIs. For each KPI, CTI will meet specified AQLs. Certain services deemed essential to Government operations also require mandatory SLAs. If we do not meet the specified service levels, then CTI will issue specified credits. The following are major components: Service Level Agreement Tables (all SLAs under the EIS contract), Service Level General Requirements, SLA Credit Management Methodology, and Service Level Reporting Requirements.

2.1.9.2 Service Level Agreement Tables (G.8.2)

2.1.9.2.1 Service Performance SLAs (G.8.2.1)

2.1.9.2.1.1 Service-Specific SLAs (G.8.2.1.1)

CTI understands that the Service-Specific SLAs are as defined in the table provided in RFP Section 8.2.1.1.1 – Service Specific SLA Table. CTI will meet the Section C performance metrics (AQLs) for the KPIs specified in both Section C and Section G.8.2. For each service SLA, CTI will meet the AQL associated with each KPI listed. We will measure and report on KPIs for each unique instance of a service as defined by the UBI. We acknowledge that failure to meet the AQL for any KPI within an SLA constitutes failing that SLA.

2.1.9.2.1.1.1 Service-Specific SLA Table (G.8.2.1.1.1)

2.1.9.2.1.1.2 Service-Specific SLA Credit Formulas (G.8.2.1.1.2) [RIN:MMR0003-DN]

With respect to the occurrence of each failed SLA, CTI shall apply the associated credit in accordance with Section G.8.4 SLA Credit Management Methodology practices and procedures. In the event that CTI misses a required SLA, the following will hold true:

As per Section G.8.2.1.1.2 is "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:

a) For the first month missing a particular SLA during the six-month window:
    a. 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.
b) For the second month missing the same SLA during the six-month window:
    a. 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.
c) For the third (or any subsequent) month missing the same SLA during the six-month window:
    a. 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.
d) The agency may also choose to cancel the affected service without penalty."

2.1.9.2.1.2 Incident-Based Service SLAs (G.8.2.1.2) [RIN: MMR0005-DN]

Upon the occurrence of a service outage, CTI, shall calculate the TTR using the following methodology:

1. Determine 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, which may include:
    a. The customer was not available to allow CTI to access the Service Delivery Point or other customer-controlled space or interface

b. The customer failed to inform CTI 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, not appropriately met, as per Section G.8.2.1.2, CTI will meet the AQL for the matching KPI associated with the service affected by the incident.

2.1.9.2.1.2.1 Incident-Based Service SLA References (G.8.2.1.2.1)

2.1.9.2.1.2.2 Incident-Based Service SLA Credit Formula (G.8.2.1.2.2)

In the occurrence of a failed SLA, CTI as per Section G.8.2.1.2.2, 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:

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

2.1.9.2.1.3 Service-Related Labor SLAs (G.8.2.1.3)

2.1.9.2.2 Service Provisioning SLAs (G.8.2.2)

CTI has read and is in agreement with the requirements of Service Provisioning SLAs in the RFP Section G.8.2.2, Section J.2.4 Ordering and Section G.3.3.1.3.

CTI understands that the SLAs for the provisioning of services under the contract are defined in the subsections below: Standard Provisioning SLAs, ICB Provisioning SLAs, and 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 will be governed by the longest provisioning interval.

As described in RFP 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.

2.1.9.2.2.1 Standard Provisioning SLAs (G.8.2.2.1)

With respect to Section G.8.2.2.1, CTI, shall complete all orders within the provisioning intervals defined in the associated table below. In addition, the failure to complete the provisioning of service within the specified timeframes shall constitute a failure to meet the SLA for that provisioning incident.

Service	Orders SLA (Days)
Disconnect (all services)	30
Circuit Switched Data Services (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

As required by Section G.8.2.2.1 if CTI fails to complete the provisioning of service within the specified timeframes it shall constitute a failure to meet the SLA for that provisioning incident.

2.1.9.2.2.1.1 Standard Service Provisioning Intervals (G.8.2.2.1.1)

2.1.9.2.2.2 Individual Case Basis Provisioning SLAs (G.8.2.2.2)

It is agreed that certain service provisioning tasks do not have predefined provisioning intervals. For these services, the performance objective shall be defined on an individual case basis (ICB) with the required delivery schedule established in the TO. As required by Section G.8.2.2.2 if CTI fails to complete the provisioning of service within the specified timeframes, as per the TO, it shall constitute a failure to meet the SLA for that provisioning incident.

2.1.9.2.2.2.1 Services Subject to ICB Provisioning Intervals (G.8.2.2.2.1)

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

2.1.9.2.2.3 Project Provisioning SLAs (G.8.2.2.3) [RIN: MMR0023-DN, MMR0024-DN, MMR0026-DN]

In compliance with Section G.8.2.2.3, for project orders (orders that require special treatment by CTI due to the size, complexity, or importance of the services ordered), the

performance objective will be based on the baseline completion dates in the Task Order Project Plan (TOPP) agreed upon and documented by the government and CTI at the time orders are placed and confirmed by CTI. With respect to Section G.8.2.2.3, for these services, the performance objective shall be defined on an individual case basis (ICB) with the required delivery schedule established in the TO. As per Section G.8.2.2.3 CTI's Failure to complete the provisioning of service within the timeframes specified in the TOPP shall constitute a failure to meet the SLA.

2.1.9.2.2.4 Rapidly Provisioned Services (G.8.2.2.4)

2.1.9.2.2.4.1 Cloud Service Provisioning (G.8.2.2.4.1) [RIN: MMC0018-DI, MMR0009-DN]

The requirement in Section G.8.2.2.4.1 requires that CTI shall propose cloud provisioning interval KPIs and SLAs with a methodology to track and monitor each SLA and KPI. CTI is currently proposing the mandatory 48 hour continuous time frame installation as requirement by section G.3.3.3.2 Rapid Provisioning Orders demands. Any additional SLAs or KPIs will be based on the Agencies specific environments and requirements at the TO or Contract level and associated credits will match or exceed those defined in G.8.2.2. CTI uses internal business management software to track and provision all services including the SLA / KPIs required by G.3.3.3.2 in each of the Cloud Services below. CTI currently utilizes UberSmith commercial software to manage and track ordering, confirmation, provisioning intervals, provisioning completion, testing and turn-up of all Cloud Services.

Service	Service ID	KPIs Defining the Service-Specific SLA	Section C Reference
Infrastructure as a Service	IaaS	Availability (IaaS Data Center Infrastructure)	C.2.5.1.4
Platform as a Service	PaaS	Availability (PaaS)	C.2.5.2.4
Software as a Service	SaaS	Availability (SaaS)	C.2.5.3.4
Content Delivery Network Service	CDNS	Availability & GOS (Time to refresh content)	C.2.5.4.4

G.8.2.1.1.1 – Service Spefici SLA Table

Service
Cloud Infrastructure as a Service (IaaS)
Cloud Platform as a Service (PaaS)
Cloud Software as a Service (SaaS)
Cloud Content Delivery Network Service (CDNS)

G.8.2.2.2.1 – Services Subject to ICB Provisioning Intervals

2.1.9.2.2.4.2 Bandwidth-on-Demand (G.8.2.2.4.2)

CTI will support Bandwidth-on-Demand as described in Section C.2.1.2 - Ethernet Services. We will support bandwidth increments and decrements on demand, as agreed between CTI and the Agency. Unless otherwise agreed by the Agency and CTI on a case-by-case basis, CTI will meet the 24-hour provisioning time interval for Bandwidth-on-Demand Change feature as specified RFP Section G.8.2.2.4.2. This measurement interval will be from the service order to the SOCN.

2.1.9.2.2.4.3 Other Services Subject to Rapid Provisioning (G.8.2.2.4.3) [RIN:MMR0010-DN]

CTI is offering IaaS solutions in this vehicle and as such, if a customer requests rapid provisioning via a service order in the Contract or TO and the order does not contain an Administrative Change Order, CTI will work with them to ensure the services are provisioned in the 48 hour continuous time frame demanded by section G.3.3.3.2 Rapid Provisioning Orders. If the 48 hour time frame is not met, CTI understands that it is subject to the SLA calculations as described in Section G.8.2.2. Outside of the 48 hour continuous timeframe, CTI does not currently offer any additional “rapid provisioning” SLAs or KPIs across the service, but will negotiate at the TO or Contract level with the Agencies that demand additional SLAs or KPIs based on their specific environments.

2.1.9.2.2.5 Service Provisioning SLA Credit Formulas(G.8.2.2.5)

For each failed SLA, CTI will apply the associated credit in accordance with RFP Section 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).

2.1.9.2.3 Billing Accuracy SLA (G.8.2.3)

CTI will submit accurate billing that meets the performance standards for Billing Accuracy for each TO as defined in Section G.4 - Billing. We acknowledge that failure to meet the accuracy standards as defined in that section will constitute failing to meet the Billing Accuracy SLA. If this SLA is failed, CTI will apply the associated credit in accordance with Section 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.

2.1.9.3 Service Level General Requirements (G.8.3)

CTI will be responsible for meeting all SLA requirements as defined in RFP 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.

2.1.9.3.1 Measurement (G.8.3.1)

CTI will measure each SLA in accordance with its definition provided in RFP Section G.8.2 - Service Level Agreement Tables. As per Section G.8.3.1, CTI will list all procedures for measuring and sampling and such shall be described in the quality assurance section of the Program Management Plan.

2.1.9.3.2 Reporting (G.8.3.2)

CTI will provide service level management reports as detailed in RFP Section G.8.5 - Service Level Reporting Requirements.

2.1.9.3.3 Credits and Adjustments (G.8.3.3)

In cases where CTI does not meet the defined contractual or TO SLA, we will provide credits and/or adjustments to the Government agency of record or to GSA using the as further detailed in Section 8.4 - SLA Credit Management Methodology

2.1.9.4 SLA Credit Management Methodology (G.8.4)

If CTI fails to meet the performance objectives specified in the SLAs defined above, the Government is entitled to receive credit within two billing cycles. We will calculate the amount of credit due as specified in the applicable portion of RFP Section G.8.2 - Service Level Agreement Tables. In cases when there are multiple SLA failures and therefore multiple credits are due, the sum of all credits paid will be with the limitation that the total maximum penalty on a service in a given month will not exceed the total billed cost for that service. CTI acknowledges that the Government may grant a waiver from all or part of a credit if exceptional circumstances warrant. The TO on the bill identifies the Customer that will receive the credit and that Customer may grant a waiver for all SLAs.

2.1.9.4.1 Credit Management (G.8.4.1)

CTI acknowledges that the GSA CO, OCO, or authorized ordering official may submit an SLA Credit Request (SLACR) to CTI as defined in RFP Section J.2.8 - SLA Management. In addition, the GSA CO or OCO may designate, in writing, additional personnel or systems authorized to submit SLACRs to CTI. CTI also acknowledges that the Government reserves the right to submit a SLACR at any time within six (6) months

of the original SLA failure. CTI will respond to the request within 30 days by submitting a SLACR response and we will issue the credit within two billing cycles of this response unless CTI chooses to reject the request. In cases where CTI chooses to reject the request, we will work with the Government to resolve any disputes and agree on an appropriate credit award in accordance with RFP Section G.4.4 - Billing Disputes.

2.1.9.5 Service Level Reporting Requirements (G.8.5)

CTI will comply with the Service Level Reporting requirements specified in RFP Sections G.8.5 through G.8.5.2.4.

2.1.9.5.1 Report Submission (G.8.5.1)

Unless otherwise specified, each report that CTI submits will be TO-specific and each report will address only those actions and metrics applicable to the TO in question. CTI will submit these reports electronically via our web interface and via direct data exchange as specified in RFP Section G.5.3.

2.1.9.5.2 Report Definitions (G.8.5.2)

2.1.9.5.2.1 Service Level Agreement Report (G.8.5.2.1)

In the Service Level Agreement Report (SLAR), CTI will document monthly SLA performance covering all aspects of service including incident-based SLAs, service-specific SLAs, service provisioning SLAs, and program management SLAs. CTI will deliver this report on the 15th day of each month.

2.1.9.5.2.2 SLA Credit Request (SLACR) Response (G.8.5.2.2)

CTI's SLA Credit Request (SLACR) response will document CTI's response to a Government request for SLA credits as described in RFP Section G.8.4.1 - Credit Management. CTI will deliver this response within 30 days after the receipt of an SLACR.

2.1.9.5.2.3 Trouble Management Performance Summary Report (G.8.5.2.3)

Unless otherwise specified by the TO, CTI will use its standard commercial report format for this report ensuring that it contains the information specified. CTI will deliver this report within 14 days after the end of each FY quarter.

2.1.9.5.2.4 Trouble Management Incident Performance Report (G.8.5.2.4)

The Trouble Management Incident Performance Report that CTI will issue will document trouble management incident-level performance by describing each trouble report issued during the reporting period by the CTI trouble report number, Agency and AHC, UBI, time opened, and time resolved. Unless otherwise specified by the TO, CTI

will use its standard commercial report format for this report ensuring it contains the information specified. CTI will deliver this report within 14 days after the end of each FY quarter.

2.1.10 PROGRAM MANAGEMENT (G.9)

Our Program Manager is the single point of accountability to GSA and GSA's Agency Customers. CTI will create a fully functional Customer Support Office (CSO) into which we will integrate our CTI Team member resources and services. We will customize our Business Support Systems and management tools and we will assign dedicated, experienced personnel to support the EIS Customer Agencies. Management and operations involves the planning, scheduling, and control of the activities that transform inputs (the EIS RFP requirements) into outputs (CTI's delivered products and services). It involves having well developed and tested tools and proven techniques. Our 18-year corporate success stems from our superior products and services, the fact we ensure compliance with federal, state, and local regulations, and our adherence to safety standards, industry standards, and best practices guidelines. CTI's compliance with the Program Management requirements under the EIS Program will remain in effect through the duration of the EIS contract. As the Prime Contractor for the EIS Program, CTI's primary Program Management objective is to staff each project with the most qualified personnel and subcontractors. We are committed to assigning EIS support personnel that have the requisite capabilities and expertise to ensure we provide a fully responsive Customer Service Office (CSO). Our EIS CSO personnel will communicate directly with the Agencies and with GSA. The personnel we assign to support Program Management will be qualified, competent people who are current CTI and Team Member employees. We monitor staff performance on a regular basis and use performance data metrics to measure both individual and Service Area performance metrics. We compile performance through the use of CTI's Project Management System (CPMS).

CTI has structured our program management team and company organization to drive high quality and responsive staff performance levels that in turn will provide the best telecom solutions and support for GSA and EIS Customer Agencies. CTI sponsors training programs, certification programs, knowledge building, knowledge sharing,

participation in industry seminars and conferences, and team building exercises. We are a results driven company and we recognize the significant value-added benefits that our well-trained, professional employees extend to our customers, partners, and vendors.

CTI's management team and staff are committed to fully supporting the GSA's EIS Program ensuring, to the extent possible, a problem-free installation, transition, and on-going support and maintenance for the EIS program. We will conduct regularly scheduled meetings with key personnel to ensure we are meeting program and project (Task Order) schedules and, as needed, assigning/allocating the appropriate number of resources to meet the specified requirements. CTI will dedicate additional resources to the program in the form of systems, tools, and facilities to ensure we meet or exceed objective levels of network performance and customer support services metrics. We are fully committed to implementing a Program Management structure that strengthens the probability of achieving problem-free and very successful results for EIS transition, implementation, on-going operations, maintenance, and customer services.

2.1.10.1 Contractor Program Management Functions (G.9.1)

This section presents CTI's program management functional organization as well as our plan for managing and maintaining control over the multiple products, multiple disciplines, and multiple EIS Agency locations that we will support immediately upon contract award. Our management approach incorporates industry best practices including Project Management Institute Bodies of Knowledge (PMBOK®) and proven processes and procedures that we use successfully on other contracts. To further ensure immediate response to all task requirements upon contract award, CTI and our Team Members have already identified the personnel who will be available to support tasks under this contract. As evidenced in this section, CTI has the processes, procedures, resources, and facilities in place to provide the following EIS program management functions immediately upon contract award: Program Control, Program Level Planning, Agency Level Planning, Contractor Performance, Resource Management, Revenue Management, Reporting and Reviews; and Senior-Level Communication.

2.1.10.1.1 Program Control

CTI will closely manage progress of both the technical and program management actions and the cost effective use of personnel and equipment resources. [redacted]

CTI's program control information structure used to control the flow of program information. This information control structure is designed to maintain control over information flowing to and from multiple tasks, multiple products, multiple technical disciplines, and multiple EIS customers. [redacted] Our process allows the Program Manager to control the required work throughout the EIS program life cycle. Moreover, it ensures program objectives are achieved within the established milestones and cost constraints. [redacted]

2.1.10.1.2 Planning at the Program Level

Program Level Planning is the responsibility of the Program Manager (PM). [redacted]

[redacted]

2.1.10.1.3 Planning at the Agency Level

CTI's Project Management personnel will perform Agency Level Planning, which will include assisting in creating the project plan, maintaining the project plan, creating, maintaining, and managing a critical milestone schedule and work breakdown structure for transition and implementation tracking purposes. The purpose of Agency level planning is to identify and document the task order transition and operational requirements in terms of scope, business requirements, task activities, schedules, costs, risk, quality, and staffing needs. This phase includes all the activities necessary for the Project Manager to establish the project staffing, project infrastructure, and stakeholder accountability, along with all the project management plans, including the appropriate levels of pre-planning documentation for the follow-on phases. [redacted]We review and update the Project Management Plans as needed at the end of each project phase and we consistently revise and improve these plans throughout the project.

2.1.10.1.4 Contractor Performance

CTI embraces the benefits of using Earned Value Management (EVM) techniques and metrics for expressing and evaluating progress within the baselines of a program or project, which are cost, schedule, and technical performance. EVM does not use a specific system or tool set, but rather, EVM is a set of guidelines that are the basis of CTI's ability for effective program control.

[redacted]

[redacted]

We design our contractor performance metrics to measure program and project results with customer satisfaction as our number one standard metric. At the Program level, [redacted] we will meet or exceed the contractor performance metrics required by the EIS Contract, which include:

- Completing and passing the BSS validation testing, as stated in the contract, within 12 months from the acceptance of the BSS Verification Test Plan
- Collecting the AGF from direct-billed customer agencies on a monthly basis throughout the life of the contract
- Billing the government in arrears at the end of every month after providing services
- Providing, as needed, a Monthly Billing Informational Memorandum to coincide with the monthly delivery of billing files
- Submitting proper Billing Invoice (BI) deliverables for all services and service related equipment within 90 days of SOCN issuance
- Prorating billing based on the number of days that the service is provided during the billing period
- Responding within seven (7) days to a billing inquiry received from the Customer
- Resolving all billing disputes within 180 days of the dispute notice
- Providing a monthly Dispute Report (DR)

- Ensuring the comprehensive list of all offered Electronic and Information Technology products (supplies and services) is available on our website within 30 days of Notice to Proceed (NTP)
- Providing a BSS Change Control Notification to the government at least 30 days prior to all BSS changes regardless of their impact
- Update all relevant BSS service documents and information posted on our website within seven (7) days of completing a BSS change
- Initially complete and submit the BSS System Security Plan within 30 days of NTP
- Initially complete and submit the Boundary and Scope Document within 15 days of the NTP
- Mitigating all critical and high-risk vulnerabilities within 30 days and all moderate risk vulnerabilities within 90 days from the date vulnerabilities are formally identified
- Providing updates on a monthly basis on the status of all critical and high vulnerabilities that have not been closed within 30 days
- Having all functional areas of the CSO fully operational within 30 days of NTP
- Submitting SCRM Plan updates on an annual basis and completing all reviews within a 45-day timeframe
- Delivering archived trouble and complaint report data within five (5) days of receiving the request
- Initially populating records of EIS services in the EIS inventory within one (1) business day of the issuance of SOCNs for EIS services delivered to customers
- Updating 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
- Removing equipment related to disconnect orders within 45 days after the termination of services.
- Delivering archived inventory data within five (5) days of receiving the request

- Retaining the monthly snapshots of the EIS inventory and provide them to the Government as requested for three (3) years following the contract expiration or termination
- Investigating EIS inventory data discrepancies reported by the Government and, if in agreement, correcting the data discrepancies within ten (10) days
- Submitting the Inventory Reconciliation deliverable each month
- Responding to the Government's SLA Credit Requests(SLACR) within 30 days by submitting a response and issuing the credit within two billing cycles of this response unless we choose to reject the request
- Delivering the Service Level Agreement Report (SLAR) on the 15th day of each month
- Delivering each of the Trouble Management Performance Summary Report and the Trouble Management Incident Performance Report within 14 days after the end of each FY quarter
- Delivering and maintaining the Contractor Points of Contact List within 30 days of the NTP
- Incorporating Government comments and delivering the revised Training Plan within 15 days after the comments were received
- Providing a monthly Financial Status Report

These metrics include KPIs that will measure:

- Percent On-Time orders completed according to CWD
- Percent Problem-free transitions and implementation
- Billing Data Accuracy
- Billing Charges Accuracy
- Timely Problem Resolution
- Service Specific SLA metrics
- Other KPIs and SLAs specific to and defined in each TO

2.1.10.1.5 Resource Management

[redacted]

[redacted]

Finally, candidates must provide a minimum of three references of previous supervisors. HR verifies education and training, and checks references. HR interviewers complete the candidate evaluation forms, reflecting the results of the interviewer's evaluation of the candidate. We then weigh the candidates' evaluation forms and reference checks against each other to determine the most qualified individual. CTI recognizes that our employees are our greatest asset and we are committed to their retention.

2.1.10.1.6 Revenue Management

[redacted]

For all of our customers, CTI considers accurate and on-time billing/invoicing to be a high priority. To ensure that CTI completes the Government invoicing procedures with accuracy and efficiency, both the Customer Support Office and the Finance office share responsibility. The Customer Service Office is responsible for reviewing Government invoicing documentation. The Finance office is responsible for preparing and providing Government invoices and financial supportive documentation to CSO. The following describes CTI's EIS invoicing procedure:

- Government Invoices will be prepared by Task Order and in compliance with the billing specifications contained in RFP Section G.4 and Section J.2.5.
- The Finance Office will prepare and send the EIS billing invoices to our Customer Service Office (CSO)
- The CTI Customer Service Office (CSO) reviews the invoices, compares the service data against the SLA information, identifies if there were any service interruptions within the billing period, and prepares any required supportive documentation that we will submit to the Government. Specifically, the CSO ensures the data on the invoice is complete, properly classified, accurate, and correctly valued to include credits and partial month proration calculations as applicable.
- When the review is complete, the CSO will forward the invoice and supporting documentation back to the Finance Office along with the applicable credit and proration information.
- The Finance Office will apply any applicable credit and/or proration adjustments due and submit the invoice to the Government, which will cover the billing period of the first through the last day of the previous calendar month.

CTI maintains the following records as part of the invoicing procedure: Government Invoice, General Ledger Detail Report, and Timesheet History Report.

2.1.10.1.7 Reporting and Reviews

In addition to the Quarterly Program Management Review (QPMR) meetings as required in RFP Section G.9.6, CTI will present the Government with accurate program and project reporting and reviews at bi-weekly intervals during the transition and implementation of each Task Order requirements. Upon receipt of Task Order test and acceptance approval from the Government, CTI will schedule and lead a TO Debriefing meeting to present and identify for each service accepted by the Government, the following: EIS Task Order/sub-task number(s) for service(s), Service data rate(s) being provided, Unique circuit number as identifier, Availability (in %) for both directions of the circuit for the reporting period, Report identifying both scheduled and unscheduled outages for the circuit, List of all repair actions on the circuit, List of all maintenance actions on the circuit, List of all abnormal occurrences involving the circuit, and Lessons-Learned to apply on future Task Orders

2.1.10.1.8 Senior-Level Communications

The CTI Team recognizes the risks associated with communication breakdowns between the prime contractor and the subcontracts, and the impacts these breakdowns have on program success. Therefore, CTI has in-place several mechanisms for reducing the risk of communication breakdowns. [redacted]

2.1.10.2 Performance Measurement and Contract Compliance (G.9.2)

CTI acknowledges and accepts that the Government will measure our performance against the set of SLAs established by the contract. To comply with the contract, CTI will: (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 our 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 our subcontractors. These include, but are not limited to, missing data, data reported in the wrong format or units, late submission from subcontractors, etc..

2.1.10.3 Coordination and Communication (G.9.3)

The administration of this contract will require open communications and coordination between the Government, its agency customers, and CTI. [redacted]

CTI's Program Manager will be the single point of contact (POC) to 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 as described in Section RFP G.6.4.1 - Trouble Ticket Management General Requirements.

Well-defined Interfaces between CTI and the Government Ensures Complete Visibility for EIS Customers at all Levels of our Program Management Organizational Structure. CTI will provide the escalation procedure for the Government to escalate issues to appropriate levels of CTI's management team to resolve disputes and issues. Specific areas where CTI will ensure clear and consistent communications and effective coordination are provided between CTI and the Government include: Resolving trouble

reports, complaints, and issue calls, Resolving billing disputes and inquiries, as well as Resolving schedule issues and reporting discrepancies.

[redacted]

Within 30 days of the Notice to Proceed, CTI will provide and maintain a Contractor Points of Contact List that provides contact information for, at a minimum, the functions that follow: Provisioning orders, Identifying and resolving service troubles and complaints, Providing customers with status of troubles and resolution, Developing and delivering training, Conducting billing inquiries, Transition project management,

Finance, Contracting, Account Management (business development and sales), Security, NS/EP, Program Management, Project Management, and Engineering.
CTI will also identify our: (a) Security POCs who will be processing background investigations and security clearances at the appropriate levels as identified in RFP Section C.1.8.7.7 - Personnel Background Investigation Requirements and RFP Section G.5.6 - BSS Security Requirements, and (b) POCs that have passed national agency checks or background investigations, and the security clearance levels held by these individuals as defined in RFP Section G.5.6 BSS Security Requirements.
CTI acknowledges that 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.

2.1.10.4 Program Management Plan (PMP) (L.30.2.1; M.2.2, G.9.4)

CTI submits our Program Management Plan (PMP) in Section 3.1 of this Management proposal.

2.1.10.5 Financial Management (G.9.5)

CTI submits our Financial Status Report in section 3.6 within this Mangement volume.

2.1.10.6 Program Reviews (G.9.6)

2.1.10.6.1 Quarterly Program Status Reports (G.9.6.1)

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

- The status of: Project Plan for program management activities, Base contract modifications, TOs and modifications, Projects, Orders entered and completed, Order Backlogs, Aging, and 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, and Corrective action to remedy
- Technical accomplishments and future plans

2.1.11 TRAINING (G.10)

CTI shall provide training on EIS as described in Section 2.1.12.1 of the GSA EIS solicitation at no additional cost to Government customers, as part of our basic service.

An agency may request additional (specialized) training as required in a TO. CTI shall include a draft Customer Training Plan in its proposal. CTI's Customer Training Plan details the designated training for Government users. 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 2.1.12.1 of the GSA EIS solicitation. The Government reserves all rights to provide comments within 30 days of Notice to Proceed and CTI shall incorporate any recommendations/suggestions and deliver the revised Training Plan within 15 days after the comments were received. Training shall be conducted on Government premises or contractor premises or via training methods that include instructor-led classroom training, distance learning, online web-based / self-paced learning, interactive video other remote training methodologies. When training is conducted at a contractor site, CTI 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. CTI shall provide training as requested by the Government throughout the life of the contract.

2.1.11.1 Training Curriculum (G.10.1)

CTI shall train designated COs, authorized ordering officials, OCOs, and CORs to fully understand and use every aspect of CTI's BSS. Courses include but are not limited billing, pricing, order submission and tracking, network performance, trouble ticketing, and inventory management. All courses may change based upon updates to CTI's BSS

2.1.11.2 Training Evaluation (G.10.2)

CTI shall 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. CTI 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. CTI shall be responsible for correcting the unacceptable issue(s). The Training Plan is as follows:

2.1.11.3 Training Plan – On Demand

CTI BSS Introduction and Overview. This informative class 2-day class introduces the government contractual member or other interested personnel to CTI's Ubersmith BSS system, minimum of 5 students per class. This course provides a general overview of the features of Ubersmith to include the following module topics: Client Manager, Advanced Billing Features, Sales Manager, Order Manager, Device Manager, Support Manager, Reports Manager, and Client Portal. Course when conducted at a government site requires a laptop for each student connectable to the internet. Courseware material and BSS Network simulation will be provided by CTI. On site at CTI, CTI will provide all laptops and materials for student use. Distance Learning training will involve PowerPoint with voiceover. Actual hands on use requires classroom attendance.

CTI Advanced BSS. Covers each module mentioned above in more depth with each class devoted to a single module, with 1 day per module. Student must name module desired, minimum of 5 students per class, per module. Requires CTI BSS Introduction and Overview as a prerequisite Course when conducted at a government site requires a laptop for each student connectable to the internet. Courseware material and BSS Network simulation will be provided by CTI. On site at CTI, CTI will provide all laptops and materials for student use. Distance Learning training will involve PowerPoint with voiceover. Actual hands on use requires classroom attendance.

2.1.12 NATIONAL SECURITY AND EMERGENCY PREPAREDNESS (G.11)

See Section 3.8, National Security and Emergency Preparedness (NS&EP).

2.1.12.1 Basic Functional Requirements (G.11.1)

See Section 3.8.2.1, Basic Functional Requirements.

2.1.12.2 Protection of Classified and Sensitive Information (G.11.2)

See Section 3.8.2.2, Protection of Classified and Sensitive Information.

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

See Section 3.8.2.3, Department of Homeland Security Office of Emergency Communications Priority Telecommunications Services of NS&EP.

2.1.12.3.1 Government Emergency Telecommunications Service (G.11.3.1)

See Section 3.8.2.3.1, Government Emergency Telecommunications Service of NS&EP.

2.1.12.3.2 Wireless Priority Service (G.11.3.2)

See Section 3.8.2.3.2, Wireless Priority Service of NS&EP.

2.1.12.3.3 Telecommunication Service Priority (G.11.3.3)

See Section 3.8.2.3.3, Telecommunication Service Priority of NS&EP.

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

See Section 3.5, Climate Risk Management Plan.

2.1.13.1 Climate Change Adaptation (G.12.1)

See Section 3.5.1.1, Climate Change Adaptation within our Climate Risk Management Plan.

2.1.13.2 Sustainability and Green Initiatives (G.12.2)

See Section 3.5.1.2, Sustainability of Green Initiatives within our Climate Risk Management Plan.

2.1.13.2.1 Electronic Product Environmental Assessment Tool (G.12.2.1)

See Section 3.5.1.2.1, Electronic Product Environmental Assessment Tool within our Climate Risk Management Plan.

2.1.13.2.2 Energy Efficient Products (G.12.2.2)

See Section 3.5.1.2.2, Energy Efficient Products within our Climate Risk Management Plan.

2.1.13.2.3 **Data Centers and Cloud Services** (G.12.2.3)

See Section 3.5.1.2.3, Data Centers and Cloud Services within our Climate Risk Management Plan.

2.2 Management Response To Requirements For Section E: Inspection And Acceptance (L.30.1.2) [RIN:]

2.2.1 Management Approach, Techniques, and Tools to Meet Section E Requirements - Inspection and Acceptance (L.30)

[redacted]

[redacted]

[redacted]Compliance includes compliance with the

Federal documents as found in section 3.7.1.1 within this Management volume, which in turn have sub-set GSA documents as denoted within other areas of this RFP.

Since the government does not cover the costs of COTS/GOTS software product integration, it is incumbent upon CTI, the offeror, to bring together software products that are robust, self-contained, and/or offer open architecture hooks that allow the transfer of data and services. The CTI strategy, therefore, is to use mature, robust, and commercially tested software packages that will not require further development, and that can comply with the test methodology of the BSS Test Plan which, in turn, complies with the specifications of the GSA EIS RFP.

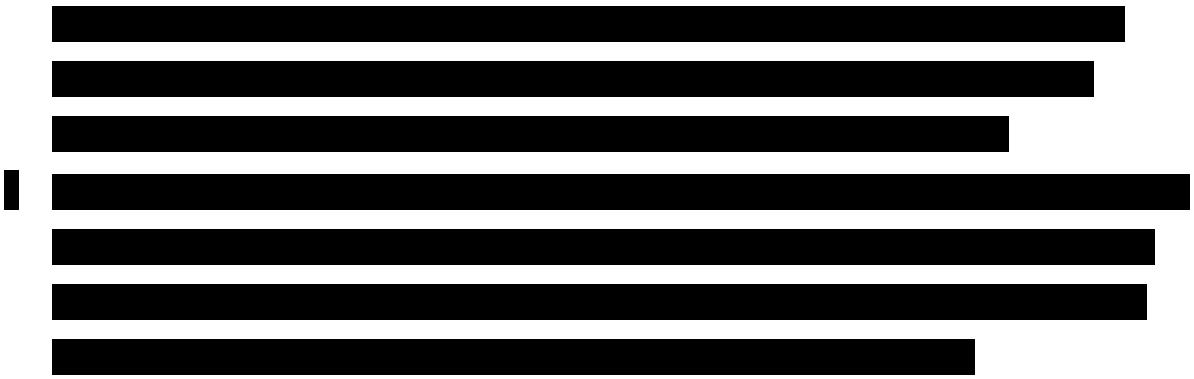
The CTI BSS system also uses or can use the following software systems to provide the Managed Security Services (MSS) which are part of the BSS. The MSS provides protection of endpoints, email, web, and networks, and includes capabilities such as authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management. These capabilities will be critical in meeting some of the Test and Use Cases stipulated elsewhere in this section. MSS comprises the following underlying functions: Managed Prevention Service, Vulnerability Scanning Service, and Incident Response Service.

These functions are described below:

Managed Prevention Service (MPS) provides the ability to monitor hosts and network traffic and analyze network protocol and application activity to identify and mitigate suspicious activity. Supporting capabilities include managed firewalls, host- and network-based threat mitigation, as well as email- and DNS-based threat mitigation services.

Vulnerability Scanning Service (VSS) searches for security holes, flaws, and exploits on agency systems, networks and applications. The service tests for vulnerabilities by comparing scanned information to data contained in a database, which is updated as new threats are discovered. VSS can also simulate a real intrusion in a controlled environment, in order to gauge a network’s susceptibility to attacks. The service performs external scans by remotely probing a network for vulnerabilities that generally come from the outside and internal scans which detect flaws originating from the inside.

Incident Response Service (INRS) is comprised of both proactive and reactive activities. Proactive services are designed to prevent incidents. They include onsite consulting, strategic planning, security audits, policy reviews, vulnerability assessments, security advisories, and training. Reactive services involve telephone and on-site support for monitoring and analyzing alert information and responding to malicious events such as Denial of Services (DoS) attacks; virus, worm, and Trojan horse infections; illegal inside activities, espionage, and compromise of sensitive internal agency databases. INRS provides an effective method of addressing these security intrusions, thereby ensuring operational continuity in case of attacks. In addition, INRS provides forensics services that can assist in apprehending and prosecuting offenders.



2.2.2 TEST METHODOLOGY [L.29.1.3; M.2.2.4.2, E.2]

CTI will follow industry accepted and government accepted testing procedures to ensure the test methodology adheres to the requirements contained within the RFP and includes protocols and standards accepted within commercial industry, which are normally more advanced than government state-of-the-art.

The test methodology includes an agreed upon testing protocol, an explanation of test procedures and testing attributes, the test results, an evaluation of the test results, the tester's signature and date and the supervisor's signature, acceptance, and date. Within this RFP, the following items are specifically outlined:

Test Scenario
Test Case ID
Test Case Description
Requirements Reference(s)
Prerequisites
Government Input(s)
Expected Output(s)
Acceptance Criteria
Data Set Description

In following the government's testing outline, CTI notes that an industry standard testing template would include the following as well, which can be added if the government desires:

• The Stakeholder of the Testing Requirement
• The Financial Statement or Target Statement Line Item
• Preparer and Preparers Contact Information
• Documentation Location
• The Business Cycle/Assessable Unit/Sub-Assessable Unit
• The Financial Statement Assertion
• Key Risk of Material Misstatement
• Financial Reporting Objectives
	• Control Activity Description
	• Use Case
	  ○ Interface
	  ○ Data entry
	  ○ Database
	  ○ Usability
	  ○ Outcome
	• Test Objectives
	• Control Type
	• Control Frequency
	• Testing Period
	• Test Method
	• Transaction Universe and Reconciliation
	• Sampling Technique
		• Sample Size and Basis
		• Acceptable Number of Deviations/Tolerable Misstatement
		• Location of Testing
		• Test Description
		• Test Procedures and Testing Attributes
		• Test Results
		• Control Effectiveness Conclusion
		• Tester's Signature & Date
		• Supervisor's Signature of Acceptance & Date

[redacted] The activities and events will be presented in chronological order with supporting narrative, as necessary, and will depict, for example:

- The overall on-site test period will be accomplished per the government's schedule after the issuance of the contract. CTI will be able to allocate time by calendar date, and portions of the period assigned to major portions of the test.
- The pretest on-site period required for system test team orientation, familiarization, and for system debugging should take approximately one week.
- The period assigned for the collection of database values, input values, and other operational data required for system test will be discussed between CTI and the government.
- The period assigned for user training, operator training, maintenance and control group training, and management orientation briefing will be discussed between CTI and the government.
- The period assigned for preparation, review, and approval of the test analysis report will be done in accordance with the government's schedule.

CTI will provide an in-brief to the government testing personnel regarding our BSS which will include:

- Manufacturer
- System name

- System Functional Description and Capability
- System Specifics
  - *Major application*: Explanation of clearly defined functions for which there is a readily identifiable security consideration and need
  - *General support system*: Explanation of general network support for a variety of users and applications as denoted in the Test Scenarios
- Overview of Operational status
  - Operational
  - Under development
  - Undergoing a major modification
- System environment and special conditions if any
- Introduction and in-brief for all test personnel going over rules and expectations.

As part of our overall EIS BSS Verification Test Plan Framework, the EIS Services Verification Test Plan follows the same government and industry best practices to ensure that all services are delivered in accordance with the GSA EIS RFP requirements. The government has set out a set of testing criteria which is illustrated in several tables contained within the BSS Verification Test Plan and is also called out in a separate EIS Services Verification Test Plan. CTI will follow the verification and acceptance test methodology described in this section in developing the verification test plan(s) for: (1) Contractor's Business Support Systems (BSS), and (2) EIS Services

2.2.2.1 BSS Verification Test Plan [L.29.1.3; M.2.2.4.2; E.2.1]

CTI's Draft BSS Verification Test Plan can be found in Section 3.3 of this Management volume.

2.2.2.2 EIS Services Verification Testing (E.2.2)

CTI's EIS Services Verification Testing Plan can be found in Section 3.4 of this Management volume.

2.3 MANAGEMENT RESPONSE TO REQUIREMENTS FOR SECTION J.2 CONTRACTOR DATA INTERACTION PLAN (L.30; G.5; J.2, L.30.1.3)

2.3.1 INTRODUCTION (L.30(3), L.30.1(3); G.1; J.2.1)

2.3.1.1 EIS Management and Operations: High-Level Process Diagram (J.2.1.1)

CTI will comply with the requirements as specified in RFP Section J.2 for the various mangement and operations functions such as ordering, billing, inventory management,

and SLA Management. We will follow the details provided for data interactions between CTI, GSA and the customers and the requirements for direct interaction between GSA's next generation network solutions managmenet system (GSA Conexus) and CTI's Business Support Systems (BSS) as described in RFP Section G.5. CTI's BSS Data Sets will be normalized so that they are consistent with the Govenrment's so that the required direct interaction between Conexus and our BSS can be designed and configured as a problem-free, efficient process.

2.3.1.2 Timeframes (J.2.1.2)

Unless otherwise specified below, all timeframes in this Contractor Data Interaction Plan (CDIP) are in calendar days.

2.3.2 COMMON DATA INTERACTION REQUIREMENTS (J.2.2) [RIN: MMC0022-DI]

As per the requirements in Section J.2.2, CTI shall support all Common Data Interaction Requirements.

2.3.2.1 Relevant Contracting Officer (J.2.2.1)

Where permitted by the applicable sections within the CDIP, exceptions to CDIP data submission requirements may be authorized, in writing, by the relevant Contracting Officer (CO). For these purposes, the relevant CO is defined as follows: For data dubmitted to GSA, the GSA CO is the relevant CO, and For data submitted to a customer, the Ordering Contracting Officer (OCO) is the relevant CO

2.3.2.2 Resubmission of Incorrect Deliverables (J.2.2.2)

CTI will notify the Government and resubmit incorrect deliverables immediately when we become aware of an error. When we do notice the error, we will determine if it is associated with billing. If the error is not associated with billing, CTI will resubmit the deliverable within three (3) days of becoming aware of the error. If, however, the error is related to billing, which we identify after the government makes a payment, we will submit a billing adjustment, as described in Section J.2.5 Billing, to the Government no later than the 15th business day and include a description covering the full details of any adjustments to CTI's invoice for the billing period. CTI will notify the relevant Contracting Officer's Representative (COR) and CO of the error via email and include a description of the action taken.

2.3.2.3 Deliverable Format, Content, and Transfer Mechanism (J.2.2.3)

CTI will ensure all deliverables covered in this Contractor Data Interaction Plan (CDIP) will meet the following requirements:

- When we submit deliverables directly to GSA, including cases where GSA receives a copy of a deliverable sent to the customer, CTI will use the format, contents, and transfer mechanism specified herein unless the GSA authorizes an exception.
- When we submit deliverables directly to the customer, including cases where the customer receives a copy of a deliverable sent to GSA, CTI will, with the approval of the OCO, use alternative formats, contents, and/or transfer mechanisms. CTI acknowledges that the Traffic Order (TO) may also specify alternative formats, contents, and/or transfer mechanisms for deliverables submitted to the Customer and, in such cases CTI will comply with the TO requirements.

2.3.2.4 Scope of Deliverables (J.2.2.4)

Unless otherwise specified by GSA or the Customer, CTI will submit all deliverables in accordance with the following deliverable scope requirements: (1) the scope of all deliverables will be at the TO level with each deliverable covering only a single TO, (2) when CTI submits deliverables directly to GSA, including cases where GSA receives a copy of a deliverable sent to the customer, we will comply with any exceptions authorized by the relevant GSA CO, and (3) when CTI submits deliverables directly to the customer, including cases where the customer receives a copy of a deliverable sent to GSA, we will comply with any exceptions authorized by the OCO or captured directly in the TO.

2.3.3 TASK ORDER DATA MANAGEMENT (J.2.3)

During initial setup and the ongoing maintenance of the TO, CTI will perform TO Data Management in a manner that ensures consistency between the GSA systems and our BSS. There are three categories of TO Data that we will manage to ensure effective date exchange between the Government and CTI, which are as follows:

1. **Task Order Controlled Data:** This is data in the TO or is directly tied to it and can only change via a TO modification. This data includes: TO documents, TO-defined customer officials: OCO, Services specified on the TO, TO-Unique CLINs (TUCs) and Individual Case Basis (ICB) data, TO-unique KPIs and SLAs, and Other customer data specified on the TO.

2. **Task Order Associated Data:** This is data that is not typically specified in the TO and can change at any time during the life of the TO. This data includes:
   - Additional TO Customer Officials not defined in the TO
   - Role-Based Access Control (RBAC) information
3. **System Reference Data:** This data is comprised of universally applicable reference tables that the GSA uses to ensure GSA systems and CTI's BSS are using consistent codes for common transactional data. Some examples of System Reference Data include: Technical features such as Access Circuit Type and Bandwidth, Business features such as Agency Bureau Code (ABCODE) and Dispute Reason, and Status features such as Yes/No and True/False codes.

2.3.3.1 Common Operational Requirements (J.2.3.1)

CTI will comply with all of RFP Section J.2.3.1 common operational requirements.

2.3.3.1.1 GSA Systems (J.2.3.1.1)

CTI acknowledges GSA systems comprise the set of tools GSA will use to manage the contract and TOs issued. CTI therefore agrees to submit data via GSA systems as proposed RFP Section J.2.3.2 Task Order Data Management Process.

2.3.3.1.2 Role Based Access Control (RBAC) (J.2.3.1.2)

CTI will apply RBAC to allow access and assigned permission to our Business Support Systems (BSS) from only authorized Government customers. CTI will capture and store the permission of authorized users for restricted access and we will restrict all BSS information so that only the authorized users have access. [redacted]

The BSS applications using RBAC will test the user for membership in a specific role, and grant or deny access based on that. The main benefit of RBAC is ease of management because, in principle, there are very few roles that are centrally administered, no matter how many users; CTI knows, however, we must assign each user the ***correct*** role.CTI will add new users within seven (7) days of receiving an Agency customer request. CTI's objective will be to arrange for the *immediate* removal of users who no longer have access authorization to our BSS and we affirm all removals will occur within one (1) business day.

2.3.3.2 Task Order Data Management Process (J.2.3.2)

CTI will follow the TO data management processes as described in the RFP Section J.2.3.2 and we will use the Government's definitions when developing our deliverables or dealing with other data sets as defined in RVP Section J.2.3.3.

2.3.3.2.1 System Reference Data (J.2.3.2.1)

CTI will follow the process described below upon the successful completion of verification and security testing for CTI's BSS as described in RFP Section G.5 - Business Support Systems and Section E.2.1 - Business Support Systems Verification Testing, and as required by changes to the data. Contract modifications may be the source for data changes. CTI will implement any resulting changes required to BSS once approved by GSA in accordance with RFP Section G.5. CTI will complete this process prior to setting up its first TO, as described in RFP Section J.2.3.2.2 - Task Order Data. GSA will provide system reference data to CTI using the data sets defined in RFP Section J.2.3.3.1, in the table that lists reference data sets the Government will provide as part of this process on an as needed basis. For each data set, CTI will support all required transfer mechanisms as defined in RFP Section J.2.9 - Data Transfer Mechanisms. CTI will configure our BSS to submit data based on the provided system reference data in RFP Section J.2.3.3.1.

2.3.3.2.2 Task Order Data (J.2.3.2.2)

For each TO, CTI will follow the initial TO setup process defined in RFP Section J.2.3.2.2 prior to processing any orders for service and as required by changes to the data. The initial setup of each TO requires a set of process steps that CTI will follow. At initial setup of each TO, CTI will submit the following deliverables to GSA: TO Services Awarded / TO CLINs Awarded, TO Country/Jurisdiction Awarded By Service / TO

Locations Awarded by Service, TO Officials, TO Customer Requirements Document Set, TO Financials, and TO Key Performance Indicators.

Collect the list of RBAC users and the associated user permissions from the customer Set up or modify appropriate RBAC permissions within our BSS as described in RFP Section G.5 - Business Support Systems. CTI will submit the Direct Billed Agency Setup (DBAS) to GSA.

CTI will complete the above process prior to provisioning or providing any services as required by the TO. CTI will omit submission of data sets when no changes have occurred subsequent updates may omit submission of data sets where unless directed otherwise by the GSA CO.

2.3.3.3 Deliverables and Data Exchange (J.2.3.3) [RIN: MMC0023-DI]

2.3.3.3.1 Government-Provided Data: System Reference (J.2.3.3.1)

CTI will support all required transfer mechanisms as defined in RFP Section J.2.9 - Data Transfer Mechanisms and as specified in RFP Section J.2.3.3.2.

2.3.3.3.2 Reserved (J.2.3.3.2) [RIN: MMR0096-DN]

2.3.3.3.3 Contractor-Provided Data Sets: Deliverables (J.2.3.3.3) [RIN: MMR0097-DN, MMR0098-DN]

The following table lists the deliverables that CTI will provide as part of this process. For each data set, CTI will support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
TO CLINs Awarded	As required	Upload to GSA Systems
TO Country/Jurisdiction Awarded by Service	As required	Upload to GSA Systems
TO Officials	As required	Upload to GSA Systems
TO Customer Requirements Document Set	As required	Upload to GSA Systems
TO Financials	As required	Upload to GSA Systems
TO Key Performance Indicators	As required	Upload to GSA Systems
TO Locations Awarded by Service	As required	Upload to GSA Systems
TO Services Awarded	As required	Upload to GSA Systems
Direct Billed Agency Setup (DBAS)	As required	Web Services

2.3.4 ORDERING (J.2.4) [RIN: MMC0024-DI]

CTI will support all Ordering requirements including Common Operational Requirements, Process requirements, and Deliverables & Data Exchange requirements.

2.3.4.1 Common Operational Requirements (J.2.4.1)

2.3.4.1.1 Task Orders (J.2.4.1.1) [RIN: MMR0099-DN]

The (Task Orders) TO process as described in Section G.3 Ordering specifies that once a TO is issued, CTI shall follow the process described in Section J.2.3 Task Order Data Management.

2.3.4.1.2 Agency Hierarchy Code (J.2.4.1.2) [RIN: MMR0100-DN, MMR0101-DN, MMR0102-DN]

The Agency Hierarchy Code (AHC) is an internal government accounting code that shall be tracked for all services from order submission through disconnection. The government has the following AHC requirements for ordering

1. An AHC is required on each line item in all orders.
2. CTI shall validate the presence of an AHC on all order line items:
    a) The government will not pay for orders processed without an AHC on each line item
    b) The government does not require validation of the content of the AHCs unless specified on the TO

CTI shall support AHC changes to provisioned services without an interruption of the associated service (see J.2.4.2.3 Administrative Change Orders).

2.3.4.1.3 Unique Billing Identifier (J.2.4.1.3) [RIN: MMR0103-DN, MMR0104-DN]

CTI shall create the UBI as described in Section J.2.10.1.1.2. CTI shall provide the UBI as a data element in the Service Order Completion Notice (SOCN).

2.3.4.1.4 Agency Service Request Number (J.2.4.1.4) [RIN: MMR0105-DN, MMR0106-DN]

In compliance with Section J.2.4.1.4 the Agency Service Request Number (ASRN) is an optional internal government control number that CTI shall track for all services from order submission through disconnection if it is provided. If the government provides ASRN data element(s) as part of a Service Order (SO), CTI shall include them on all deliverables that reference that order or the services included in that order(SO).

2.3.4.1.5 Contract Line Item Number (J.2.4.1.5) [RIN: MMR0107-DN, MMR0108-DN]

The government has the following CLIN requirements for ordering: (1) CTI shall provide the CLIN and any associated ICB data element(s) for each line item in all ordering deliverables as required in Section J.2.3.3.3 CTI Provided Data Sets: Deliverables,' and (2) CTI shall ensure the CLINs reported on billing files match those included on the SOCN for a particular order.

2.3.4.1.6 Ordering Data Sets and Notices (J.2.4.1.6)

2.3.4.1.7 Auto-Sold CLINs (J.2.4.1.7) [RIN: MMR0109-DN, MMR0110-DN, MMR0111-DN, MMR0112-DN]

Unless otherwise specified in the SO or TO, in accordance with Section G.3.3.1.2 Auto-Sold CLINs, the government has the following auto-sold CLIN requirements for ordering: (1) CTI shall include any auto-sold CLINs in all notices and deliverables that require reporting CLINs, (2) unless otherwise specified in the SO or TO, CTI shall apply

the AHC listed for the base CLIN to all associated auto-sold CLINs, (3) unless otherwise specified in the SO or TO, CTI shall apply the ASRN(s) listed for the base CLIN to all associated auto-sold CLINs, and (4) CTI shall manage activation and deactivation of auto-sold CLINs in accordance with Section J.2.4.1.10 Service State and Section J.2.4.2.5 Service State Changes.

2.3.4.1.8 Order Types (J.2.4.1.8)

2.3.4.1.9 Splitting Complex Orders into Suborders (J.2.4.1.9) [RIN: MMR0113-DN, MMR0114-DN]

Upon confirmation of such an order, CTI may split the order into logical suborders using its standard provisioning process with the following restrictions:

1. Services logically linked by a Service Grouping ID as described in Section J.2.10.1.1.2 Unique Billing Identifier, shall not be split across multiple suborders.
2. CTI shall not split any SO into suborders if the SO or the TO contains instructions prohibiting such splitting.

2.3.4.1.10 Service State (J.2.4.1.10) [RIN: MMR0115-DN, MMR0116-DN]

CTI will ensure that all provisioned UBIs have a valid service state assigned at all times: (1) a UBI is not considered provisioned prior to the SOCN for its installation, (2) a UBI is not considered provisioned after the SOCN for its disconnection.

CTI shall not change the service state of a UBI except in response to direct government action (e.g., beginning or ending the use of an auto-sold CLIN) or as required based on predefined criteria captured in the contract or the TO.

2.3.4.2 Ordering Process (J.2.4.2) [RIN: MMR0117-DN]

In compliance with Section J.2.4.2, unless otherwise specified, CTI shall submit all deliverables and other data sets included in the processes defined in Section J.2.4.3 Deliverables and Data Exchange. Unless otherwise specified, CTI shall submit all deliverables in the process below to GSA and, if requested, to the customer.

2.3.4.2.1 Standard Orders (J.2.4.2.1) [RIN: MMR0118-DN, MMR0119-DN, MMR0120-DN, MMR0121-DN, MMR0122-DN, MMR0123-DN, MMR0124-DN, MMR0125-DN, MMR0126-DN, MMR0127-DN]

Per Section J.2.4.2.1, CTI recognizes and agrees with the Standard orders, including moves, adds, changes (excluding administrative change orders), and disconnect orders, shall follow the process below (order updates are addressed in Section J.2.4.2.6):

1. The government will issue an SO.
2. CTI shall submit an SOA within one (1) business day of SO.

3. If CTI determines that the SO is invalid, then CTI shall submit a SORN within five (5) days of SO:
    a. A SORN submitted by CTI shall apply to the entire order (i.e., CTI may only reject entire orders, not individual line items).
    b. In the event of order rejection, the government may issue a new SO with the corrected information and restart this process.
4. If CTI determines that the SO is valid, it shall submit a SOC within five (5) days of SO.
5. The government may modify or cancel the order during the provisioning process as described in Section J.2.4.2.6 (see also Section J.2.10.1.1.4.3 and Section G.3.3.2.3).
6. If CTI chooses to split a complex SO into suborders as described in Section J.2.4.1.9, CTI shall follow the remainder of this process for each suborder including submitting separate deliverables for each suborder.
7. If CTI must obtain local access services, CTI shall submit a FOCN indicating its FOC date within one (1) business day of receiving the FOC date from the local provider.
8. If CTI does not need to obtain local access services, CTI shall submit a FOCN indicating its FOC date NLT the earlier of: 1) 5 days after SOC, or 2) 10 days before the FOC date.
9. Upon completion of the order, CTI shall submit a SOCN within three (3) days of installation and testing unless otherwise specified in the TO.
10. If the government reports a problem within the acceptance period defined in Section E, Inspection and Acceptance (or as specified in the TO), CTI shall fix, test, and submit a new SOCN.

2.3.4.2.2 Telecommunications Service Priority Orders (J.2.4.2.2) [RIN: MMR0128-DN, MMR0129-DN, MMR0130-DN]

When the government submits a Telecommunications Service Priority (TSP) order as described in Section G.3.3.3.1 TSP Orders, CTI will follow the standard process (see Section J.2.4.2.1) and shall apply with the appropriate caveats. CTI:

1. Shall follow the prioritizations applicable to TSP orders as noted in Section G.3.3.3.1 Telecommunications Service Priority Orders and/or Section G.11 National Security and Emergency Preparedness.
2. Shall not delay the delivery of services in any way based on the need to submit deliverables specified in this process.

2.3.4.2.3 Administrative Change Orders (J.2.4.2.3) [RIN: MMR0132-DN]

Pursuant to Section J.2.4.2.3, CTI agrees to handle, administrative data changes to previously provisioned services, as described in Section G.3.3.2.2.4 Administrative Change Orders. They shall be handled based on the restrictions and processes as further described in subsequent subsections.

2.3.4.2.3.1 Administrative Change Order Process (J.2.4.2.3.2) [RIN: MMR0133-DN, MMR0134-DN]

In compliance with Section J.2.4.2.3.2, CTI will, unless otherwise specified, submit all deliverables described in the process below to GSA and, if requested, to the customer:

1. The government will issue an Administrative Change Order specifying the inventory items to be changed and details of the change.
2. CTI shall update its systems and submit a SOAC within seven (7) days of the Administrative Change Order.
3. Other order notices (SOA, SOC, FOCN, and SOCN) are not required.

2.3.4.2.4 Rapid Provisioning (J.2.4.2.4) [RIN: MMR0135-DN]

CTI shall follow the standard process (Section J.2.4.2.1) with the following changes:

1. The SOC and the FOCN are not required.
2. If CTI completes the provisioning process and issues a SOCN within twenty-four (24) hours of order submission, the SOA is not required.
3. If CTI rejects an order, the SORN must be issued prior to the end of the defined provisioning interval.
4. The government's option to modify or cancel the order during the provisioning process is subject to the restrictions noted in Section G.3.3.3.2 Rapid Provisioning Orders.

2.3.4.2.5 Service State Changes (J.2.4.2.5) [RIN: MMR0136-DN]

CTI agrees that if a service (defined by a single UBI) changes from one state to another (as defined in J.2.4.1.10 Service State), CTI shall issue a SSCN within 24 hours. CTI

may combine multiple notices as individual line items on a single SSCN provided all notices are submitted within 24 hours of the individual state change.

2.3.4.2.6 Supplements or Updates to In-Progress Orders (J.2.4.2.6) [RIN: MMR0137-DN, MMR0138-DN, MMR0139-DN, MMR0140-DN, MMR0141-DN, MMR0142-DN, MMR0143-DN, MMR0144-DN]

CTI will comply with all requirements as stated and require the government to issue a supplement SO when updating an in-process order.

1. The government will issue a supplement SO.
2. CTI shall submit an SOA in response to the supplement SO within one (1) business day of receiving it from the Government.
    a. The Contractor Service Request Number (CSRN) reported on the SOA shall be the same as that reported on the original order.
    b. Note: TSP (Section J.2.4.2.2) and Rapid Provisioning (Section J.2.4.2.4) orders may have shorter submission times as defined in the applicable section
3. If CTI determines that the supplement SO is invalid, then CTI shall submit a SORN in response to the supplement SO within three (3) days of the supplement SO.
    a. The CSRN reported on the SORN shall be the same as that reported on the original order.
    b. Note: TSP (Section J.2.4.2.2) and Rapid Provisioning (Section J.2.4.2.4) orders may have shorter submission times as defined in the applicable section.
4. CTI understands that it shall update the original order with the new data.
5. CTI agrees that if any changes are required to data sets already submitted in response to the original order (e.g., SOC, FOCN), that CTI shall issue updated versions of those notices.
6. CTI shall complete the provisioning of the original order with updated information as described in the applicable order process.
    a. Section J.2.4.2.1 – Standard Orders
    b. Section J.2.4.2.2 – Telecommunications Service Priority Orders
    c. Section J.2.4.2.4 – Rapid Provisioning Orders

2.3.4.3 Deliverables and Data Exchange (J.2.4.3)

2.3.4.3.1 Government-Provided Data Sets (J.2.4.3.1) [RIN: MMR0145-DN]

CTI shall support all required transfer mechanisms for each data set as provided by the government, as required. The data sets include Service Orders (SO) and Administrative Change Orders, with transfer mechanisms including: Direct Data Exchange, Contractor's Web Interface, Email, and Other means as per the TO.

2.3.4.3.2 Contractor-Provided Data Sets (J.2.4.3.2) [RIN: MMR0146-DN, MMR0147-DN]

With respect to Section J.2.4.3.2, the following table lists the deliverables CTI shall provide as part of this process. CTI shall support all required transfer mechanisms for each data set as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
Service Order Acknowledgement (SOA)	NLT one (1) business day after SO	Web Services, Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO
Service Order Rejection Notice (SORN)	NLT 5 days after SO	Web Services, Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO
Service Order Confirmation (SOC)	NLT 5 days after SO	Web Services,Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO
Firm Order Commitment Notice (FOCN)	Local access subcontractor required: within one (1) business day of receiving FOC date Local access subcontractor not required: NLT the earlier of 5 days after SOC or 10 days before the FOC date	Web Services, Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO
Service Order Completion Notice (SOCN)	NLT 3 days after service is installed and tested	Web Services, Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO
Service Order Administrative Change (SOAC)	NLT 7 days after Administrative Change Order	Web Services, Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO
Service State Change Notice (SSCN)	Within 24 hours of state change	Web Services, Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO

2.3.5 BILLING (J.2.5) [RIN: MMC0025-DI]

CTI will fully comply with all billing requirements which includes:

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

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

2.3.5.1 Common Operational Requirements (J.2.5.1)

2.3.5.1.1 Billing Cycle (J.2.5.1.1) [RIN: MMR0148-DN]

CTI shall comply with the government's defined billing cycle, which runs from the first through the last day of the calendar month.

2.3.5.1.2 Unique Billing Identifier (J.2.5.1.2) [RIN: MMR0149-DN]

As per the requirements in Section J.2.5.1.2, CTI shall ensure the UBI reported on billing deliverables matches the UBI included on the SOCN for a particular element.

2.3.5.1.3 Contract Line Item Number (J.2.5.1.3) [RIN: MMR0150-DN, MMR0151-DN]

The government has the following CLIN requirements for billing:

1. CTI shall provide the CLIN and any associated ICB data element(s) for each line item in all billing deliverables (as described in Section J.2.5.2 Billing Process).
2. CTI shall ensure that the CLINs reported on billing deliverables match those included on the SOCN for a particular order.

2.3.5.1.4 Associated Government Fee (J.2.5.1.4) [RIN: MMR0152-DN, MMR0153-DN, MMR0154-DN]

The government has the following AGF requirements for billing:

1. CTI shall calculate the AGF as described in Section J.2.10.1.1.1.
2. CTI shall provide the AGF as a data element in billing deliverables (described in Section J.2.5.2 Billing Process).
3. For TOs set up with direct billing (see Section G.4.2 Billing Methods), CTI shall collect the AGF on behalf of GSA and transfer funds as described in Section G.4.6 Associated Government Fee.

2.3.5.1.5 Proration (J.2.5.1.5) [RIN: MMR0155-DN, MMR0014-DN]

For services not delivered for the full calendar month billing cycle, CTI shall apply the appropriate proration requirements as further defined in next sections.

2.3.5.1.5.1 Proration Formula (J.2.5.1.5.1) [RIN: MMR0156-DN, MMR0015-DN, MMR0016-DN, MMR0017-DN, MMR0018-DN]

CTI will support the proration type, Normalized 30-Day Month Proration, as defined in Section J.2.5.1.5.1.2 within this proposal. Within its response to each customer agency solicitation, CTI will indicate this supported proration type. If CTI does not support the proration type specified on the customer TO solicitation, CTI will be sure to clearly state within its response that it does not currently support the requested proration type.

CTI understands that it may add support for the Month-Length Proration type, which is currently not supported with this proposal, at any time without contract modification by following the BSS Change Control process in Section G.5.5.1. CTI will complete successful retesting of the BSS test cases associated with proration prior to billing.

2.3.5.1.5.1.1 Normalized 30-Day Month Proration (J.2.5.1.5.1.2)

CTI shall follow the process below to calculate prorated billing:

1. Calculate the Daily Charge: divide the Monthly Recurring Charge (MRC) by 30 to get the Daily Charge. Daily Charge = MRC/30
2. Calculate the number of billable days for the service in that month.
    a. For new installations or new service pricing starts based on a service change order.
    b. Number of days in the month minus the number of days in the month prior to installation or start
    c. Billable Days = Days in Month – (Start Day – 1)
    d. Example: service installed on March 17th,
        - 31 [days in month] – (17 [start day] -1) = 15 billable days
3. For disconnections or prior service pricing ends based on a service change order:
    a. Number of days up to and including disconnect or end date
    b. Billable Days = Disconnect or End Day
    c. Example: service disconnected on June 10th:
        - 10 [disconnect day] = 10 billable days
4. Note: if Billable Days from Step 2 is equal to or greater than 30, proration does not apply; CTI shall bill the full MRC for that month.
5. The billable amount for the service in that month is equal to the daily charge from step 1 multiplied by the billable days from step 2.
    a. Billable Amount = Daily Charge x Billable Days.

2.3.5.1.5.2 Service Charge Order Proration (J.2.5.1.5.2) [RIN: MMR0157-DN]

CTI shall follow the process below to calculate prorated billing:

1. Treat the change as two connected events: A previous service price end & A new service price start.
2. The new service price is assigned a start date equal to the change date.

3. The previous service price is assigned an end date one (1) day prior to the start date for the new service price.
4. Calculate the prorated billing amount for each service pricing (ended previous and started new) using the standard proration formula (see J.2.5.1.5.1).

2.3.5.1.6 Rounding (J.2.5.1.6)

2.3.5.1.6.1 Rounding Requirements (J.2.5.1.6.1) [RIN: MMR0158-DN, MMR0159-DN, MMR0160-DN, MMR0161-DN, MMR0162-DN]

CTI shall comply with all necessary requirements for rounding as described in the following requirements.

1. CTI shall store charges and use in all calculations six (6) decimal places for service price [Quantity x Unit Price], prorating, taxes, fees and surcharges.
    a. When rounding is necessary to reach 6 decimal places, CTI shall apply the rounding standards in Section J.2.5.1.6.2.
2. When calculating summary data (including total cost), CTI shall:
    a. Total each of the cost components that comprise the service including CLIN unit price (prorating if applicable), taxes, fees, and surcharges.
    b. Add the charges at the service level while maintaining the full 6 decimal places
3. When totaling the entire submitted bill, CTI shall:
    a. Add the individual 6-decimal place service charges
    b. Round the total 6-decimal place value to 2 decimal places using the rounding standards in Section J.2.5.1.6.2.

2.3.5.1.6.2 Rounding Standards (J.2.5.1.6.2) [RIN: MMR0163-DN]

CTI shall comply with the following rounding standards:

1. Rounding to reach 6 decimal place values:
    a. Upward rounding shall occur when the 7th decimal place is 5 or higher.
    b. Downward rounding shall occur with the 7th decimal place is 4 or lower.
    c. For example: if a cost component is $1113.8870974, since the 7th decimal place is 4, the cost component will be rounded to $1113.887097.
2. Rounding to reach 2 decimal place values:
    a. Upward rounding will occur when the 3rd decimal place is 5 or higher.

b. Downward rounding shall occur when the 3rd decimal place is 4 or lower.
c. For example: if the total amount due was $8395.4681674, since the 3rd decimal place is 8, the calculated amount due would be $8395.47'

2.3.5.1.7 Taxes, Fees, and Surcharges (J.2.5.1.7) [RIN: MMR0164-DN, MMR0165-DN, MMR0166-DN]

CTI shall comply with the following data requirements for taxes and surcharges:

1. Taxes shall be applied to each taxable line item as an aggregated total per billing line item.
2. CTI shall provide the detail composition of the aggregated tax on the Tax Detail (TAX) deliverable.
3. CTI shall not aggregate taxes, surcharges, and fees into any other data element unless the TO specifies such aggregation (fully-loaded pricing) as described in Sections H.14 and H.23.

2.3.5.1.8 Billing Level (J.2.5.1.8) [RIN: MMR0167-DN, MMR0270-DN, MMR0168-DN]

CTI shall submit billing deliverables as described in Section J.2.5.2 using a TO billing level where each deliverable covers only a single TO, unless the TO specifies another billing level.

2.3.5.1.9 Billing Data Sets (J.2.5.1.9)

CTI understands that several data sets are exchanged between the government and CTI as part of the ordering process. The delivery process, frequency, timing and detailed specifications for each are understood as described in J.2.5.2 Billing Process. The standard data sets are acceptable and agreed upon by CTI as defined below:

- Billing Invoice (BI) Deliverable: Provides the government with the full details of the contractor's invoice for the billing period. The BI shall include all taxes, fees, and surcharges as described in Section J.2.5.1.7. It shall not include any credits or adjustments. The contents of the BI and the BA together are used to calculate the total amount due from the government. CTI understands and complies.
- Billing Adjustment (BA) Deliverable: Provides the government with the full details of any credits and other adjustments to the contractor's invoice for the billing period. The contents of the BI and the BA together are used to calculate the total amount due from the government. CTI understands and complies.

- Tax Detail (TAX) Deliverable: Provides the government with the full details of the taxes, fees, and surcharges included in contractor's invoice for the billing period. CTI understands and complies.
- AGF Detail (AGFD) Deliverable: Provides the government with the full details of the AGF collected by the contractor from direct billed customers for the billing period. CTI understands and complies.
- AGF Electronic Funds Transfer Report (ATR) Deliverable: Notifies the government that the contractor has transferred the collected AGF via Electronic Funds Transfer (EFT). CTI understands and complies.
- Monthly Billing Information Memorandum Deliverable: Provides the government with background information, as necessary, to explain any items in the contractor's invoice for the billing period that may be unclear based on the contents of the BI alone. CTI understands and complies.

2.3.5.2 Billing Process (J.2.5.2) [RIN: MMR0169-DN, MMR0170-DN, MMR0171-DN, MMR0172-DN, MMR0019-DN]

The standard billing process described below is applicable to all TOs. Unless otherwise specified, CTI shall submit all deliverables in the process below to GSA and, if requested, to the customer.

1. NLT the 15th business day of each month, CTI shall submit billing deliverables based on the billing levels defined in Section J.2.5.1.8.
    a. Billing invoice (BI)
    b. Tax Detail (TAX) unless the TO specifies fully-loaded pricing
    c. Monthly billing information Memorandum
    d. Billing Adjustment (BA)
2. NLT the 15th business day of each month, CTI shall submit the following billing deliverables to GSA only based on the billing levels defined in Section J.2.5.1.8:
    a. AGF Detail (AGFD)
    b. AGF Electronic Funds Transfer Report (ATR)
3. If the government determines that the BI is valid in its entirety, it will pay CTI in full, as specified in Section G.4.5 Payment of a Bill by the Government.
4. If the government determines that the BI is not valid, in whole or in part, it will: (a) initiate a billing dispute as specified in Section G.4.4 Disputes; (b) enter the

dispute process described in Section J.2.6 Disputes; and (c) withhold payment to CTI, in whole or in part, as specified in Section G.4.4 Disputes and further clarified in Section H.32 Payments and Incorrectly Billed Items.

5. If required to correct errors identified after payment, CTI shall submit a BA. Note: this does not apply to errors that have resulted in disputes as described in Section J.2.6 Disputes.

2.3.5.3 Deliverables & Data Exchange (J.2.5.3)

2.3.5.3.1 Government-Provided Data Sets (J.2.5.3.1)

2.3.5.3.2 Contractor-Provided Data Sets (J.2.5.3.2) [RIN: MMR0173-DN, MMR0174-DN]

As per Section J.2.5.3.2, the following table lists the deliverables that CTI shall provide as part of this process, as well as all the required transfer mechanisms as defined in Section J.2.9. Data Transfer Mechanisms that will be supported.

Data Set	Frequency	Transfer Mechanism
Billing Invoice (BI)	Monthly, NLT 15th business day	Secure FTP, Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO
Billing Adjustment (BA)	Monthly, NLT 15th business day (as needed)	Secure FTP, Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO
Tax Detail (TAX)	Monthly, NLT 15th business day	Secure FTP
AGF Detail (AGFD)	Monthly, NLT 15th business day	Secure FTP
AGF Electronic Funds Transfer Report (ATR)	Monthly, NLT 15th business day	Secure FTP
Monthly Billing Information Memorandum	Monthly, NLT 15th business day (as needed)	Email, Contractor's Web Interface, and Other means as agreed or required in the TO

2.3.6 DISPUTES (J.2.6) [RIN: MMC0026-DI, MMR0006-DN]

CTI understands and complies with all requiremnents under Disputes in Section G.4.4. The dispute process shall apply under any of the following conditions: (a) the government disputes the content of a BI submitted by CTI, (b) the government disputes the content of an Inventory Reconciliation (IR) submitted by CTI, or (c) the government disputes a SLACR response submitted by CTI.

The GSA CO, OCO, or authorized ordering official may submit to CTI 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.

CTI shall accept and process the government's disputes. CTI shall comply with the processes, deliverables, and data exchange requirements described in Section J.2.6 Billing & Inventory Disputes. The government will accept and process CTI's disputes.

CTI 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.

Billing Disputes Resolution

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, CTI shall submit corrected billing on the next available bill. The following requirements apply to billing dispute resolution:

1. CTI shall resolve billing disputes with the agency that submitted the dispute.
2. CTI shall work to resolve disputes within 180 days of the dispute notice.
3. In cases where a complete resolution is not forthcoming, CTI will 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 CTI's proposed resolution. Either party may escalate the dispute at any time to the OCO. In cases where CTI 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, CTI 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. CTI shall provide a monthly Dispute Report (DR) in accordance with Section J.2.6 Billing & Inventory Disputes.

CTI understands and complies with all Dispute sections.

2.3.6.1 Common Operational Requirements (J.2.6.1) [RIN: MMR0175-DN]

Pursuant to the requirements in Section J.2.6.1, CTI will follow all requirement processes and procedures: Common Operational Requirements

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

- The government disputes the content of a BI or TAX submitted by CTI (see Section J.2.5 Billing)
- The government disputes the content of an Inventory Reconciliation (IR) submitted by CTI (see Section J.2.7 Inventory Management). Inventory disputes will only occur if the remedies in G.7.1.4.1 are not sufficient
- The government disputes a SLA Credit Request (SLACR) Response submitted by CTI (see Section J.2.8 SLA Management)

2.3.6.2 Dispute Process (J.2.6.2) [RIN: MMR0176-DN, MMR0177-DN, MMR0178-DN, MMR0179-DN]

With respect to the requirements in Section J.2.6.2, CTI will follow all requirement processes and procedures and shall submit them to both the customer and to GSA:

1. If the government is opening the dispute, it will submit a Dispute data set.
2. CTI shall work with the government to resolve the dispute as described in Section G.4.4 Disputes.
3. NLT the 15th business day of each month, CTI shall submit a Dispute Report (DR) that captures the current status of each opened dispute.
4. If applicable, upon resolution, CTI shall apply any credits on a BA within two (2) billing cycles

2.3.6.3 Deliverables & Data Exchange (J.2.6.3)

2.3.6.3.1 Government-Provided Data Sets (J.2.6.3.1) [RIN: MMR0180-DN]

For each data set, CTI shall support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms' including the following:

Data Set	Frequency	Transfer Mechanism
Dispute	As required	Secure FTP, Email, Contractor's Web Interface, and Other means as agreed or required in the TO

2.3.6.3.2 Contractor-Provided Data Sets (J.2.6.3.2) [RIN: MMR0181-DN, MMR0182-DN]

As per Section J.2.6.3.2, the following table lists the deliverables CTI shall provide as part of this process. For each data set, CTI shall also support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms:

Data Set	Frequency	Transfer Mechanism
Billing Adjustment (BA)	See Section J.2.5 Billing	See Section J.2.5 Billing

Data Set	Frequency	Transfer Mechanism
Dispute Report (DR)	Monthly, NLT 15th business day	Secure FTP, Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO

2.3.7 INVENTORY MANAGEMENT (J.2.7) [RIN: MMC0027-DI]

Per the requirement in Section J.2.7, CTI shall support all Inventory Management requirements including Common Operational Requirements, Process requirements, and Deliverables and Data Exchange requirements.

2.3.7.1 Common Operational Requirements (J.2.7.1)

2.3.7.1.1 GSA Conexus Inventory (J.2.7.1.1)

2.3.7.1.2 Agency Hierarchy Code (J.2.7.1.2) [RIN: MMR0183-DN, MMR0184-DN, MMR0185-DN]

The AHC must be tracked for all services from order through disconnection and CTI agrees to: (1) support AHC changes without an interruption of service, and (2) provide the AHC as a data element in the Inventory Reconciliation (IR) deliverable (see Section J.2.7.2 Inventory Management Process).

2.3.7.1.3 Unique Billing Identifier (J.2.7.1.3) [RIN: MMR0186-DN]

In compliance with requirements in Section J.2.7.1.3, CTI shall ensure the UBI reported on the IR, matches the UBI included on the SOCN, and BI for a particular element.

2.3.7.2 Inventory Management Process (J.2.7.2) [RIN: MMR0187-DN, MMR0188-DN, MMR0189-DN, MMR0190-DN]

Unless otherwise specified, CTI shall submit all deliverables in the process below to GSA and, if requested, to the customer. All deliverables and other data sets included in the process below are defined in Section J.2.7.3 Deliverables and Data Exchange.

1. CTI shall submit an IR deliverable monthly, NLT the 15th day of the month.
2. If CTI identifies a discrepancy in a previously submitted IR, it shall submit a corrected IR within 3 days of identifying the discrepancy.
3. If the government identifies a discrepancy in the IR, it will follow the dispute process (Section J.2.6 Disputes).

2.3.7.3 Deliverables & Data Exchange (J.2.7.3)

2.3.7.3.1 Government-Provided Data Sets (J.2.7.3.1)

2.3.7.3.2 Contractor-Provided Data Sets (J.2.7.3.2) [RIN: MMR0191-DN, MMR0192-DN]

The following table lists the deliverables CTI shall provide as part of this process. For each data set, CTI shall support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms

Data Set	Frequency	Transfer Mechanism
Inventory Reconciliation (IR)	Monthly, NLT 15th day of month	Secure FTP, Email (if requested by the customer), Contractor's Web Interface, and Other means as agreed or required in the TO

2.3.8 SLA MANAGEMENT (J.2.8) [RIN: MMC0028-DI]

Per the requirement in Section J.2.8, CTI shall support all SLA Management requirements including Common Operational Requirements, Process requirements, and Deliverables and Data Exchange requirements.

2.3.8.1 Common Operational Requirements (J.2.8.1)

2.3.8.1.1 SLA Measurement (J.2.8.1.1) [RIN: MMR0193-DN]

Pursuant to the requirement in Section J.2.8.1.1, CTI shall proactively measure each applicable SLA in accordance with its definition, capturing its performance relative to each KPI associated with the SLA as described in Section G.8.3.1 Measurement.

2.3.8.1.2 SLA Credit Requests (J.2.8.1.2) [RIN: MMR0194-DN]

In the event of a missed SLA, the government shall issue a credit request within six (6) months of the SLAR containing the SLA failure. In conformance to Section J.2.8.1.1 and based on the procedure as laid out in G.8.4.1 Credit Management, CTI will respond to the request within 30 days by submitting a SLACR response and issue the credit within two billing cycles of this response unless CTI chooses to reject the request.

2.3.8.2 SLA Management Process (J.2.8.2) [RIN: MMR0195-DN]

Per the requirement in Section J.2.8.2, Unless otherwise specified, CTI shall submit all deliverables in the process below to GSA and, if requested, to the customer.

2.3.8.2.1 SLA Reporting Process (J.2.8.2.1) [RIN: MMR0196-DN, MMR0197-DN, MMR0198-DN]

1. CTI will measure each KPI associated with each applicable SLA as described in Section G.8 Service Level Management.
2. CTI will submit a Service Level Agreement Report (SLAR), which captures its performance on all applicable SLAs and associated KPIs monthly, NLT the 15th day of the month.
3. CTI will submit supplementary reports quarterly:
    a. Trouble Management Performance Summary Report (see G.8.5.2.3)
    b. Trouble Management Incident Performance Report (see G.8.5.2.4)

2.3.8.2.2 SLA Credit Process (J.2.8.2.2) [RIN: MMR0199-DN, MMR0200-DN]

In accordance with Section G.8.4 SLA Credit Management Methodology, credits for failed SLAs are managed with the following process:

1. The government shall issue a SLA Credit Request (SLACR) within six (6) months of the SLAR containing the SLA failure.
2. CTI shall submit a SLACR response within 30 days of the SLACR.

3. If CTI accepts the government's finding, the credit shall be reflected on a BA within two (2) billing cycles of the SLACR response.
4. If CTI disagrees with the government's finding, the government may use the dispute process as defined in Section G.4.4 Disputes and Section J.2.6 Disputes.

2.3.8.3 Deliverables and Data Exchange (J.2.8.3)

2.3.8.3.1 Government-Provided Data Sets (J.2.8.3.1) [RIN: MMR0201-DN]

As per the requirement in Section J.2.8.3.1, for each data set, CTI shall support all defined transfer mechanisms as defined in Section J.2.9: Data Transfer Mechanisms.

2.3.8.3.2 Contractor-Provided Data Sets (J.2.8.3.2) [RIN: MMR0202-DN, MMR0203-DN]

As per the requirement in Section J.2.8.3.2, the following table lists the deliverables CTI shall provide as part of this process. For each data set, CTI shall support all required transfer mechanisms as defined in Section J.2.9 Data Transfer Mechanisms.

Data Set	Frequency	Transfer Mechanism
Service Level Agreement Report (SLAR)	Monthly, NLT 15th day of month	Secure FTP, Email (if requested by the customer), and Other means as agreed or required in the TO
SLA Credit Request Response	Within 30 days of SLACR	Email/Other means as agreed or required in the TO
Trouble Management Performance Summary Report	Quarterly, NLT 14 days after the end of the FY quarter	Email Other means as agreed or required in the TO
Trouble Management Incident Performance Report	Quarterly, NLT 14 days after the end of the FY quarter	Email Other means as agreed or required in the TO
Billing Adjustment (BA)	See Section J.2.5 Billing	See Section J.2.5 Billing

2.3.9 DATA TRANSFER MECHANISMS (J.2.9) [RIN: MMC0029-DI, MMR0204-DN]

CTI shall support all Data Transfer Mechanism requirements including Common Operational Requirements, Direct Data Exchange requirements, CTI Web Interface requirements, Email requirements, GSA Systems requirements and Other requirements. CTI shall support all data transfer mechanisms required for each data set Common Operational Requirements (J.2.9.1)

2.3.9.1.1 Governance of Exceptions (J.2.9.1.1)

2.3.9.1.2 Multiple Transfer Mechanisms (J.2.9.1.2) [RIN: MMR0205-DN, MMR0206-DN]

As per the requirement in Section J.2.9.1.2 , CTI shall maintain the capability to accept all required data transfer mechanisms for data sets transferred from the government back to CTI. CTI shall also submit data to the government using the listed data transfer mechanisms unless an exception is approved by the relevant CO.

2.3.9.2 Direct Data Exchange (J.2.9.2)

2.3.9.2.1 Direct Data Exchange Mechanisms (J.2.9.2.1) [RIN: MMR0207-DN]

CTI shall support direct data exchange between its BSS and GSA Conexus based on the requirements captured in Section G.5.3.2 Direct Data Exchange using the following methods:

- Web Services: Extensible Markup Language (XML) over secure hypertext transfer protocol (HTTPS) using SOAP (formerly Simple Object Access Protocol) and applying commercial practices and standards
- Secure File Transfer Protocol (SFTP): Pipe-Separated Value (PSV) exchanged via a server operated by or on behalf of GSA

2.3.9.2.2 Attachments via Direct Data Exchange (J.2.9.2.2) [RIN: MMR0208-DN, MMR0209-DN, MMR0210-DN, MMR0211-DN]

CTI shall also submit any Binary Large Object (BLOB) attachments required in the definitions of the various data sets in Section J.2.10.2. CTI shall also transfer these files separately via SFTP as described above and name the files based on the following template:

- CTRPREFIX-DTT-SEQNUM-ELEMENT.EXT

Each part of this filename template is defined below:

- CTRPREFIX = Code that uniquely identifies CTI
- DTT = Data Transaction Code from the associated data set:
  - See Section J.2.10.1.1.5
- SEQNUM = Data Transaction Sequence Number from the associated data set:
  - See Section J.2.10.2 Data Set Content
- ELEMENT = Element name of the attachment
- EXT = Standard file extension based on file type
- Each component of the filename is separated by a single dash, “-” with the exception of the extension, which is separated by a single period, “.”

Example: ABC-SOCN-0837654-design_documents.zip would indicate that CTI had registered the prefix ABC, was submitting this file as part of a Service Order Completion Notice (SOCN), had given the SOCN in question the sequence number 0837654, was submitting this file as the design documents data element, and had packaged one or more files in a ZIP container.

Note: CTI shall not submit attachments with filenames that are not fully compliant with the specified template except as authorized in Section J.2.9.1.1 Governance of Exceptions.

2.3.9.3 Contractor's Web Interface (J.2.9.3)

2.3.9.4 Email (J.2.9.4) [RIN: MMR0212-DN]

As per the requirement in Section J.2.9.4 , when emailing data to the government, CTI shall follow the following requirements:

Email is specified as the data transfer mechanism in cases where the data is unstructured or not intended for automated analysis. Data emailed from the government to CTI may be included in the body of the email or in one or more attachments.

When emailing data to the government, CTI shall:

- Use body text only for brief information (not to exceed 150 words).
- Use attachments for longer data sets or for structured data.
- Use attachment formats that are compatible with one of the following: (a) Microsoft Office (current version and two most recent prior versions); (b) Portable Document Format (PDF); or (C) other formats as approved in writing by the relevant CO.
- Encrypt attachments if required by the TO or the relevant CO.
- Include appropriate contract and TO identification information in the body and all attachments.
- Submit directly to the Point of Contact (POC) specified by the OCO.

2.3.9.5 GSA Systems (J.2.9.5) [RIN: MMR0213-DN]

Pursuant to the requirements in Section J.2.9.5, any Data submitted to GSA Systems, by CTI, will be submitted as uploaded files in either: (1) the original format of the document; or (2) in Comma-Separated Value (CSV) format, as defined for each deliverable specified as submitted via GSA Systems in Section J.2.10.2.

2.3.9.6 Other Means as Agreed or Required in the TO (J.2.9.6)

2.3.10 DATA DICTIONARY (J.2.10) [RIN: MMC0030-DI]

As per the requirement in Section J.2.10, CTI shall support all Data Dictionary requirements including Common Data Requirements, Data Set Content requirements, and Data Element Specification requirements.

2.3.10.1 Common Data Requirements (J.2.10.1)

2.3.10.1.1 Extended Data Element Definitions (J.2.10.1.1)

2.3.10.1.1.1 Associated Government Fee (J.2.10.1.1.1) [RIN: MMR0214-DN]

As per the requirement in Section J.2.10.1.1.1, for direct-billed customers, on a monthly basis CTI shall collect the AGF from the customer and remit to GSA as described in Section G.4.6 Associated Government Fee (AGF). The following requirements will be met concerning how the AGF rate structure is governed:

1. The AGF rate will be the same for all TOs under this contract
2. The AGF rate may change during the period of performance of this contract
3. The GSA CO will provide CTI with notice of any changes to the AGF rate at least 30 days prior to the effective date of the new rate.

2.3.10.1.1.1.1 AGF Rate Structure (J.2.10.1.1.1.1)

2.3.10.1.1.1.2 AGF Calculation (J.2.10.1.1.1.2)

2.3.10.1.1.2 Unique Billing Identifier (J.2.10.1.1.2)

2.3.10.1.1.2.1 UBI Specifications (J.2.10.1.1.2.1) [RIN: MMR0215-DN, MMR0216-DN, MMR0217-DN, MMR0231-DN]

The UBI consists of two substrings separated by an underscore, "_":

1. Service Grouping ID: This value is unique to the grouping of services. It is shared by all components of the group but never reused for another group.
2. Component ID: This value is unique to each component within the group. It shall not be reused within the group but is not necessarily unique across groups.

CTI shall provide the UBI in accordance with those specifications and the following requirements: the complete UBI shall contain only the single prescribed underscore, and the complete UBI shall be unique across the contract and shall never be reused. Provided all other UBI requirements are met, CTI may: Use existing fields in its system to capture the Service Grouping ID and the Component ID provided they are concatenated as described above on submission and/or Determine the form of the Service Group ID and Component ID.

2.3.10.1.1.2.2 UBI Process Requirements (J.2.10.1.1.2.2) [RIN: MMR0218-DN, MMR0219-DN, MMR0220-DN, MMR0221-DN, MMR0222-DN, MMR0020-DN]

1. CTI shall create and assign the UBI for each installed service instance in compliance with the UBI Specifications described above, even if there is only one member of the group.
    a. Installed Service Instance Definition: a unique installation of a particular CLIN (or CLIN + ICB Case Number combination, if applicable)

b. For SRE, the UBI is assigned as above with each associated SRE Pricing Element using the same UBI (see also Section B.2.10)

2. CTI shall provide the UBI to the government as part of the SOCN (see Section J.2.4 Ordering) and all other deliverables where it is a listed data element as specified in Section J.2.10.2 Data Set Content.
3. For auto-sold CLINs and CLIN bundling (see Section B.1.2.12), CTI shall assign UBIs to the base CLIN (including TUCs), and to each associated auto-sold or component CLIN, and ensure the service grouping is the same on each.
4. CTI shall maintain the UBI assignment for the duration of the contract even if the service is later disconnected.
5. CTI shall apply logical grouping when constructing the service grouping (e.g., a circuit with originating and terminating ends and equipment at each end shall all be included in the same service grouping).

2.3.10.1.1.3 Network Site Code (J.2.10.1.1.3) [RIN: MMR0223-DN]

In compliance with the requirements in Section J.2.10.1.1.3, CTI will agree to the following specifications. CTI shall:

1. Obtain access to the iConectiv CLONES database if CTI does not already have such access. Although such access is required to support this contract, the government will not reimburse CTI for access to the database. CTI shall be solely responsible for any charges incurred.
2. Use the iconectiv CLONES database to derive the NSC for all locations associated with an order:
    a. For dedicated access circuits, the circuit terminating location shall be used to derive the NSC.
    b. For installed Service Related Equipment (SRE), the physical location of the SRE shall be used to derive the NSC.
    c. For all other cases, including those services with no originating or terminating location, the address of the customer representative accepting the service (typically a local point of contact) shall be used to derive the NSC.

3. Request an NSC from the iconectiv CLONES provider if the NSC for the location does not exist in the iconectiv CLONES database.
4. Capture and store the NSC, billing, originating and terminating address information as applicable, and provide the same on all deliverables as specified in the deliverable content list.

2.3.10.1.1.4 Order Types (J.2.10.1.1.4)

2.3.10.1.1.4.1 Orders for New Services (J.2.10.1.1.4.1) [RIN: MMR0224-DN]

For orders for new services, CTI shall assign order types as follows: Header Order Type = Install & Line Item Order type = Add.

2.3.10.1.1.4.2 Orders to Change Existing Services (J.2.10.1.1.4.2)

2.3.10.1.1.4.2.1 Move Orders (J.2.10.1.1.4.2.1) [RIN: MMR0225-DN]

For move orders, CTI shall assign order types as follows:

- Header Order Type = Change
- Removal of the existing service: Line Item Order type = Remove
- Re-installation of the same service at the new location: Line Item Order type = Add

2.3.10.1.1.4.2.2 Change in Features (J.2.10.1.1.4.2.2) [RIN: MMR0226-DN, MMR0227-DN]

For feature changes that require a CLIN change, CTI shall assign order types as follows:

- Disconnection of existing features and CLINs: Header Order Type = Change & Line Item Order type = Remove
- Installation of new features and CLINs: Header Order Type = Install & Line Item Order type = Add
- For feature changes that do not require a CLIN change, CTI shall assign order types as follows:
- Feature additions: Header Order Type = Change & Line Item Order type = Add
- Feature removals: Header Order Type = Change & Line Item Order type = Remove

2.3.10.1.1.4.2.3 Configuration (J.2.10.1.1.4.2.3) [RIN: MMR0228-DN]

For configuration orders, CTI shall assign order types as follows: Header Order Type = Change & Line Item Order type = Configuration.

2.3.10.1.1.4.2.4 Disconnect (J.2.10.1.1.4.2.4) [RIN: MMR0229-DN]

For disconnect orders, CTI shall assign order types as follows: Header Order Type = Change & Line Item Order type = Remove.

2.3.10.1.1.4.2.5 Change in Administrative Data (J.2.10.1.1.4.2.5) [RIN: MMR0230-DN]

For administrative change orders, CTI shall assign order types as follows: Header Order Type = Change & Line Item Order type = Administrative.

2.3.10.1.1.4.3 Orders to Supplement or Update In-progress Orders (J.2.10.1.1.4.3)

2.3.10.1.1.4.3.1 Order Cancellation (J.2.10.1.1.4.3.1) [RIN: MMR0232-DN]

For order cancellation updates, CTI shall assign order types as follows:

- Header Order Type = Cancel
- Line Item Order type = Cancel

2.3.10.1.1.4.3.2 Line Cancellation (J.2.10.1.1.4.3.2) [RIN: MMR0233-DN]

For order cancellation updates, CTI shall assign order types as follows:

Line cancellation updates are defined as order updates that cancel the line item in the original order. For line cancellation updates, CTI shall assign order types as follows:

- Header Order Type = Supplement
- Line Item Order type = Cancel

2.3.10.1.1.4.3.3 Updated Specified Location (J.2.10.1.1.4.3.3) [RIN: MMR0234-DN, MMR0235-DN]

For location change updates that have an impact on LEC provisioning, CTI shall assign order types as follows:

- Cancelation of existing SO line item:
  - Header Order Type = Supplement
  - Line Item Order type = Cancel
- Corrected order with addition of new features and CLINs:
  - Header Order Type = Install
  - Line Item Order type = Add

For location change updates that do not have an impact on LEC provisioning, the contractor shall assign order types as follows: Header Order Type = Supplement & Line Item Order type = Update.

2.3.10.1.1.4.3.4 Updated Specified Features (J.2.10.1.1.4.3.4) [RIN: MMR0236-DN, MMR0237-DN]

For feature changes that require a CLIN change, CTI shall assign order types as follows:

- Cancel of original order features and CLINs:

- Header Order Type = Supplement
- Line Item Order type = Cancel

- Corrected order with addition of new features and CLINs:
  - Header Order Type = Install
  - Line Item Order type = Add

For feature changes that do not require a CLIN change, CTI shall assign order types as follows: Header Order Type = Supplement & Line Item Order type = Update.

2.3.10.1.1.4.3.5 Update Specified Customer Want Date (J.2.10.1.1.4.3.5) [RIN: MMR0238-DN]

For CWD updates, CTI shall assign order types as follows: Header Order Type = Supplement & Line Item Order type = Update.

2.3.10.1.1.4.3.6 Update Specified Administrative Data (J.2.10.1.1.4.3.6) [RIN: MMR0239-DN]

For administrative data updates, CTI shall assign order types as follows: Header Order Type = Supplement & Line Item Order type = Update.

2.3.10.1.1.4.3.7 Clarification of Line Items Being Updated (J.2.10.1.1.4.3.7)

2.3.10.1.1.5 Data Transaction Code (J.2.10.1.1.5) [RIN: MMR0240-DN, MMR0241-DN]

Each data set exchanged between CTI and GSA, regardless of direction, shall include an element labeled data_transaction_code. This code uniquely identifies the specific data set (i.e., it distinguishes a Billing Invoice from a Billing Adjustment). Unless otherwise specified, each data set defined in Section J.2.10.2 has a unique data transaction code included in its definition. CTI shall include the correct code in each data set submitted to GSA as detailed in the data set definition.

2.3.10.1.2 Data Consistency (J.2.10.1.2) [RIN: MMR0242-DN]

Per the requirements in Section J.2.10.1.2, CTI shall submit each data element in a consistent format as per the following: Unless otherwise specified, CTI is free to format data according to its normal commercial practices. However, CTI shall submit each data element in a consistent format.

2.3.10.1.3 Data Set Infrastructure (J.2.10.1.3)

2.3.10.1.3.1 GSA Systems CSV Structure (J.2.10.1.3.1) [RIN: MMR0243-DN]

Per the requirements in Section J.2.10.1.3.1, for all data sets submitted as CSV via GSA Systems, the data element order listed in Section J.2.10.2 shall be used in structuring the table (i.e., the column order of the submitted table shall match the specified field order). For data sets submitted with multiple rows of data, all data elements are included in each row even if unchanged from the previous row.

2.3.10.1.3.2 PSV Structure (J.2.10.1.3.2) [RIN: MMR0244-DN]

Per the requirements in Section J.2.10.1.3.2, for all data sets submitted using PSV over SFTP, the data element order listed in Section J.2.10.2 shall be used in structuring the PSV file (i.e., the column order of the submitted file shall match the specified field order). For data sets submitted with multiple rows of data, all data elements are included in each row even if unchanged from the previous row.

2.3.10.1.3.3 XML & Web Services Structure (J.2.10.1.3.3) [RIN: MMR0245-DN, MMR0246-DN]

Pursuant to the requirement in Section J.2.10.1.3.3, for all data sets submitted using XML over Web Services, the data shall be structured in accordance with the applicable XML Schema Definitions (XSDs), Web Services Definition Language (WSDL) documents, and associated documents provided by GSA. CTI shall use these schemas and documents in establishing Web Services connections with GSA Conexus.

2.3.10.2 Data Set Content (J.2.10.2)

2.3.10.2.1 Data Sets: Primary Data (J.2.10.2.1) [RIN: MMR0247-DN, MMR0248-DN, MMR0249-DN, MMR0250-DN]

The columns of the tables in this section are defined below:

- Value Requirement:Contains one of the following which have specific defined meanings:
    - Always: CTI shall supply the correct value for the element on all submissions.
    - If Applicable: CTI shall supply the correct value for the element on all submissions where the value is applicable.
    - Either/Or: CTI shall supply the correct value for only one of the data elements so labeled and shall apply the specific requirements for that data set in choosing which to supply.
- Unique Value Level: Contains one of the following values, which have specific defined meanings:
    - Data Set: Each data set contains only one unique value for this element. For data sets submitted in tabular format (e.g. PSV over secure FTP), each line item shall contain the same value for this data element.

2.3.10.2.1.1 Administrative Change Order (J.2.10.2.1.1)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.2 AGF Detail (J.2.10.2.1.2)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.3 AGF Electronic Funds Transfer Report (J.2.10.2.1.3)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.4 Billing Adjustment (J.2.10.2.1.4)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.5 Billing Invoice (J.2.10.2.1.5)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.6 Reserved [RIN: MMR0251-DN]

Reserved.

2.3.10.2.1.7 Reserved [RIN: MMR0252-DN]

Reserved.

2.3.10.2.1.8 Direct Billed Agency Setup (J.2.10.2.1.8) [RIN: MMR0253-DN]

Per the requirements in Section J.2.10.2.1.8, if multiple transactions are required, each will be submitted separately by CTI. CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.9 Dispute (J.2.10.2.1.9)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.10 Dispute Report (J.2.10.2.1.10)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.11 Firm Order Commitment Notice (J.2.10.2.1.11)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.12 Inventory Reconciliation (J.2.10.2.1.12)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.13 Monthly Billing Information Memorandum (J.2.10.2.1.13)

Ulness otherwise specified by the TO, CTI has the option to use its standard commercial report format for this report provided it contains the sufficient data to: uniquely identify the associated BI, clearly communicate key elements in the BI that require explanation or background information, and provide an overview of CTI's reasoning, explanation and/or background information.

2.3.10.2.1.14 Service Level Agreement Report (J.2.10.2.1.14)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.15 Service Order (J.2.10.2.1.15) *table* [RIN: MMR0254-DN, MMR0255-DN]

Data Transaction Code: SO

When submitted via any means other than CTI's web interface, the government may use a variety of structured or unstructured formats for this data set unless otherwise specified by the TO. In all cases, the data set submitted by the government will contain sufficient information for CTI to successfully complete the order and meet contract and

TO requirements. The information that CTI shall collect includes but is not limited to: TO Number and TO Modification Number (if applicable), Header Level Order Type, Customer Want Date and Early Installation Approval/Disapproval, Contact information for COR, Government project code (optional), Line Item Details[Line Item Level Order Type (If type is Administrative, see Section J.2.10.2.1.1 Administrative Change Order), AHC, ASRN(s), CLIN, Quantity], Any comments from the government on handling the order, Any data elements necessary to successfully complete the order or required by the TO, and If the header level order type is Supplement (see also Section J.2.10.1.1.4.3), the government will include sufficient information to clearly communicate: The order being updated (e.g. CSRN), The line items being updated, or Updates to be made. When submitted via CTI's web interface, the government will use the format required by that interface for this data set and will supply the data elements marked as required on that interface.

Note: CTI shall be responsible for collecting all order information from the government necessary to complete all other deliverables. CTI may, with OCO concurrence, further define how that data is provided - e.g. limiting the number of different AHCs or ASRNs that may be processed on a single order, requiring pre-registration of project codes, etc.

2.3.10.2.1.16 Service Order Acknowledgement (J.2.10.2.1.16)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.17 Service Order Administrative Change (J.2.10.2.1.17)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.18 Service Order Completeion Notice (J.2.10.2.1.18)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.19 Service Order Confirmation (J.2.10.2.1.19)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.20 Service Order Rejection Notice (J.2.10.2.1.20)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.21 Service State Change Notice (J.2.10.2.1.21)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.22 SLA Credit Request (J.2.10.2.1.22)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.23 SLA Credit Request Response (J.2.10.2.1.23)

Unless otherwise specified by the TO, CTI has the option to use its standard commercial report format for this report provided it contains sufficient data to: uniquely

identify the associated SLACR, clearly communicate CTI's agreement or disagreement with the SLACR, indicate if CTI intends to issue a BA, and provide an overview of CTI's reasoning in reaching its decision.

2.3.10.2.1.24 Tax Detail (J.2.10.2.1.24)

CTI acknowledges the presence of this data transaction code.

2.3.10.2.1.25 Trouble Management Incident Performance Report (J.2.10.2.1.25))

Unless otherwise specified by the TO, CTI may use its standard commercial report format for this report provided it contains the information specifried in Section G.8.5.2.4 Trouble Management Incident Performance Report.

2.3.10.2.1.26 Trouble Management Performance Summary Report (J.2.10.2.1.26)

Unless otherwise specified by the TO, CTI may use its standard commercial report format for this report provided it contains the information specifried in Section G.8.5.2.3 Trouble Management Performance Summary Report.

2.3.10.2.2 Data Sets: Reference Data (J.2.10.2.2)

CTI acknowledges the data transaction codes in Sections J.2.10.2.2.1 through J.2.10.2.2.32, and the data elements therein. These data sets will be transferred from GSA to CTI and will always include values for all data elements.

2.3.10.2.3 Data Sets: Task Order Data (J.2.10.2.3)

2.3.10.2.3.1 TO CLINs Awarded (J.2.10.2.3.1) [RIN: MMR0256-DN]

The TO CLINs Awarded deliverable is required when not all CLINs for a service have been awarded to CTI. It contains only the CLINs that were awarded to CTI within the TO. This data shall be submitted in CSV format via GSA Systems and contain the data elements from the table in Section J.2.10.2.3.1.

2.3.10.2.3.2 TO Customer Requirements Document Set (J.2.10.2.3.2) [RIN: MMR0257-DN]

The TO Customer Requirements Document Set deliverable fully describes the TO requirements. CTI shall submit the following documents in their original formats to GSA Systems: final version of the Request for Proposal (RFP), Request for Quote (RFQ), or equivalent document issued by the agency, inclusive of all amendments, any other documents the customer uses to support its requirements, Final TO Proposal Volumes, and TO Award Document.

2.3.10.2.3.3 TO Financials (J.2.10.2.3.3) [RIN: MMR0258-DN, MMR0259-DN, MMR0021-DN]

The TO Financials deliverable contains the financial data for each TO. The table shall include a separate line for each performance period covered by the TO. This data shall

be submitted in CSV format to GSA Systems and contain the data elements from the table in Section J.2.10.2.3.3.

2.3.10.2.3.4 TO Country/Jurisdictions Awarded by Service (J.2.10.2.3.4) [RIN: MMR0260-DN]

The TO Country/Jurisdictions Awarded by Service deliverable contains all countries/jurisdictions awarded by service to CTI within the TO. This data shall be submitted in CSV format to GSA Systems and contain the data elements from the table in Section J.2.10.2.3.4.

2.3.10.2.3.5 TO Key Performance Indicators (J.2.10.2.3.5) [RIN: MMR0261-DN]

The TO Key Performance Indicators deliverable contains all KPIs specific to the TO where: 1) the KPIs are not in the contract, or 2) the TO overrides the contract KPI. This data shall be submitted in CSV format to GSA Systems and contain the data elements from the table in Section J.2.10.2.3.5.

2.3.10.2.3.6 TO Locations Awarded by Service (J.2.10.2.3.6) [RIN: MMR0262-DN, MMR0263-DN]

The TO Locations Awarded by Service deliverable contains customer locations by service awarded to CTI within the TO for those services not awarded at the country/jurisdiction level. Services awarded at the country/jurisdiction level shall be omitted from this deliverable. This data shall be submitted in CSV format via GSA Systems and contain the data elements from the table in Section J.2.10.2.3.6.

2.3.10.2.3.7 TO Officials (J.2.10.2.3.7) [RIN: MMR0264-DN]

The TO Officials deliverable contains all OCOs and CORs (if applicable) associated with the TO. This data shall be submitted in CSV format via GSA Systems and contain the data elements the table from Section J.2.10.2.3.7.

2.3.10.2.3.8 TO Services Awarded (J.2.10.2.3.8) [RIN: MMR0265-DN]

The TO Services Awarded deliverable contains all services awarded to CTI within the TO. This data shall be submitted in CSV format via GSA Systems and contain the contractor_invoice_level_account_number, service_id, and all_clins.

2.3.10.3 Data Element Specifications (J.2.10.3)

2.3.10.3.1 Primary Data Element Dictionary (J.2.10.3.1)

2.3.10.3.1.1 Interpreting the Primary Data Element List (J.2.10.3.1.1) [RIN: MMR0266-DN, MMR0267-DN]

CTI will abide by the requirements for the Edit Mask Values.

2.3.10.3.1.2 Primary Data Element List (J.2.10.3.1.2) [RIN: MMR0268-DN, MMR0269-DN]

Element Name	Description	Data Type	Length	Edit Mask
data_transaction_line_sequence_number	Data Transaction line sequence number. CTI shall assign a unique data transaction line sequence number to each record within a deliverable.	Numeric	14	

2.3.10.3.2 Reference Data Element Dictionary (J.2.10.3.2)

2.3.10.3.2.1 Interpreting the Reference Data Element List (J.2.10.3.2.1)

2.3.10.3.2.2 Reference Data element Dictionary Table (J.2.10.3.2.2)

3.0 MANAGEMENT VOLUME DOCUMENTS (L.30.2)

3.1 PROGRAM MANAGEMENT PLAN (PMP) (L.30.2.1; M.2.2 (3); G.9.4)

[redacted]

CTI's management team and staff are committed to fully supporting the GSA's EIS Program ensuring, to the extent possible, a problem-free installation, transition, and on-going support and maintenance for the EIS program. As part of our overall program management effort detailed in the sections below, we will conduct regularly scheduled meetings with key personnel to ensure we are meeting program and project (Task Order) schedules, and assigning/allocating the appropriate number of resources to meet the specified requirements. [redacted]

[redacted] We are fully committed to implementing a Program Management structure that strengthens the probability of achieving problem-free and very successful results for EIS transition, implementation, on-going operations, maintenance, and customer services.

3.1.1 SUMMARY OF CONTRACT MANAGEMENT REQUIREMENTS [L.30.2.1 (1); G.9.4 (1)] [RIN: MMR0011-DN]

CTIs contract management, including government dependencies and assumptions regarding government services, facilities, and personnel are summarized in the following paragraphs. [redacted]

CTI shall provide technical expertise across all services, via our subject matter experts and/or Program Manager and customer representatives and 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 the Trouble Ticket Management General Requirements. CTI shall provide the escalation procedure for the government to escalate issues to appropriate levels of our management to resolve disputes and issues. CTI shall have the authority to:

- Support disaster recovery planning and execution
- Resolve interoperability problems
- Respond to escalation of service concerns
- Participate in contract performance reviews
- Participate in contract modification negotiations
- Perform basic network management functions in support of the government's requirements as described in our Service Level Management section.
- Help resolve billing queries and reconciliation issues
- Support NS/EP requirements
- Provide the EIS PMO with information on customer requirements and customer demographics

Within 30 days of the Notice to Proceed, CTI shall provide and maintain a Contractor Points of Contact List that provides contact information for, at a minimum, the functions that follow:

- Provisioning orders
- Identifying and resolving service troubles and complaints
- Providing customers with status of troubles and resolution
- Developing and delivering training
- Conducting billing inquiries
- Transition project management
- Finance
- Contracting
- Account Management (business development and sales)
- Security
- NS/EP

3.1.2 CTI SHALL IDENTIFY ITS SECURITY POCS WHO WILL BE PROCESSING BACKGROUND INVESTIGATIONS AND SECURITY CLEARANCES AT THE APPROPRIATE LEVELS AND PERFORM PERSONNEL BACKGROUND INVESTIGATION REQUIREMENTS AND OTHER BSS SECURITY REQUIREMENTS. POCS THAT HAVE PASSED NATIONAL AGENCY CHECKS OR BACKGROUND INVESTIGATIONS, AND THE SECURITY CLEARANCE LEVELS HELD BY THESE INDIVIDUALS AS DEFINED IN BSS SECURITY REQUIREMENTS. CTI'S ASSUMPTIONS IN EXECUTING THE ABOVE DEPENDS UPON CONTRACTUAL FUNDING IN PLACE TO PERFORM THE ACTIVITIES, ASSIGNMENT OF THE GOVERNMENT POC/KO, EXPEDITIOUS APPROVAL OF SECURITY DOCUMENTS AND OTHER DOCUMENTATION REQUIRED TO ACCESS GOVERNMENT FACILITIES AND PERSONNEL AND ALL OTHER STIPULATIONS OF THE GSA EIC CONTRACT. CTI ASSUMES THAT 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. THE CTI TEAM UNDERSTANDS THAT SOME TASK ORDERS WILL REQUIRE WORK TO BE PERFORMED CONUS AND OCONUS AT GOVERNMENT FACILITIES AND AT-FIELD SITES BOTH ASHORE AND, AND THAT SOME SITES MAY BE UNDER AUSTERE CONDITIONS. CTI TEAM ALSO UNDERSTANDS THAT SOME TASK ORDERS MAY REQUIRE THE USE OF GOVERNMENT SERVICES AND/OR INTEGRATION OF GOVERNMENT SERVICES WITH COMMERCIAL SERVICES. REGARDLESS, THE CTI TEAM WILL INTEGRATE GOVERNMENT SERVICES AND WILL PERFORM TO THE GOVERNMENT'S SATISFACTION ON TASK ORDERS AWARDED. PLEASE SEE THE SUPPLY CHAIN RISK MANAGEMENT PLAN, PROGRAM MANAGEMENT PLAN AND BUSINESS SUPPORT SYSTEM FOR ADDITIONAL DETAIL.SUMMARY DESCRIPTION OF THE SERVICE SOLUTION [L.30.2.1 (2), G.9.4 (2)]

[redacted]

3.1.3 DRAFT PROGRAM MANAGEMENT SCHEDULE (L.30.2.1 (3); G.9.4 (3))

Core Technologies, as a result of the EIS contract will be required to tackle a very large, complex effort of combining the delivery of network elements, network infrastructure, new and changed business models, and overall changes to organizational structure and capabilities. CTI, like many other IT companies, are turning to the substantial body of experience that supports the discipline of **program management**.

[redacted]Program Management support is governed by comprehensive, efficient, and effective processes developed to consistently exceed the EIS contractual requirements.

Overview

The Government (with respect to the EIS Contract) will be provided a dedicated EIS support mechanism through CTI's EIS Program Organization (EPO). The EPO is a highly-visible organization made up of and reporting directly into the CTI executive management team, 100% dedicated to Government Accounts. The EPO will be in place and operational shortly after contract award stipulations.

The EPO coordinates and communicates the Government's EIS needs and interfaces directly with the subscribing Agencies and the GSA Program Management Office (PMO). Operating as the primary program management support for the GSA and the Agencies, the EPO manages program control, planning at the program and Agency levels, contractor performance, resource management, and revenue management. In addition, the EPO manages reporting and reviews including senior-level communications.[redacted]

The EPO comprises five offices dedicated to implementing EPO functions. They are the following primary functions:

1. Strategic Planning Office (SPO)
2. Customer Support Office (CSO)
3. Transition, Implementation & Migration Office (TIMO)
4. Product & Service Assurance Office (PSAO)
5. Business Management Office (BMO)

Each office is described in the following sections

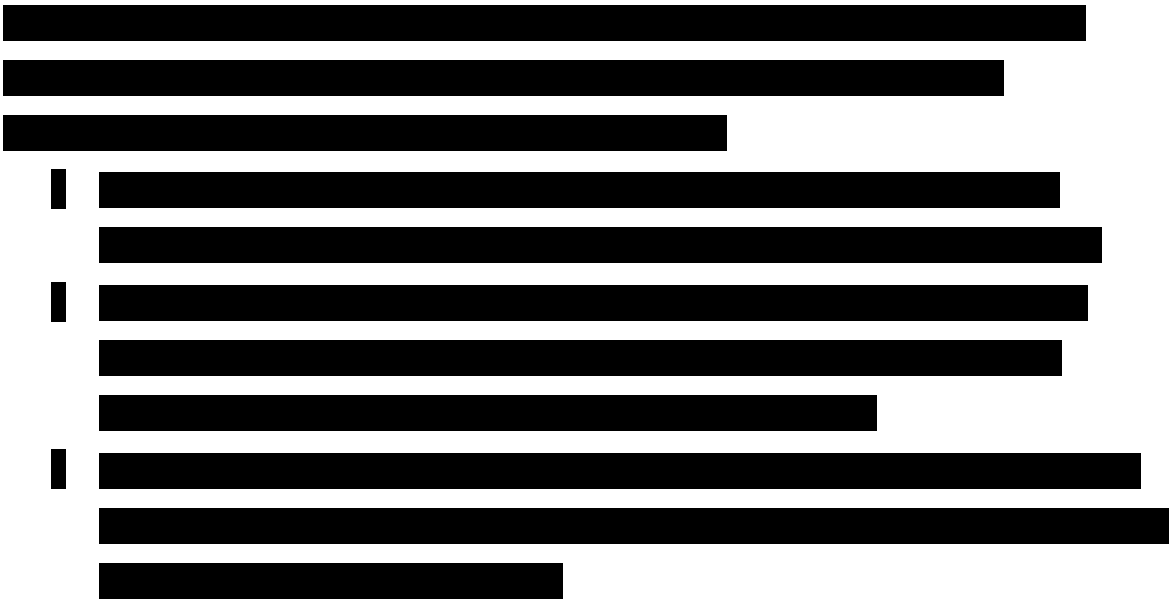
- The SPO provides Strategic Planning of the entire vendor contractual environment as well as all aspects of the EIS contract stipulations. The SPO has ultimate control over all planning and strategic steps and decisions and reports directly into the CTI Executive Management. SPO is the lead organization for planning and execution of the EIS contract.
- CSO – is a Customer-centric organization that focuses on providing world class customer support to all GSA- EIS customers. The CSO is empowered to resolve any and all customer support issues and is fully supported by CTI Executive management. The CSO acts as a single point of contact, whose entire job-focus is addressing EIS specific needs and ensuring the best possible customer service for the Government. The CSO is led by the Customer Service Manager and includes the functional key personnel critical for providing effective communication and issue resolution to the Agencies. This includes Service Ordering, Billing, Network Management, Tier 1 Support, Critical Services Support, Training and OSS Management and Change Control.
- TIMO - TIMO provides a smooth, low-risk transition by assigning SMEs who are qualified to determine appropriate escalation procedures. Transition plans produced and implemented by this team, are built with the knowledge obtained from successfully transitioning large, multi-service Government and Commercial clients with a focus on risk identification, prevention, and mitigation. The CTI TIMO will develop a Project Management approach to managing complex implementations across a variety of business units and services within one overall network transition. This methodology will be used in the development of transition plans, and in managing transitions.
- PSAO - Product & Service Assurance Office is a group that focuses heavily on quality control. Aspect such as quality of service and equipment, network functionality, trouble resolution follow up, new technology, and overall functionality of the network. A cogitative loop is formed with the CSO group as well as the TIMO group to ensure that quality controls are of the highest standards. When applicable, new equipment and services will be added and older problematic services and equipment will be sunset as appropriate. This will

assure continuous high quality service and equipment during the EIS contractual period.

- BMO – the Business Management Office provides a consistent level of support to all EIS customers for ongoing billing, accounting, rebates, SLA management, KPI management, as well as all financial EIS contractual stipulations. The BMO will also have a closely managed loop including all other CTI offices (SPO,CSO,TIMO,PSAO) to make sure that all business and financial aspects of the EIS contract are properly and efficiently managed.

Tools and Best Practices

CTI's EPO is designed to provide effective and efficient program management through the application of support tools and industry best practices.



The CTI PMO(Project Management Office), provides industry and corporation best practice guidance, tools, and templates for use by program/project teams throughout CTI. The EIS EPO will draw on this expertise in setting up EIS related program management processes and procedures.

Conclusion

Together the teams outlined above form a cohesive EPO with the capability and authority to perform all functional requirements of the EIS contract. The EPO's capability and authority spans from billing queries to disaster recovery execution.

The Draft Program management Schedule is part of the Program Management Transition and Implementation Planning Schedule in the section spreadsheet below.

3.1.4 DRAFT TRANSITION MANAGEMENT APPROACH [L.30.2.1 (4); C.3; G.9.4 (4)] [RIN: MMR0093-DN, MMR0094-DN]

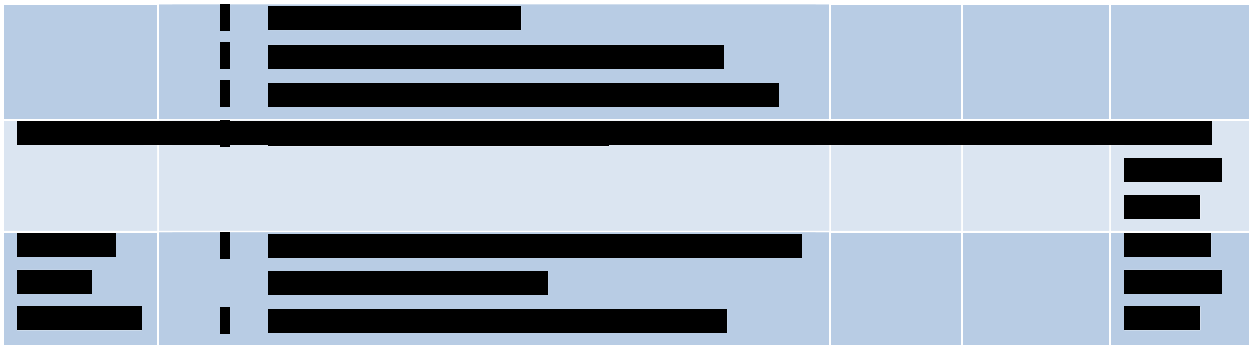
[redacted]

Our CSO PM will be responsible for overseeing Agency transitions and GSA PMO coordination. The PMO's are also responsible for planning, communication and reporting, issuance of transition notices; subcontractor management; project schedule, cutover, and final acceptance.

The goal of our TPM is to meet the GSA EIS Program's goals and objectives with minimum risk, minimum cost, and minimum impact to the day -to-day operations of the end user agency. Our TPM has the explicit authority to ensure that the appropriate planning, management, engineering, and field resources are applied to meet the Program's objectives. [redacted]

[redacted]

	[redacted]			
	[redacted]			
[redacted]	[redacted]			
	[redacted]			
	[redacted]			
	[redacted]			
	Implementation Complete			



Post Implementation Support

Many of the personnel assigned to the GSA account team during service transition and implementation will remain active on the account after implementation. This provides the steady-state GSA account team with the advantage of detailed account familiarity acquired during service transition. As the GSA account team leader, the Client Relationship Manager will ensure that we complete proper account management activities on an ongoing basis.

3.1.4.1 Transition Processes, Procedures, and Tools [L.30.2.1 (4); G.9.4 (4)] [RIN: MMR0012-DN]

This section describes CTI's approach to transition project management, including our project management process, procedures, and tools to meet the transitions requirements of GSA EIS solicitation Section C.3. Additional information is available in Section 2.4 of this volume.

For EIS there are two types of transition, "Transition On" and "Transition Off."

Transition "On" is the transfer of service from a Networx contract or a GSA Local Services Agreement (LSA) to the EIS contract.

Transition "Off" is the transfer of service from the EIS contract to a follow-on contract or service arrangement, managed by GSA in a coordinated way to prepare for the expiration of the EIS contract, conducted as specified in FAR Clause 52.237-3. Within each transition type the agency undergoing the transition may require new or enhanced

services to replace services on expiring contacts. The incentive for selecting new or enhanced services and/or undergoing a smooth transition experience is cost savings and minimizing operational impacts. [redacted]

[redacted]CTI understands the Transition – Off objectives and we will comply with the requirements for transitioning services from the EIS contract to a follow-on vehicle. CTI will conduct transition planning with GSA and provide advice on strategies to select the proper services, or improvement to current services and how to minimize the transition time and possible reduce costs. [redacted]

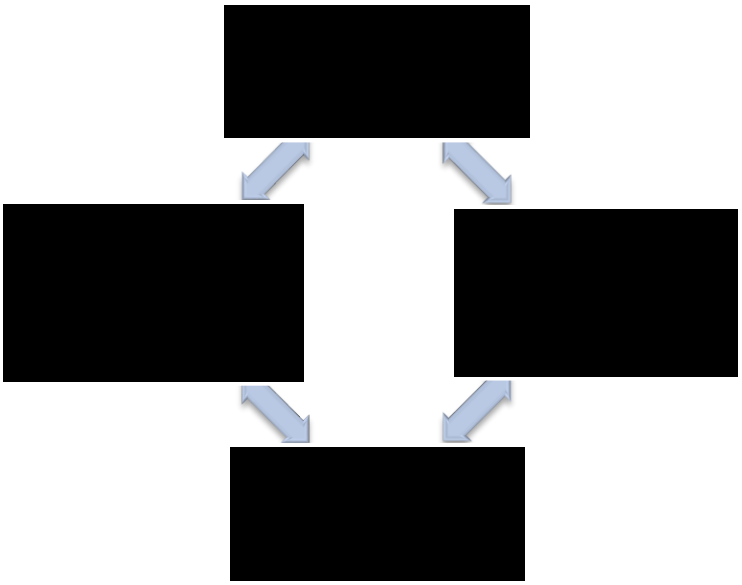
[redacted]

[redacted] The assigned transition project manager (TPM) oversees the overall implementation, including planning, development, execution, and change control. The TPM will be the main point of contact to ensure proper and timely integration of GSA or client objectives throughout the project(s) and program(s).

[redacted]

[redacted]

[redacted]



[redacted]

- [redacted]
- [redacted]
- [redacted]

[redacted]

In preparation for Transitioning-off the EIS contract, the government must have a complete and accurate Transition Inventory.

If GSA exercises all the contract options, for the final five (5) years of the EIS contract, CTI will conduct periodic validations (approximately once every 6 months) of its Transition Inventory with GSA and reconcile any discrepancies. If GSA exercises all the contract options, for the final three years of the EIS contract CTI will conduct monthly validations with GSA. At the GSA CO's request, CTI will deliver an inventory summary of all services active – that is, in service, whether in use or not – at the time of the request, by AB code, service, quantity, and location. At the OCO's request, CTI will deliver an inventory summary of all the agency's services active at the time of the request.

If GSA exercises all the EIS contract options, for the final three (3) years of the contract, CTI will deliver weekly reports of services disconnected and active services based upon the transition inventory.

During that same three-year period, CTI will deliver a monthly Transition Status Report that includes the following:

- Data file of invoiced amount by AB code for the most recently completed billing period
- Discussion of transition issues reported by agency customers or experienced by CTI either during the reporting period or unresolved since the last report, corrective action, and status
- Risk analysis and response plan

3.1.4.1.1 Transition Project Management [L.30.2.1 (4a); G.9.4 (4a)]

3.1.4.1.1.1 Transition Project Management Processes Unique for Transitioning onto EIS [L.30.2.1 (4a); G.9.4 (4a)]

CTI will assign staffing to form a strong, robust CTI Transition Team (CTT). [redacted]

[redacted]

As CTI Team is not presently an incumbent upon any EIS Task Order, should a transition occur from CTI Team to another Vendor, we will follow that Vendors written transition plan. In the event the incoming Vendor has no Transition Plan, CTI Team will follow the transition steps outlined within our own Transition Plan.

[redacted]

[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

[redacted]

[redacted]

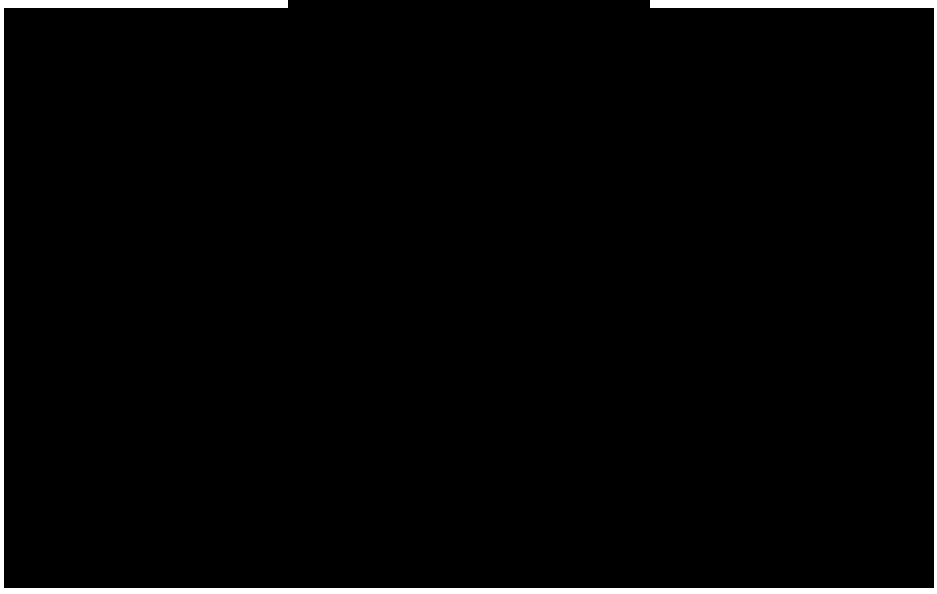
[redacted] CTI Team's BSS meets all

requirements, security stipulations and data exchange requires in this solicitation. Data produced by our BSS in the forms of data and or reports are human readable and are made available via the web interface. Data is also machine-readable – as part of the direct data exchange described in Section G.5.3.2 Direct Data Exchange of the GSA EIS solicitation. CTI Team BSS also meets web-interface and security requirements and provides complete insight into the financial and logistics requirements required to meet GSA EIS RFP stipulations.

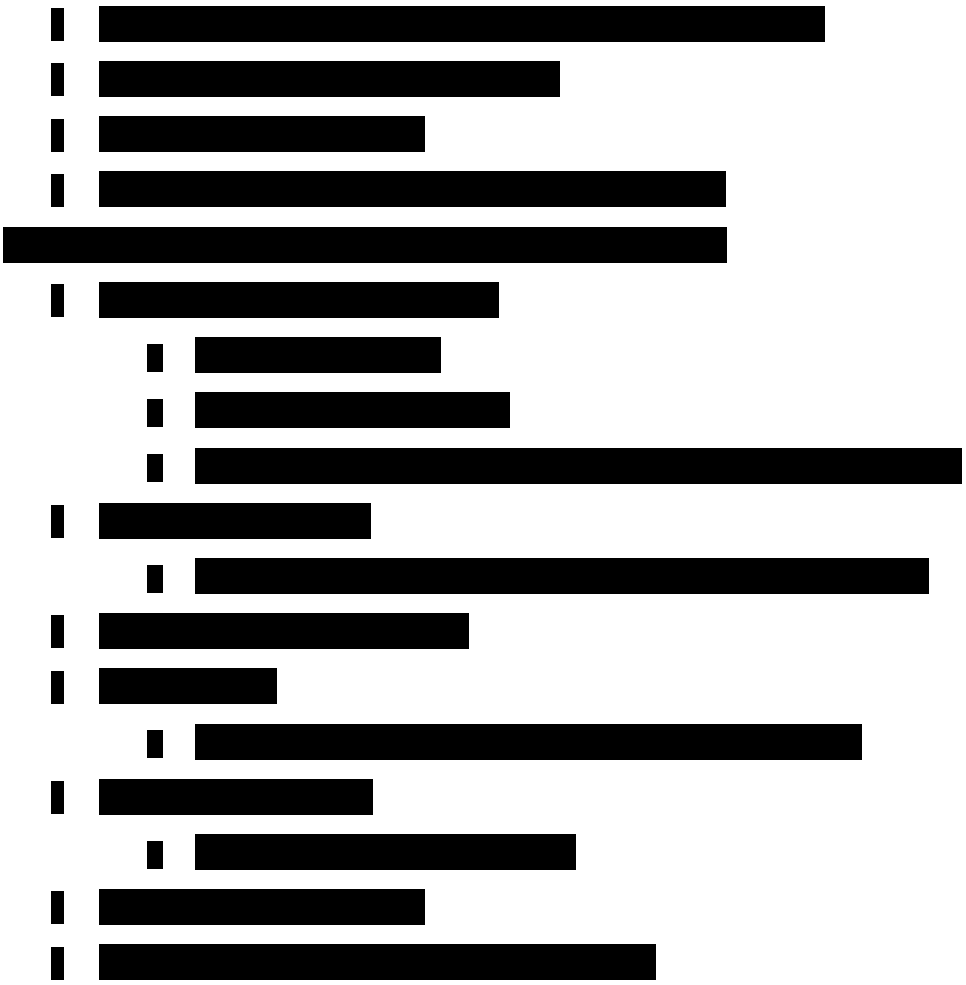
[redacted]

Web Services: Transactions over HTTPS via CTI Business to Business (B2B) Application Program Interfaces (APIs) for system-to-system data exchange between government and CTI systems. CTI will support XML over HTTPS using SOAP as the web services exchange mechanism. The transactions are bi-directional. CTI team understands that GSA Conexus will use X.509-based digital certificates to support mutual authentication and encryption, and HTTPS as the protocol for secure web services between CTI 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 CTI systems using government provided FTP service. The transactions will include transfer of data from the government to CTI and from CTI to the government.



Our [redacted] BSS meets all services requirements as noted in Section 2.4.10.6 [redacted]



[redacted]

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

CTI will tailor our BSS processes so that they apply to the transitioning of Agencies from Networx services (Transition-On) onto EIS and, when the contact is complete, the transitioning of Agencies off (Transition-Off) EIS to follow-on contracts.

Our approach to coordinating with other incumbent provides to ensure a smooth, successful, and timely transition is outlined in Section 2.4 .

3.1.4.1.1.2 Identify, Assess, Major Transition Risks and Propose a Response [L.30.2.1 (4a); G.9.4 (4a)]

CTI's Risk analyses and assessments address all aspects of a project, and include elements such as:

- Financial impact
- Schedule impact
- Quality impact

For each risk that we identify and assess, we will propose a mitigation response to each. Table 2.4.1.1-1 lists some

potential transition risks and our risk mitigation strategies. The following table lists the most obvious risks associated with new IDIQ awards.

3.1.4.1.2 Agency Solicitations [L.30.2.1 (4b); G.9.4 (4b)]

For each service, we will provide a list of features that are available. CTI will then work with Agency management personnel, to

rank each of the features as “mandatory”, “desirable”, or “not needed.” Based on this information, CTI will provide our recommendations for system enhancements that are available for the same price that we proposed on the Task Order or that will result in a nominal price increase for transition.

3.1.4.1.3 Customer Support during Transition [L.30.2.1 (4c); G.9.4 (4c)]

CTI Team will use our Task Order proposal response to identify, describe, and provide an outline for any handbooks useful to the Agency that is transitioning to EIS and make them available to clients immediately.Handbook information will include instructional information on assessing and using CTI’s on-line portal to access information , trouble shooting Aids , contact information and escalation proceedures.

3.1.4.1.4 Interconnection Plan [L.30.2.1 (4d); G.9.4(4d)] [RIN: MMR0013-KS]

[redacted]

[redacted] Some of the interconnections could include one or more of the following methods:

Cloud exchange or cloud connect is a variation on the virtual cross-connect service. Where an IX platform is facilitating the movement of data across the public internet, a cloud exchange is facilitating the connection of a party to a cloud service provider in a private, secure manner rather than via the public Internet. Like an IX, a single port enables access to multiple providers that are collocated in a carrier neutral datacenter.

Carrier hotels: A carrier hotel is also a colocation facility, but the name typically connotes a facility that has a very high concentration of networks, carriers and service providers. The term also reflects that fact that many of the famous carrier hotels are not single-purpose datacenters, but mixed-use buildings. They are often located in the heart of a city's business district, have office space rented to third parties, and weren't built specifically to house computer networks and servers.

Datacenter interconnection: The networking of two more or more datacenters for a common business purpose. The datacenters have a physical connection between at least two facilities, and are connected at a designated space within a building. Direct connections to cloud providers: A type of interconnection that connects a cloud service provider to a customer via a 'direct' connection, with connectivity provided by a carrier partner that links a customer with a fiber or other high-speed connection to the cloud provider's node at a datacenter facility. Examples include Amazon's Direct Connect or Microsoft's ExpressRoute.

IX providers: An IX provider is an entity that manages the infrastructure used by organizations such as carriers, ISPs, hosting companies and CDN service providers to exchange Internet traffic. Peering agreements form the basis for the exchange of traffic. Some IXs are operated as nonprofit, member-based associations. Characteristics of this type of provider include operating a peering fabric, and pricing services in line with the costs to provide the service to its members. The nonprofit IXs don't run or sell colocation services; instead, the peering fabric is installed in a facility managed by a third-party colocation provider – sometimes in multiple providers in a given region. In the US, a more common model is for the IX to be run as a for-profit service that is managed

by the colocation provider, which is of course also managing the facility and selling space along with the opportunity to participate in the IX peering fabric. The members of the IX in this case are customers of the colocation provider. The commercial IX model is the dominant model in the North American market, while the nonprofit, member-based IXs are more commonly found in Europe.

Physical cross-connect: A cross-connect is a means of physically patching (connecting) two customers together via a fiber-optic or copper cable at a patch panel. This initially was used to connect telecom networks together but now can connect ISPs, content providers, cloud providers or enterprise networks together. Virtual cross-connect: A virtual cross-connect is a service that allows a customer to connect to a single port to gain access to multiple other parties via a common switch. While a standard physical cross-connect has no electronics involved, being a physical connection of cables, a virtual cross-connect has a switch in the path; the switch is what enables customers to access a wider range of partners than would be physically possible (given space and power constraints) if they were to connect on a 1:1 basis with each partner.

3.1.4.1.4.1 Potential Impact to Customers' Operations [L.30.2.1 (4d); G.9.4(4d)]

CTI Team anticipates minimal impact, if any, to the customer's operations. Impacts, should they occur, may involve some level of network down time if no mirrors have been designed into the service architecture. [redacted]

3.1.4.1.5 Transition Contingency Plan [L30.2.1 (4e); G.9.4 (4e); C.3.1.2]

If unforeseen difficulties arise that result in loss of service, CTI Team will work through its service providers to activate backup services and or re-route lines/cables to working assets to ensure services remain operational as the Team works out the resolution to the main problem. Since the realm of potential possibilities (however minor) include acts of terrorism and physical destruction of it is difficult to fully describe how services will be restored except to say that CTI Team will use every asset at our disposal to restore

unforeseen lost services. Under normal conditions and normal levels of difficulty within CONUS services are normally restored by re-routing traffic over unaffected lines through whatever service carrier provides the best value and quality. Otherwise CTI Team will manage transition activities as described in our Program Management Plan.

3.1.4.2 Resource Plan [L.30.2.1 (5); G.9.4 (5)]

3.1.4.2.1 Financial Resources

CTI's approach to budgeting, tracking, and controlling costs is the continuous tracking and documentation costs and employing a variety of GAAP accounting and cost control techniques. [redacted]

The stability and robustness of our financial reporting system balances the positive and negative cost-driving factors to ensure the highest quality products, on schedule at the and at the lowest reasonable costs. [redacted]

3.1.4.2.2 Human Resources

[redacted]

[redacted]

All candidates must complete a CTI employment application during the initial interview. The interviewer receives a checklist of minimum qualifications for the labor category and a checklist of task specific requirements. Interviewers must ensure that all items on the checklists are covered. The interviewer must also ensure that cited experience applicable to each requirement is verifiable, for example, technical references are given.

In addition, candidates must provide several references, including names and phone numbers of previous supervisors. A potential candidate must provide a minimum of three references prior to further consideration. Our HR department verifies education and training information through the candidate's transcript of courses, or by a certified copy of the degree. Interviewers complete reference checks and candidate evaluation forms, reflecting the results of reference checks and the interviewer's evaluation of the candidate. Finally, we evaluate a candidate's evaluation form and reference check forms against all other forms and reference checks to determine the most qualified individual(s).

The meticulous verification of education, references, training, performance, dependability, and technical experience ensures the selection of only the most competent, highly skilled individuals

3.1.4.2.3 Equipment

Hardware asset management is the process of tracking and managing the physical components of computers and computer networks, from acquisition through disposal. The goals of hardware asset management are to account for all hardware assets on the infrastructure to provide a comprehensive view of the inventory. Moreover, asset management helps with contract and lease management, and assists in making budgetary forecasts based on the stock of assets and current / planned business requirements.

Software asset management is similar to hardware asset management but focuses on software assets, including licenses, versions, and installed endpoints. ITIL states that the goals of software asset management are to reduce IT costs and limit business, legal, and security risks related to the ownership and use of computer software, while maximizing IT responsiveness and end - user productivity.

[redacted]

[redacted]

3.1.4.3 Quality Control Program [L.30.2.1 (6); G.9.4 (6)]

[redacted]

[redacted]

CTI uses proven project management procedures that allow us to consistently succeed in the effective management of people, processes, and tools. It is these procedures that allow us to deliver high quality products and services that represent best value to our customers. [redacted]

[redacted]

[redacted]

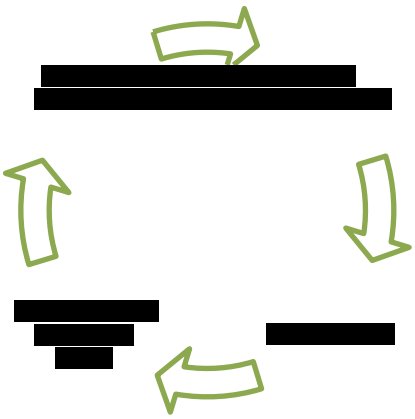
[redacted]

[redacted]

3.1.4.4 Key Personnel and Organizational Structure [L.30.2.1 (7); G.9.4 (7)]

3.1.4.4.1 The organizational structure and responsibilities for this effort is proposed as follows:

The GSA EIS Contracting Officer acts as the interface between the Customer or End User/Requestor of services and the GSA EIS IDIQ. [redacted]



3.1.4.4.2 Roles and Responsibilities of key Individuals [L.30.2.1 (7); G.9.4 (7); H.10]

3.1.4.4.3 Substitutions and Additions of CTI Key Personnel [L.30.2.1 (7); G.9.4 (7); H.10.2]

CTI Team will ensue that resumes for substitutions and/or additions to CTI's key personnel will be submitted for the written approval of the GSA CO. CTI Team understands that during the first 180 days of contract performance, no key personnel substitutions will be permitted unless such substitutions are due to illness, injury, death, disciplinary action, demotion, bona-fide promotion, termination of employment, or other exceptional circumstances when approved by the GSA CO. CTI will promptly notify the GSA CO and provide the information required by the solicitation. After the initial 180-day period, all proposed substitutions and additions of key personnel will be submitted to the GSA CO in writing 15 days (30 days if security clearance is to be obtained) prior to our anticipated effective date of the proposed substitutions and additions. CTI will provide a detailed explanation of the circumstances requiring the proposed substitution or addition. CTI will certify that the proposed replacement is better qualified than, or at least equal to, the key personnel to be replaced, subject to the penalties in 18 USC

1001. The GSA CO or the GSA CO's authorized representative will evaluate such requests and promptly notify CTI of the approval or disapproval thereof.

3.1.4.4.4 Organizational Structure [H.10.3]

The organizational structure below represents the direct relationships and partnering relationships between CTI, the GSA EIS CO/PMO. [redacted]

[redacted]

[redacted]

3.1.4.5 Risk Management Plan [L.30.2.1 (8); G.9.4 (8)] [RIN: MMC0004-DI]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]	
[redacted]	
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	
[redacted]	

[redacted]	
[redacted]	
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

3.1.4.6 Information Systems [L.30.2.1 (9); G.9.4 (9); G.5]

See BSS in this Management Volume Section 2.1.6

3.1.4.6.1 Business Support Systems (BSS) Description [L.30.2.1 (9); G.9.4 (9); G.5.1]

See BSS in this Management Volume Section 2.1.6.1

3.1.4.6.2 Availability of Systems to Meet BSS Technical Requirements [G.5.3]

See BSS in this Management Volume Section 2.1.6.2

3.1.4.6.2.1 Web Interface [G.5.3.1]

See BSS in this Management Volume Section 2.1.6.2.1

3.1.4.6.2.1.1 Web Interface Functions [G.5.3.1.1]

See BSS in this Management Volume Section 2.1.6.2.1.1

3.1.4.6.2.1.2 Technology Standards [G.5.3.1.2]

See BSS in this Management Volume Section 2.1.6.2.1.2

3.1.4.6.2.1.3 Accessibility [G.5.3.1.3]

See BSS in this Management Volume Section 2.1.6.2.1.3, CTI team will comply with all requirements in this section to include making the BSS Voluntary Product Accessibility Template (VPAT) available on our website, www.coretechinc.com.

3.1.4.6.2.2 Direct Data Exchange [G.5.3.2]

See BSS in this Management Volume Section 2.1.6.2.2

3.1.4.6.2.2.1 Direct Data Exchange Methods [G.5.3.2.1]

See BSS in this Management Volume Section 2.1.6.2.2.1

3.1.4.6.2.2.2 Direct Data Exchange Formats [G.5.3.2.2]

CTI Team's BSS will accept data transfers from the government and will submit data to the government in formats specified.

3.1.4.6.2.2.3 Direct Data Exchange Governance [G.5.3.2.3]

CTI Team understands that 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 CTI Team.

Once the BSS is operational, CTI Team will not make any changes to the data exchange formats or methods without government approval via the established change control process.

3.1.4.6.2.3 Role Based Access Control (RBAC) [G.5.3.3]

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

3.1.4.6.2.4 Data Detail Level [G.5.3.4]

See BSS in this Management Volume Section 2.1.6.2.4

3.1.4.6.3 Systems Availability to Meet BSS Service Requirements [G.5.4; G.5.4.1]

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 Tracking	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

3.1.5 BSS DEVELOPMENT AND IMPLEMENTATION PLAN (G.5.5) [RIN:]

[redacted]

CTI understands that the government will not pay for or otherwise finance the development or maintenance of the BSS, however that shall not be necessary even if it were allowed as the BSS is part of the normal operating expenses of CTI. As an internal CTI expense as part of our operating overhead, CTI is solely responsible for all development, testing, and maintenance including, but not limited to, security validation, functional testing, and configuration control. Thus CTI can provide upgrades to its BSS at no additional cost to the government, as these upgrades become available to our commercial customers. BSS functional testing requirements and BSS security testing requirements are defined in Section G of the GSA EIS Solicitation.

[redacted]

3.1.5.1 Complete Billing and Customer Lifecycle Control

[redacted]

[redacted]

3.1.5.2 Advanced Billing Features

[redacted]

3.1.5.3 Sales Manager

[redacted]

3.1.5.4 Order Manager

[redacted]

3.1.5.5 Device Manager

[redacted]

[redacted]

3.1.5.6 Special Device Module Framework Features

[redacted]

3.1.5.7 Support Manager

[redacted]

3.1.5.8 Reports Manager

[redacted]

3.1.5.9 Client Portal

[redacted]

[redacted]

[redacted]

3.1.5.10 Integrations

[redacted]

3.1.5.11 API

[redacted]

3.2 SUPPLY CHAIN RISK MANAGEMENT (SCRM) PLAN: [L.30.2.2; G.6.3] [RIN: MMC0003-DI, MMC0011-DI]

Background:

Information and communications technology (ICT) supply chain is a complex, globally distributed, and interconnected ecosystem that is long, has geographically diverse routes and consists of multiple tiers of outsourcing. This ecosystem includes public and private sector entities that depend upon each other to develop, integrate, and use ICT products and services. The ecosystem has evolved to provide a set of highly refined, cost-effective, reusable ICT solutions, either commercially licensable, open source, or delivered as services.

Federal government information systems have rapidly adopted this ecosystem of solution options, which increased their reliance on commercially available (commercial off-the-shelf [COTS] or open source) products, system integrator support for custom-built systems, and external service providers. This resulted in increased complexity, diversity, and scale of the federal government's ICT supply chains. COTS products are developed by a globalized ecosystem of vendors for a global base of public and private sector customers. This globalized ecosystem of vendors affords significant benefits to its customers, including low cost, interoperability, rapid innovation, a variety of product features, and choice among competing vendors. However, the same globalization that creates these benefits enables increased opportunities for adversaries (individuals, organizations, or nation- states) to directly or indirectly affect the management or operations of companies, in a manner that may result in risks to the end user. Currently, federal agencies, and many private sector integrators and suppliers use varied and nonstandard practices, which makes it difficult to consistently measure and manage ICT supply chain risks across different organizations.

ICT Supply Chain Risk Management (SCRM) is the process of identifying, assessing, and mitigating the risks associated with the global and distributed nature of ICT product and service supply chains. ICT encompasses activities in the system development life cycle, including research and development (R&D), design, manufacturing, acquisition, delivery, integration, operations, and disposal/retirement of an organization's ICT products (i.e., hardware and software) and services.

CTI SCRM Plan Approach:

[redacted]

Managing ICT supply chain risk requires ensuring the integrity, security, and resilience of the supply chain and its products and services thus addressing the issue of counterfeit and illegally modified products. [redacted]

CTI also employs the following strategies and tactics to support its SCRM plan and mitigate risks around illegal and counterfeit parts:

Use of Risk Assessment Checklists –

Use of Security Policies – [redacted]

Organization of Information Security – [redacted]

Asset Management– [redacted]

Human Resources Security– [redacted]

Physical and Environmental Security-– [redacted]

[redacted]

Communications and Operations Management– [redacted]

[redacted]

Information Systems Acquisition, Development and Maintenance – [redacted]

[redacted]

[redacted]

Information Security Incident Management and Operations Security – [redacted]

[redacted]

CTI shall comply with NIST SP 800-161 Supply Chain Risk Management (SCRM) Practices and will update its SCRM Plan to include any future changes to the NIST SCRM Guidelines with all such modifications to the Plan made at no cost to the government.

The SCRM plan to manage supply chain risk throughout each of the following supply chain phases:

3.2.1 SUPPLY CHAIN PHASES [L.30.2.2]

3.2.1.1 1) Design and Engineering [RIN: MMC0005-DI]

Design and engineering perform activities in various contexts. This includes support to field users, operational headquarters, acquisition agencies and program offices, policy and oversight organizations, as well as independent efforts of all forms (e.g., red teams,

blue teams) across a range of collaborating stakeholders. They plan and technically manage engineering efforts, and sometimes those of others, for projects and programs throughout the system life cycle.

In the design and engineering requirements process our entire CTI team scrutinizes current activity and prioritizes areas that need attention such as:

- **Corporate Risk Team**, [redacted]
- **Supplier Management Team**, [redacted]

[redacted]

[redacted]

3.2.1.2 2) Manufacturing and Assembly [RIN: MMC0006-DI]

[redacted] Suppliers are also subject to regular audits.

3.2.1.3 3) Distribution and Warehousing [MMC0007-DI]

When CTI controls the shipment, it uses specific carriers who agree to specific carrying requirements and CTI tracks and monitors shipments to their destination. One key concern is what happens when customers select their own carrier to move the products.

[redacted]

[redacted]

- **Distribution and Warehousing Audits**: [redacted]

Distribution and Warehousing Standards: [redacted]

[redacted]

3.2.1.4 4) Operations and Support [RIN: MMC0008-DI]

[redacted]

All of CTI's functions that touch our supply chain are linked through our Supply Chain Risk Management Council which meets on a regular basis to review risk exposure. [redacted]

3.2.1.5 5) Disposal and Return [RIN: MMC0009-DI]

Lifecycle Approach Including Disposal and Return: CTI uses an integrated systems process in its approach to green lifecycle design. [redacted]

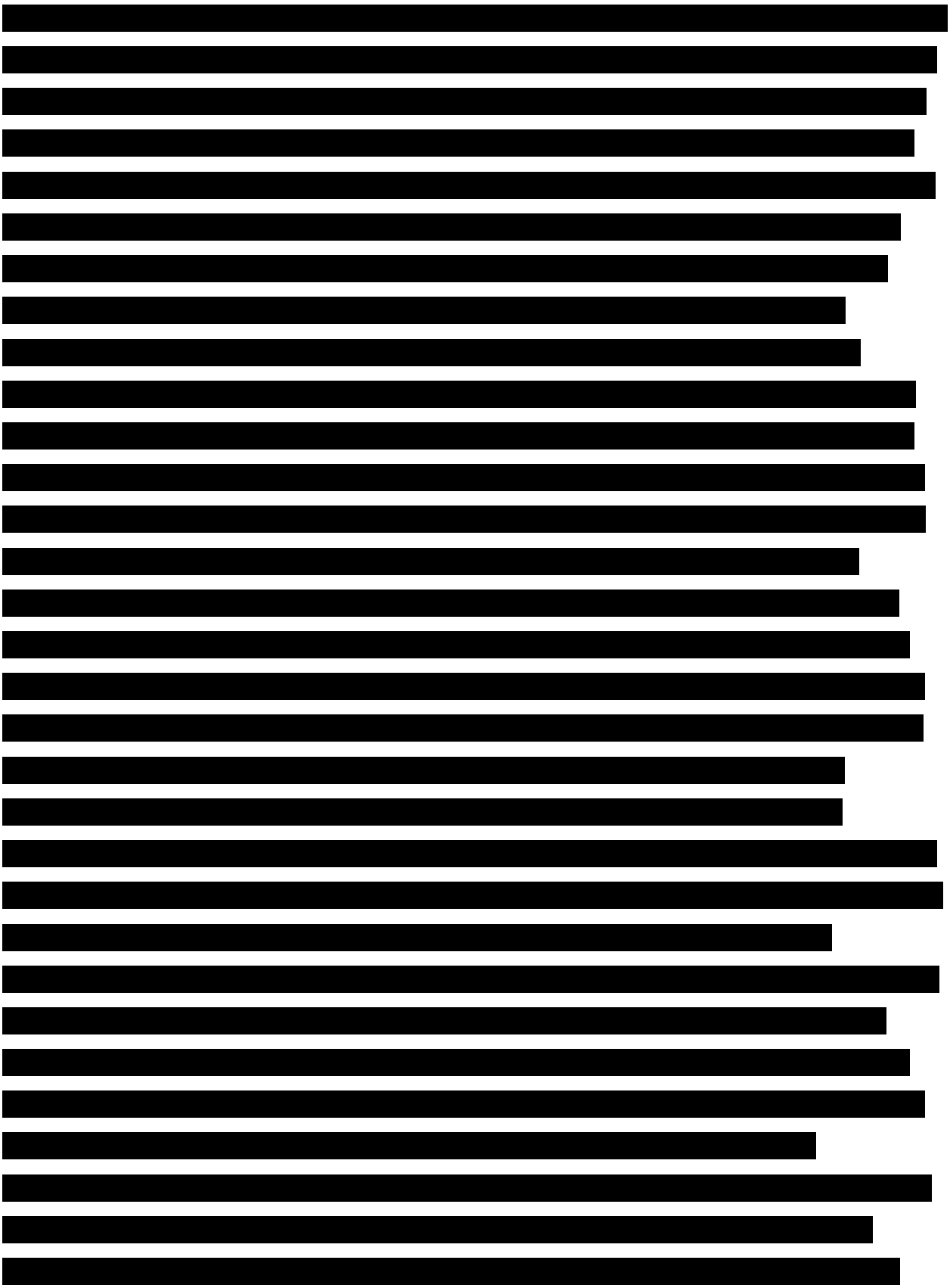
[redacted]

3.2.2 SCRM PLAN COMPONENTS & SUPPORTING INFRASTRUCTURE [RIN: MMC0019-DI, MMC0010-DI]

Since the substance of this provision is part of all subcontracts then the SCRM plans of all of our subcontractors and the policies and provisions they have in place to prevent the use or acquisition of counterfeit and/or illegal parts are part of the supporting infrastructure beyond the system boundary of what CTI can directly affect and are integral to CTI's SCRM Plan. [redacted]

CTI's SCRM plan shall address the following:

3.2.2.1 (1) Imposing Genuine Information Technology Tools (ITT) [L.30.2.2(1); G.6.3(1)]



[redacted]

3.2.2.1.1 (1a.) Ensuring SCRM Plan is Performed for ITT [L.30.2.2 (1a); G.6.3 (1a)]

CTI performs reasonable steps to ensure its SCRM Plan is performed for ITT in its delivered and installed configuration by:

- **Require completion of appropriate CTI Team SCRM questionnaire:** [redacted]
- **Perform continuous integrator review:** [redacted]

3.2.2.1.2 (1b.) CTI's Equipment Resellers with Valid OEM Licenses [L.30.2.2(1b); G.6.3(1b)]

[redacted]

3.2.2.1.3 (1c.) Quality Control Ensuring OEM Products Exclude Counterfeit Components [L.30.2.2(1c); G.6.3(1c)]

[redacted] CTI's definition of Counterfeit Products is any equipment hardware or software component that is not genuine because it:

Does not have a Certificate of Authenticity (COA) so that customers can identify software such as genuine Microsoft Windows software (for example).

- Does not conform to original OEM design, model, and/or performance standards because of a lack of a certification from a standards organization such as a COA, ISO or other standards authority, or from an international or industry organization such as IEEE, UL, CE, PSE, TIY, SAFETY Mark, or other industry standard mark/seal for the specific product.
- Is not produced by the OEM or contains parts from countries known to be a non OEM supplier to an OEM integrator, or is produced by unauthorized contractors or is not specified within a published catalog available to industry members.
- Is an off-specification, defective, or used OEM product sold as "new" that may be on a list of known counterfeit products as published by the US Government.
- Has incorrect or false markings and/or documentation or is visibly damaged, in incorrect packaging, is obviously defective in terms of appearance or manufacture, or does not pass acceptance testing by CTI.
- Is from a supplier that has not filled out a supplier questionnaire in accordance with the CTI SCRM Plan.

[redacted]

3.2.2.1.4 (1d.) Ensure Traceability of ITT Genuineness [L.30.2.2(1d); G.6.3(1d)]

As part of CTI's SCRM Plan, we require that each OEM product and component that is delivered comes accompanied with an original part certificate directly from the OEM and its warranty label. If either document is not available, an official certification from the licensed distributor is requested.

3.2.2.2 (2.) System Security Engineering Processes to Protect against Threats [L.30.2.2(2); G.6.3(2)]

CTI utilizes disciplined, structured, systems security engineering (SSE) processes and controls that consist of a combination of systems engineering principles with security architecture best practices in specifying and designing a system that is protected against external threats and against hardware and software vulnerabilities. These processes and controls focus on security requirements, secure system architectures, strict configuration management processes, information assurance processes, and technology controls. [redacted]

3.2.2.3 (3.) Strategy for Implementing SCRM Security Requirements [L.30.2.2(3); G.6.3(3)]

The supplier to CTI is required to fill out a Threat Risk Identification and Risk Mitigation questionnaire from the CTI SCRM Plan. [redacted]

[redacted]

3.2.2.4 (4.) Criticality Analysis Process [L.30.2.2(4); G.6.3(4)]

CTI's criticality analysis (CA) process involves completing the Risk Assessment within the SCRM Plan for the particular product or service, identifying mission critical functions and the mitigation solutions that will be used to provide the counter-measure and sub-countermeasure used to achieve system protection and mission effectiveness. [redacted]

3.2.2.5 (5.) Ensure Products/Components are not Repaired then Shipped as New [L.30.2.2(5); G.6.3(5)]

CTI's subcontractors and suppliers are prohibited from conducting repairs on products and/or components then shipping them as new, or receiving repaired products that are

labeled as new. [redacted]

3.2.2.6 (6.) Ensure Supply Channels are Monitored for Counterfeit Products [L.30.2.2(6); G.6.3(5)]

[redacted]

3.2.2.7 (7.) How Physical and Logical Delivery Mechanisms are Protected [L.30.2.2(7); G.6.3(7)]

CTI uses national and international delivery services to ship products. [redacted]

[redacted]

3.2.2.8 (8.) How CTI's Operational and Disposal Processes Limit Data/System Compromise [L.30.2.2(8); G.6.3(8)]

[redacted]

3.2.2.9 (9.) Relationships between CTI and Manufacturers [L.30.2.2(9); G.6.3(9)]

[redacted]

3.2.2.10 (10.) CTI's Standard Commercial COTS Warranties [L.30.2.2(10); G.6.3(10)] [RIN: MMC0013-DI]

CTI's standard warranty for software is the OEM's standard or extended warranty that expresses that the software shall be free from all computer viruses, worms, 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 for Commercial-Off-the-Shelf (COTS) components consistent with clause 52.246.17. In the case of standard commercial warranties that exceed one year, CTI will ensure the government receives the additional term(s) of the commercial warranty.

3.2.2.11 (11.) Ensuring IV&V of Assurances and Supporting Information [L.30.2.2(11); G.6.3(11)] [RIN: MMC0014-DI]

CTI provides independent verification and validation of assurances, and will provide supporting evidence as required to government customers for our suppliers.

3.2.3 INCORPORATING SCRM PROVISIONS INTO SUBCONTRACTS [L.30.2.2; G.6.3] [RIN: MMC0012-DI, MMR0008-DN]

The substance of this clause is incorporated in subcontracts at all tiers where a subcontractor provides personnel, components, or processes identified as 1) a critical component, or 2) part of CTI's supporting infrastructure. [redacted]

3.2.4 COMPLY WITH NIST SP 500-161 SCRM PRACTICES [L.30.2.2; G.6.3] [RIN: MMC0015-DI, MMC0016-DI]

CTI will comply with NIST SP 800-161 Supply Chain Risk Management practices and has included the practices within our SCRM Plan as noted within this document. CTI will update the SCRM plan to include any future changes to the NIST SCRM Guidelines and all such modifications will be made at no cost to the government.

3.2.4.1 Plan Submittal and Review [G.6.3.1]

This plan is submitted with our proposal. Updates will be submitted on an annual basis or as required to ensure good business practices are followed at no cost to the government.

3.3 DRAFT BSS VERIFICATION TEST PLAN (L.30.2.3, E.2.1)

As a general description, CTI's BSS testing will be in accordance with our BSS Verification Test Plan. The BSS Verification Test Plan as outlined in the sections below will verify that all BSS functional, regression, load, and security requirements have been successfully met. Our testing will be performed for all management and operation functions supporting the Ordering, Billing, Inventory Management, Disputes, SLA Management and Trouble Ticketing processes that are described in GSA EIS RFP Sections G.3 – G.8 and Sections J.2.2 – J.2.10. Our security testing will be based on functional requirements described in Section G.5.6. BSS Security Requirements. The security requirements' acceptance will be based on evaluation for completeness for the ATO certification and FedRAMP certification and in accordance with the testing methodology. Our testing includes multiple test cases that are defined in Section E.2.1.3 Test Cases and the BSS will include use cases for quality, utility and customer access features.

CTI will provide a draft BSS Verification Test Plan (BSS Test Plan) with its proposal and a final BSS Test Plan 30 days after notice to proceed. This plan will comply with the test methodology for BSS defined in Sections E.2.1.1 – E.2.1.5. CTI understands that the government reserves 21 days from the date of receipt of final plan to accept or reject the plan. If it is rejected, CTI will be given the opportunity to update the plan based on government comments.

Based on GSA Conexus readiness and other factors, CTI understands that the government may, at its option, offer the opportunity for contractors to perform preliminary testing prior to award, but after submission of proposals. We understand that if this opportunity is offered, it will be offered to all contractors who submit a proposal, pending only CTI's demonstration of primary security features such as anti-virus protection. Any such preliminary testing will not replace formal testing post-award. The government offers no guarantees that the GSA Conexus configuration offered as the preliminary system will be identical to the final system used in post-award formal testing. If the government offers such preliminary testing, the government will issue terms and conditions for such testing which CTI must accept prior to accessing the test system.

CTI will provide updates to the BSS Test Plan within fourteen (14) days of receipt of government comments. The government reserves fourteen (14) days after receipt of the updated plan to accept or reject it. If necessary to gain approval, CTI may repeat this process.

3.3.1 SCOPE [E.2.1.1]

CTI will ensure the entire scope of the government's requirements is met by accomplishing the following:

- The BSS testing will verify that all BSS functional, regression, load, and security requirements have been successfully met.
- The BSS testing will be performed for all management and operation functions supporting Ordering, Billing, Inventory Management, Disputes, SLA Management and Trouble Ticketing processes that are described in Sections G.3 – G.8 and Sections J.2.2 – J.2.10 of the GSA EIS RFP.
- Security testing will be based on functional requirements described in Section G.5.6 BSS Security Requirements. The security requirements acceptance will be based on evaluation for completeness that is for the ATO certification and FedRAMP compliance, if applicable.
- The testing will include multiple test cases that are defined in Section E.2.1.3. Test Cases.
- The BSS testing will include Use Cases for quality, utility and customer access features.
- CTI will allow government representative(s) to observe all or any part of the verification testing.
    - If the government so requests, CTI will perform tests to ensure continued compliance each time a new service is offered or we modify features/functionality of the BSS that affect the functional requirements described in Sections G.3 – G.9.
    - If the government requests this retest, CTI will provide a BSS Verification Test Results report, including analysis, within seven (7) days after performance of the tests. CTI understands that the government reserves fourteen (14) days to accept or reject the test results, in part or in whole. If

the government rejects the test results, CTI shall retest until such time the results are acceptable to the government.

- CTI will perform BSS verification testing according to the accepted BSS Test Plan at a mutually acceptable date with the government.

EIS Verification testing follows the same testing protocols as the overall BSS Test Plan, meaning that test tables will be followed, and all reports and errors generated will be given to the government and retesting done until all tests are passed to the government and CTI's satisfaction.

3.3.2 BSS TEST SCENARIOS (E.2.1.2)

3.3.2.1 Testing Prerequisites (E.2.1.2.1) [RIN: MMR0029-DN]

Prior to initiating BSS testing, CTI will:

Provide written notice to the government that CTI's BSS has passed its internal testing and is ready to begin BSS interface testing with GSA Conexus.

Provide a finalized BSS Test Plan that is accepted by GSA.

The purpose of the verification and acceptance testing is to ensure that CTI's BSS meets requirements in Section G and Section J.2. CTI will support BSS security and functional testing as defined in Section G.5.6 BSS Security Requirements and Section G.2.3 BSS Final Contract Acceptance.

3.3.2.2 Test Scenarios (E.2.1.2.2)

The following table contains a high-level list of BSS Test Scenarios for which CTI's BSS must pass the defined acceptance criteria. CTI will address the test scenarios based on the functional requirements defined in the relevant portions of Section G and/or Section J.2 (see the "RFP References" column for references).

The scenarios will address relevant data exchange mechanisms and validation of data exchanged. [redacted]

[redacted]	[redacted]		
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]	[redacted]	[redacted]	[redacted]
			[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

3.3.3 BSS TEST CASES (E.2.1.3)

CTI will accept, incorporate into the BSS Test Plan, and successfully execute test cases provided for each of the test scenarios above.

CTI will accept the following test conditions:

- No testing between CTI and GSA will occur until CTI's BSS and GSA Conexus have both passed unit testing.
- All testing to be performed on the actual system to be used in delivering service (i.e. special purpose "test systems" will not be used).
- Unless otherwise specified, all data transfers are to use the mechanism specified in Section J.2 for that data set.

CTI will use GSA provided test data for all BSS verification testing unless otherwise specified:

- This data will be used for testing purposes only.
- No customer "live" data will be used for testing.
- This data will be a realistic simulation of actual customer data.
- The test data will include, in some tests, intentional errors intended to test CTI's BSS error handling.

BSS testing will follow a tiered approach:

- CTI will accept multiple test cases for the test scenarios defined in Section E.2.1.2.
- CTI will accept, incorporate into the BSS Test Plan, and successfully execute each test case with one or more test data sets.
- In providing test data sets, GSA will group them into Test Subcases:
  - Each Test Subcase will contain data sets intended to test a specific "real world" test case (e.g. a complete and accurate disconnect order).
  - Each test subcase will include at least two complete test data sets.

BSS functional testing acceptance:

- CTI's BSS will not have completed functional testing until all BSS Test Scenarios (Section 3.3) are passed.
- A test scenario will not be considered passed until CTI's BSS properly handles each associated test case.
- A test case will not be considered passed until CTI's BSS properly handles each associated subcase twice in succession using different data sets.

- A subcase will not be considered passed until CTI's BSS properly handles the data sets following the prescribed actions with no errors or warnings.

BSS security testing acceptance is defined in Section G.5.6 and associated references.

The individual test cases are defined in the tables in the subsections below. Each test case table includes the following headings:

Test Scenario: The associated test scenario from Section E.2.1.2.

Test Case ID: Identification number for the test case.

Test Case Description: Brief title of the test case.

Requirements Reference(s): Where the functional requirements that are being tested can be found.

Prerequisites: Actions that must be completed prior to implementing the test case (in addition to the general prerequisites for all testing).

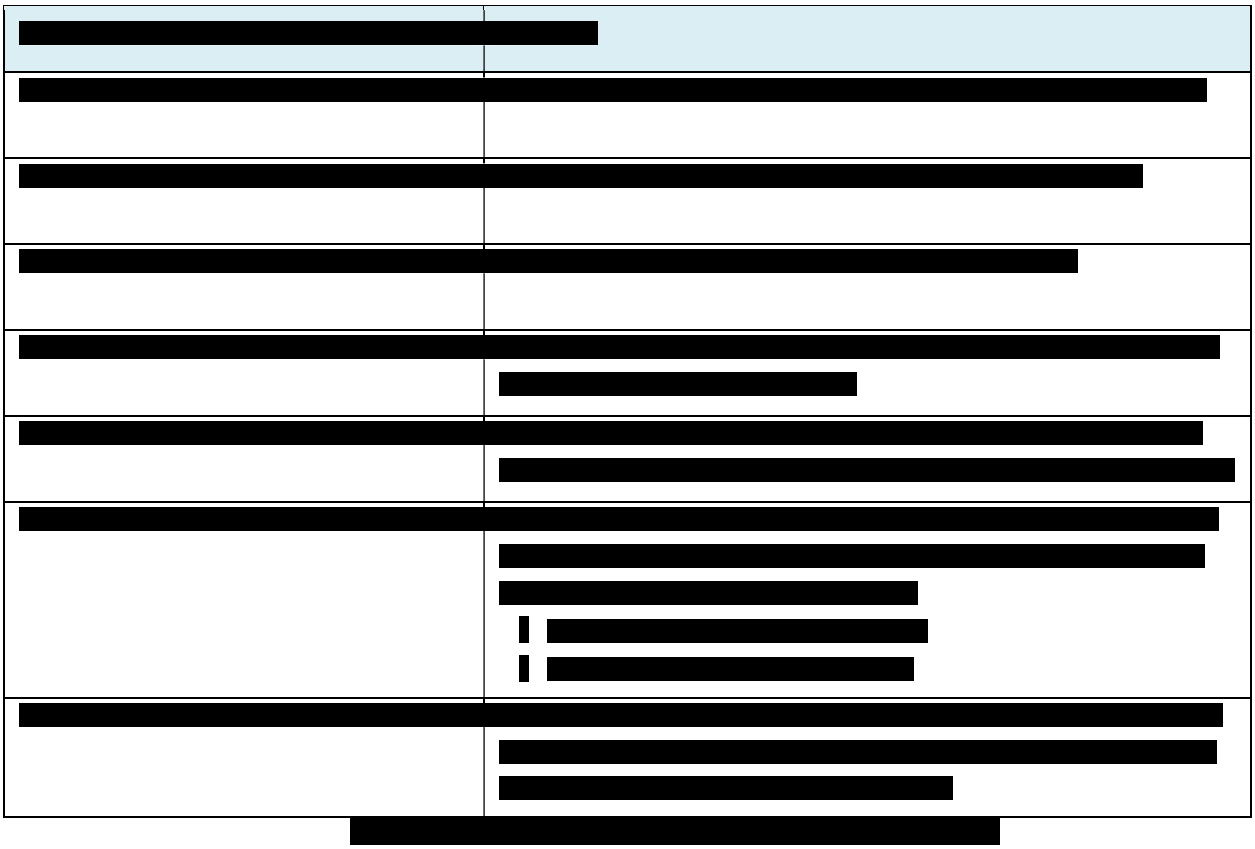
Government Input(s): Data the government will provide as input to the test case.

Expected BSS Output(s): Expected data or actions from CTI's BSS.

Data Set Description: Brief description of the data sets the government intends to provide as part of testing.

Acceptance Criteria: Factors to be checked prior to acceptance of the test results.

The table below defines the terms used:



3.3.4 TEST RESULTS (E.2.1.4) [RIN: MMR0027-DN]

CTI will demonstrate that we successfully meet the BSS acceptance criteria for the various test scenarios/test cases and that CTI will provide test results that show details of testing the following:

- Functional requirements for the Ordering, Billing, Inventory Management, Disputes, SLA Management and trouble ticketing processes as described in Sections G.3 – G.9.
- System to system data exchange mechanism requirements defined in Section G.5 for each CDRLs defined in Section J.2.
- Correct CDRLs are used in the data exchange.
- Mandatory data elements for each CDRL defined in Section J.2.10 Data Dictionary are populated and accurate.
- Available optional data elements for each CDRL defined in Section J.2.10 Data Dictionary are populated and accurate.

- Timely and successful system to system data exchange to meet defined performance SLAs and provisioning intervals.
- Load testing performance for concurrent data exchange through SFTP.
- Load testing performance for concurrent data exchange through web services.
- The test results will detail at a minimum the following:
    - Test scenario # / Test case # / Test Data Set # / Test #; Date of Test performed, Acceptance Criteria, Test Result (Pass/Fail), etc.

3.3.5 DELIVERABLES (E.2.1.5)

CTI will deliver a final BSS Test Plan IAW the specifications outlined within the GSA EIS RFP. This includes applicable services Verification Test Plans and CTI will deliver Test Results to be incorporated by the government into its final accreditation process for BSS. The final BSS Test Plan will include the test methodologies as defined in the RFP and CTI acknowledges that it will successfully complete verification testing prior to accepting orders from the government. CTI will also successfully complete verification testing for accepted changes to the CDRLs / data exchange mechanisms acceptance criteria during the life of the contract.

3.3.5.1 Verification Test Plan for Contractor's BSS (E.2.1.5.1) [RIN: MMR0001-DN]

CTI will submit a BSS Verification Test Plan (BSS Test Plan) based on the following timeline:

Draft: with proposal

Final: 30 days after NTP

Revisions: 14 days after receipt of government comments

The BSS Test Plan will:

Reflect the test methodology defined in Section 3.3.

Include CTI's approach to testing each test scenario and test case

Include CTI's timeline and test sequencing

CTI has developed a test schedule ensure that our BSS meets the standards set forth in G.5.4. The testing schedule will comprise of all of the components of the BSS shown below:

[redacted]

Note 1: This is a sample test schedule to demonstrate the activities and milestones to be planned. Actual test schedule dates will be applied and revisions to the schedule may occur

3.3.5.2 Verification Test Results Report for Contractor's BSS (E.2.1.5.2)

CTI will provide a BSS Verification Test Results Report that includes analysis of the current testing and a summary table of all previously submitted test results, within seven (7) days after performance of the tests. The government reserves fourteen (14) days to accept or reject the test results, in part or in whole.

CTI will perform re-test of test cases with test data sets that failed until they are accepted by the government.

CTI will rerun tests, in part or in whole, as deemed necessary by the government, to verify that the government's comments on the test results are satisfactorily addressed.

3.4 EIS SERVICES VERIFICATION TEST PLAN (L.30.2.4, E.2.2) [RIN:]

CTI will provide an EIS Services Verification Test Plan (EIS Test Plan) based on the test methodology defined in Section E.2.2.1 – E.2.2.5 (test scenarios, test cases, test data sets, acceptance criteria) of the GSA EIS Solicitation in response to the RFP for each of the proposed EIS services. The EIS Services Verification Testing follows the BSS verification testing described above since ordering is accomplished via the BSS for EIS services and is used to ensure the EIS Services can be adequately ordered, delivered and billed to the government.

3.4.1 GENERAL TESTING REQUIREMENTS (E.2.2.1) [RIN:]

CTI will meet the following EIS Services testing requirements:

- CTI shall provide a verification and acceptance testing approach for all awarded EIS services defined in Section C.2 of the GSA EIS Solicitation.
- CTI shall develop an EIS Test Plan that includes, but is not limited to:
    - The test methodology for each EIS Service with test cases that will define the parameters to be measured, the measurement procedure, and the acceptance (pass/fail) criteria.
    - Fallback approach to describe the fallback process and procedures in case of testing failure.
    - An EIS Test Plan will be required for all new services during the life of the contract.

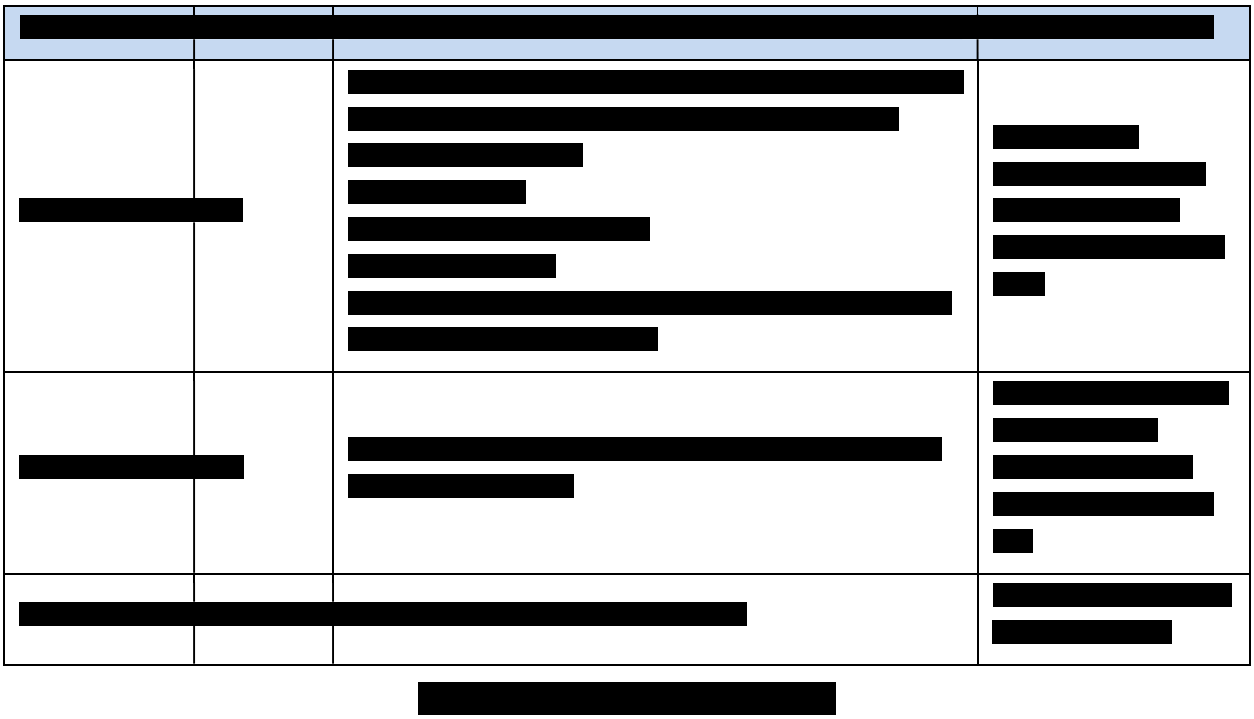
The following conditions also apply:

- An agency may define additional testing in the TO.
- CTI will allow government representative(s) to observe all or any part of the EIS services verification testing.
- CTI will provide all necessary test equipment: data terminals, load boxes, test cables, and any other hardware and software required for testing.

3.4.2 TEST SCENARIOS (E.2.2.2)

CTI's EIS Test Plan will include, but not be limited to, the following test scenarios:

3.4.2.1 EIS Services Verification Test Scenarios (E.2.2.2.1)



3.4.3 TEST CASES (E.2.2.3)

CTI will provide test cases for each of the test scenarios defined in Section E.2.2.2. The test cases will be defined in the EIS Test Plan.

3.4.4 TEST DATA SETS (E.2.2.4)

CTI will successfully test all of the test cases defined in the EIS Test Plan using one or more test data sets proposed by CTI. CTI will test all services and service features proposed at the TO. CTI will use test data sets that reflect real-world service conditions and locations, and will address all relevant test cases.

3.4.5 TEST RESULTS AND ACCEPTANCE (E.2.2.5)

CTI will provide an EIS Services Verification Testing Report (EIS Testing Report) that shows successful completion of testing defined in the EIS Test Plan. CTI will complete verification and acceptance testing based on the acceptance criteria defined in the government accepted EIS Test Plan. Acceptance will include government compliance requirements, such as FedRAMP for cloud services, and the ATO for FISMA related security requirements for EIS services. CTI will provide the following in order for the government to approve the test results:

- FedRAMP certification if cloud services are included in the TO.

- EIS Testing Report showing that each service provisioned works properly according to the KPIs defined in Section C.2 and the acceptance criteria defined in the EIS Test Plan.

Once verification testing is successfully completed, the government may complete acceptance testing based on the acceptance criteria defined in the EIS Test Plan. The acceptance test will verify satisfactory end-to-end service performance and proper operation of all ordered features and functions. Performance will be considered satisfactory when services, equipment, systems, and their associated features and functions perform as specified in the contract and TO. CTI may not assign an effective billing date to an EIS Service until the agency accepts it in accordance with the agreed-upon acceptance testing procedures described in the EIS Test Plan.

The government reserves the right to perform additional tests to confirm proper operation of a delivered EIS service as defined by the TO. If the government does not report a problem to CTI during this test period, the effective billing date will be the completion date on the SOCN. CTI will 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. CTI will issue a new SOCN for services after correcting the reasons for rejection.

The service will be considered accepted if the government does not reject the service within the acceptance period defined above. If the government rejects the service, it may at its option:

1. Direct CTI to repeat the procedure outlined above;
2. Withdraw the service from acceptance testing;
3. Direct CTI to facilitate the return of the services to their original provider (for services transitioned or migrated from another contractor’s network);
4. Request a replacement of the service (in whole or in part); or
5. Cancel the service order without penalty.

If the government exercises any of these options as a consequence of unacceptable acceptance testing results, all expenses incurred by the government will be borne by CTI.

If the government elects option 1 above, CTI will immediately initiate corrective actions to remedy the problem reported on the trouble ticket, and will keep the government informed of progress. In such cases, the government reserves the right to exercise option 2, 3, 4 or 5 at any time.

If the government elects any of the options above other than option 1, all expenses incurred by the government, including recurring charges and non-recurring charges (NRC) to return services to the previous network configuration, will be borne by CTI. In cases when the government cannot successfully complete acceptance testing due to circumstances beyond the control of CTI, CTI will notify government of the details surrounding the deficiencies and of the steps CTI has taken to overcome the deficiencies.

These cases will be discussed between the government and CTI. On a case-by-case basis, the GSA CO or the OCO may choose to waive the acceptance testing or extend the testing period. Waiver of the acceptance testing may be considered in those instances when CTI has demonstrated that the problems encountered are not the fault of CTI and that the government has determined that CTI has taken all reasonable actions to correct all problems. The waiver issued by the GSA CO or the OCO will specify the grounds for the waiver. If the waiver is not granted, CTI will be obligated to continue to attempt correction of the deficiencies encountered in order to successfully accomplish the acceptance testing.

3.4.6 DELIVERABLES (E.2.2.6) [RIN: MMR0031-DN]

CTI is in compliance with Section E.2.2.6 and as such shall provide an EIS Testing Report as defined in Section E.2.2.5 within 3 days of service installation and testing.

3.4.7 GENERAL INFORMATION VERIFICATION TEST PLAN

3.4.7.1 Purpose

CTI will provide an EIS Services Verification Test Plan (EIS Test Plan) based on the test methodology defined in Section E.2.2.1 – E.2.2.5 (test scenarios, test cases, test data sets, acceptance criteria) of the GSA EIS Solicitation in response to the RFP for each of the proposed EIS services. The EIS Services Verification Testing follows the BSS verification testing described above and is used to ensure the EIS Services can be adequately ordered, delivered and billed to the government.

3.4.7.2 Scope

CTI shall meet the following Inspection and Acceptance requirements for the EIS Test Plan which intersects with the BSS testing:

- The EIS Services testing shall verify that all BSS functional, regression, load, and security requirements have been successfully met.
- The EIS Services testing shall be performed for all management and operation functions supporting Ordering, Billing, Inventory Management, Disputes, SLA Management and Trouble Ticketing processes that are described in Sections G.3 – G.8 and Sections J.2.2 – J.2.10.
- Security testing shall be based on functional requirements described in Section G.5.6 BSS Security Requirements. The security requirements acceptance shall be based on evaluation for completeness that is for the ATO certification and FedRAMP compliance, if applicable.
- The testing shall include multiple test cases that are defined in Section 3.3 Test Cases.
- The EIS Services testing shall include use cases for quality, utility and customer access features.
- CTI shall allow government representative(s) to observe all or any part of the verification testing.
- If the government so requests, CTI shall perform tests to ensure continued compliance each time a new service is offered or CTI modifies features/functionality of the BSS that affect the functional requirements described in Sections G.3 – G.9. If the government requests this retest, CTI shall provide a EIS Services Verification Test Results report, including analysis, within seven (7) days after performance of the tests. The government reserves 14 days to accept or reject the test results, in part or in whole. If the government rejects the test results CTI shall retest until such time the results are acceptable to the government.
- CTI shall perform BSS verification testing according to the accepted BSS Test Plan and EIS Services Test Plan at a mutually acceptable date with the government.

3.4.7.3 System Overview

[redacted]

3.4.7.4 Project References

Clause #	FAR Clause #	Title and Date	Date
E.1.1	52.246-2	Inspection of Supplies - Fixed Price	AUG 1996
E.1.2	52.246-4	Inspection of Services - Fixed Price	AUG 1996
E.1.3	52.246-6	Time-and-Material and Labor-Hour	MAY 2001
E.1.4	52.246-16	Responsibility for Supplies	APR 1984
E.1.5	52.246-19	Warranty of Systems and Equipment under Performance Specifications or Design Criteria	MAY 2001

3.4.7.5 Points of Contact

[redacted]

3.4.8 TEST EVALUATION

3.4.8.1 Requirements Traceability Matrix and Use Cases and General Testing Requirements

CTI shall meet the following EIS Services testing requirements:

- Provide a verification and acceptance testing approach for all awarded EIS services defined in Section C.2.
- Develop an EIS Test Plan that will include, but not be limited to:
  - The test methodology for each EIS Service with test cases that will define the parameters to be measured, the measurement procedure, and the acceptance [pass/fail] criteria.
  - Fallback approach to describe the fallback process and procedures in case of testing failure.

- An EIS Test Plan shall be required for all new services during the life of the contract.

The following conditions also apply:

- An agency may define additional testing in the TO.
- CTI shall allow government representative(s) to observe all or any part of the EIS services verification testing.
- CTI shall provide all necessary test equipment: data terminals, load boxes, test cables, and any other hardware and software required for testing.

The following charts are a functions/test matrix that lists all application functions on one axis and cross-reference them to all tests included in the test plan. In addition to meeting general BSS requirements the EIS Test Plan includes the following:

3.4.8.2 Test Evaluation Criteria

CTI will reference the Test Scenarios table from Section 3.3.2.2 BSS Test Scenarios for EIS Services Verification Test Evaluation Criteria.

3.4.8.3 User System Acceptance Criteria

CTI's BSS for EIS Services must pass the defined acceptance criteria. CTI shall address the test scenarios based on the functional requirements defined in the relevant portions of Section G and J within the GSA EIS solicitation.

The scenarios shall address relevant data exchange mechanisms and validation of data exchanged. Each Test Scenario is associated with one or more Test Cases defined in Section E.2.1.3 of the GSA EIS solicitation.

CTI shall provide test cases for each of the test scenarios defined in Section E.2.2.2. of the GAS EIS RFP. The test cases will be defined in the EIS Test Plan.

CTI shall successfully test all of the test cases defined in the EIS Test Plan using one or more test data sets proposed by CTI. CTI shall test all services and service features proposed at the TO. CTI shall use test data sets that reflect real-world service conditions and locations and shall address all relevant test cases.

3.4.9 TESTING SCHEDULE

3.4.9.1 Overall test Schedule and Location

The overall Test Schedule shall be determined upon contract award with GSA representatives at CTI's headquarters.

3.4.9.2 Security

Access will be granted to GSA employees to observe the testing and test results. Any special security considerations (e.g., passwords, classifications, security or monitoring software, or computer room badges) will be provided the day of testing.

3.4.9.3 Testing Guidelines

CTI shall accept, incorporate into the EIS Services Test Plan, and successfully execute test cases provided for each of the test scenarios above.

- CTI shall accept the following test conditions:
  - No testing between CTI and GSA shall occur until both CTI's BSS and the GSA System have passed unit testing.
  - All testing to be performed on the actual system to be used in delivering service (i.e. special purpose "test systems" shall not be used).
  - Unless otherwise specified, all data transfers are to use the mechanism specified in Section J.2 for that data set.
- CTI shall use GSA provided test data for all BSS verification testing unless specified otherwise:
  - This data shall be used for testing purposes only.
  - No customer "live" data shall be used for testing.
  - This data shall be a realistic simulation of actual customer data.
  - The test data shall include, in some tests, intentional errors intended to test CTI's BSS error handling.
- EIS Services Verification testing shall follow a tiered approach:
  - CTI shall accept multiple test cases for the test scenarios defined in Section E.2.1.2.
  - CTI shall accept, incorporate into the EIS Services Verification Test Plan, and successfully execute each test case with one or more test data sets.
  - In providing test data sets, GSA will group them into Test Subcases:
    - Each Test Subcase shall contain data sets intended to test a specific "real world" test case (e.g. a complete and accurate disconnect order)
    - Each test subcase shall include at least two complete test data sets
- EIS Services Verification functional testing acceptance:

- CTI's BSS shall not have completed functional testing until all EIS Services Verification Test Scenarios (Section 3.3) are successfully passed.
- A test scenario shall not be considered passed until CTI's BSS properly handles each associated test case.
- A test case shall not be considered passed until CTI's BSS properly handles each associated subcase twice in succession using different data sets.

- EIS Services security testing acceptance is defined in Section G.5.6 and associated references.

The individual test cases are defined in the tables in the subsections below. Each test case table includes the following headings:

- Test Scenario: The associated test scenario from Section E.2.1.2.
- Test Case ID: Identification number for the test case.
- Test Case Description: Brief title of the test case.
- Requirements Reference(s): Where the functional requirements that are being tested can be found.
- Prerequisites: Actions that must be completed prior to implementing the test case (in addition to the general prerequisites for all testing).
- Government Input(s): Data the government will provide as input to the test case.
- Expected EIS Services Verification Output(s): Expected data or actions from CTI's BSS.
- Data Set Description: Brief description of the data sets the government intends to provide as part of testing.
- Acceptance Criteria: Factors to be checked prior to acceptance of the test results. The table below defines the terms used:

[redacted]	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

3.4.9.4 Test Results and Acceptance

CTI shall provide an EIS Services Verification Testing Report (EIS Testing Report) that shows successful completion of testing defined in the EIS Test Plan. CTI shall complete verification and acceptance testing based on the acceptance criteria defined in the government accepted EIS Test Plan. Acceptance shall include government compliance requirements such as FedRAMP for cloud services, and the ATO for FISMA related security requirements for EIS services. CTI shall provide the following in order for the government to approve the test results:

- FedRAMP compliance if cloud services are included in the TO.
- EIS Testing Report showing that each service provisioned works properly according to the KPIs defined in Section C.2 and the acceptance criteria defined in the EIS Test Plan.

Once verification testing is completed successfully the government may complete acceptance testing based on the acceptance criteria defined in the EIS Test Plan. The acceptance test will verify satisfactory end-to-end service performance and proper

operation of all ordered features and functions. Performance will be considered satisfactory when services, equipment, systems and their associated features and functions perform as specified in the contract and TO. CTI may not assign an effective billing date to an EIS Service until the agency accepts it in accordance with the agreed-upon acceptance testing procedures described in the EIS Test Plan.

The government reserves the right to perform additional tests to confirm proper operation of a delivered EIS service as defined by the TO. If the government does not report a problem to CTI during this test period, the effective billing date will be the completion date on the SOCN. CTI 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. CTI shall issue a new SOCN for services after correcting the reasons for rejection.

The service will be considered accepted if the government does not reject the service within the acceptance period defined above. If the government rejects the service, it may at its option:

1. Direct CTI to repeat the procedure outlined above;
2. Withdraw the service from acceptance testing;
3. Direct CTI to facilitate the return of the services to their original provider (for services transitioned or migrated from another contractor’s network);
4. Request a replacement of the service (in whole or in part); or
5. Cancel the service order without penalty.

If the government exercises any of these options as a consequence of unacceptable acceptance testing results, all expenses incurred by the government shall be borne by CTI.

If the government elects option 1 above, CTI shall immediately initiate corrective actions to remedy the problem reported on the trouble ticket and shall keep the government informed of progress. In such cases, the government reserves the right to exercise option 2, 3, 4 or 5 at any time.

If the government elects any of the options above other than option 1, all expenses incurred by the government, including recurring charges and non-recurring charges (NRC) to return services to the previous network configuration, shall be borne by CTI. In

cases when the government cannot successfully complete acceptance testing due to circumstances beyond the control of CTI, CTI shall notify government of the details surrounding the deficiencies and the steps CTI has taken to overcome the deficiencies. These cases shall be discussed between the government and CTI. On a case-by-case basis, the GSA CO or the OCO may choose to waive the acceptance testing or extend the testing period. Waiver of the acceptance testing may be considered in those instances when CTI has demonstrated that the problems encountered are not the fault of CTI and government has determined that CTI has taken all reasonable actions to correct all problems. The waiver issued by the GSA CO or the OCO will specify the grounds for the waiver. If the waiver is not granted, CTI shall be obligated to continue to attempt correction of the deficiencies encountered in order to successfully accomplish the acceptance testing.

3.4.9.5 Equipment and Software Requirements

CTI's Business Support System, supporting equipment and networking infrastructure to allow for data queries. All office furniture and other standard office items as required for personnel to conduct the testing and obtain required reports and data in an easily transportable format for inspection and analysis.

3.4.9.6 Personnel Requirements

CTI will provide all personnel required to act as simulated government test customer, an industry partner product/service provider(s) and CTI as the contractual executor.

3.4.9.7 Deliverable Materials

CTI shall provide an EIS Test Plan in its proposal that describes the testing of EIS Services based on test methodology described in GSA EIS solicitation Sections E.2.1.1 through E.2.2.5. CTI shall provide an EIS Testing Report as defined in GSA EIS solicitation Section E.2.2.5.

3.4.9.8 Testing Tools

CTI's Business Support System, supporting equipment and networking infrastructure to allow for data queries.

3.4.9.9 Site Supplied Materials

CTI shall provide all desks, chairs, computers, printers, papers, pads, and writing equipment needed to take notes and print results of the testing.

3.4.10 TESTING CHARACTERISTICS

3.4.10.1 Testing Conditions

Testing conditions for both the EIS and BSS shall be done on any BSS capable computer and can be selected at random by a government official to ensure a standard computer is used. All computers used to access the system are housed in normal office conditions and may be in a controlled access location. [redacted]

3.4.10.2 Extent of Testing

Testing will test each of the parameters as annotated within this test plan.

3.4.10.3 Data Recording

All data will be kept within the BSS and can be printed upon request.

3.4.10.4 Testing Constraints

Testing will not have limitations except on the use of private customer data.

3.4.10.5 Test Progression

As each test is performed and the results given the testers can move to the next Use Case.

3.4.10.6 Test Evaluation

3.4.10.6.1 Test Data Criteria

[redacted]

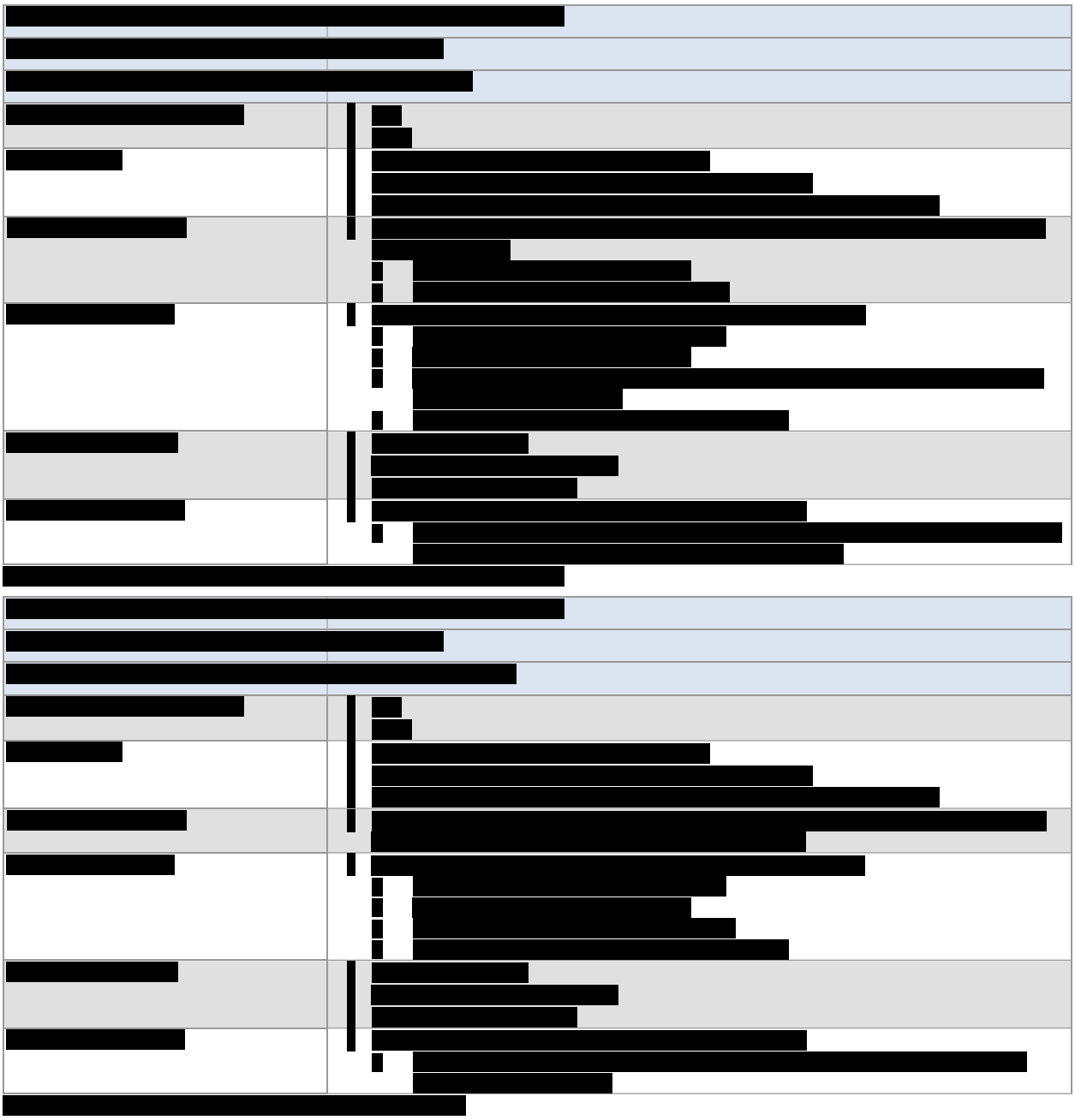
The purpose of the verification and acceptance testing is to ensure that CTI's BSS meets requirements in Sections G.3 – G.9 and Sections J.2.2 – J.2.10 to accomplish EIS services verification testing. CTI shall support BSS security and functional testing as defined in Section G.5.6 BSS Security Requirements and Section G.5.5.1 BSS Testing.

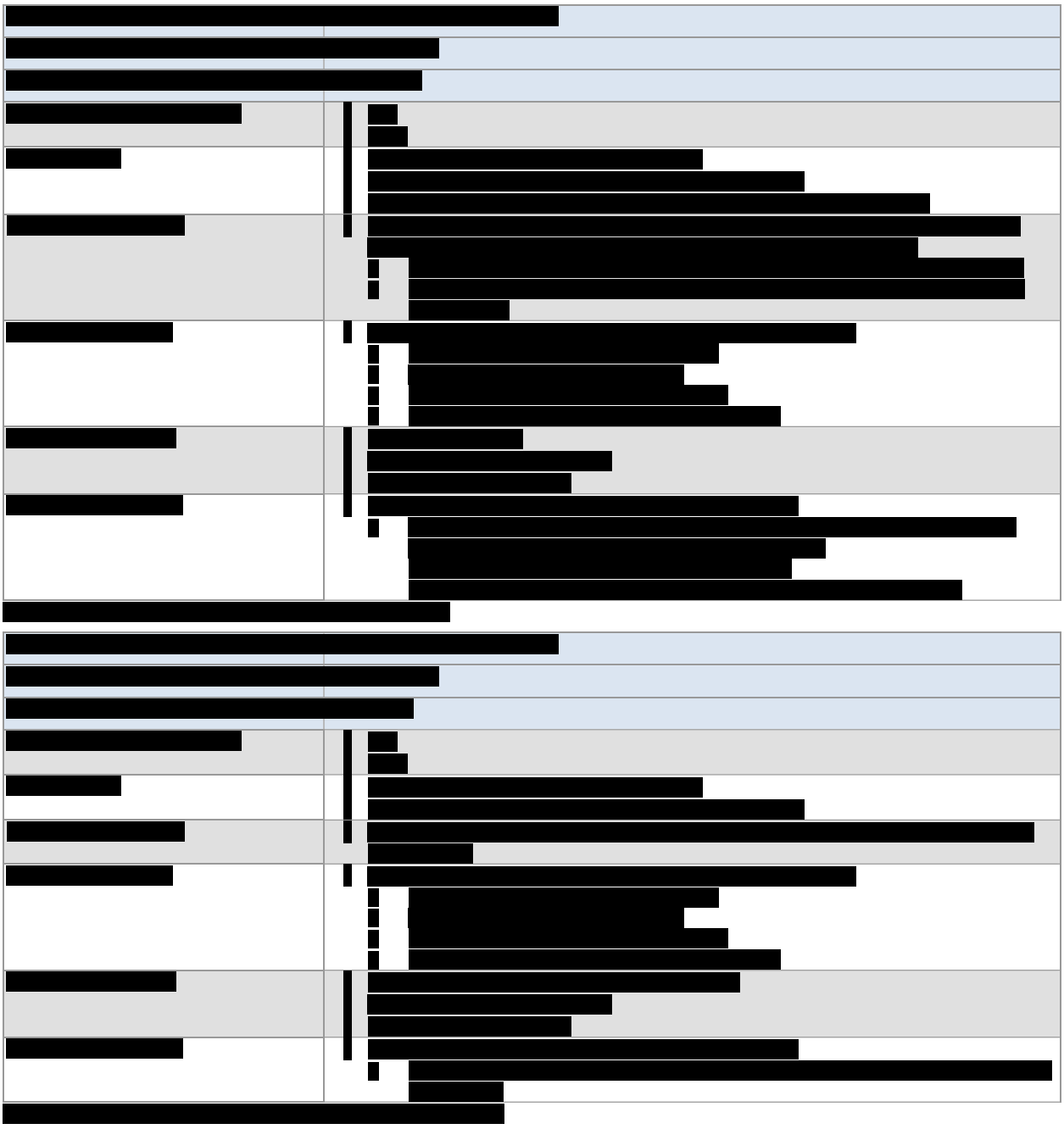
3.4.10.6.2 Test Data Reduction

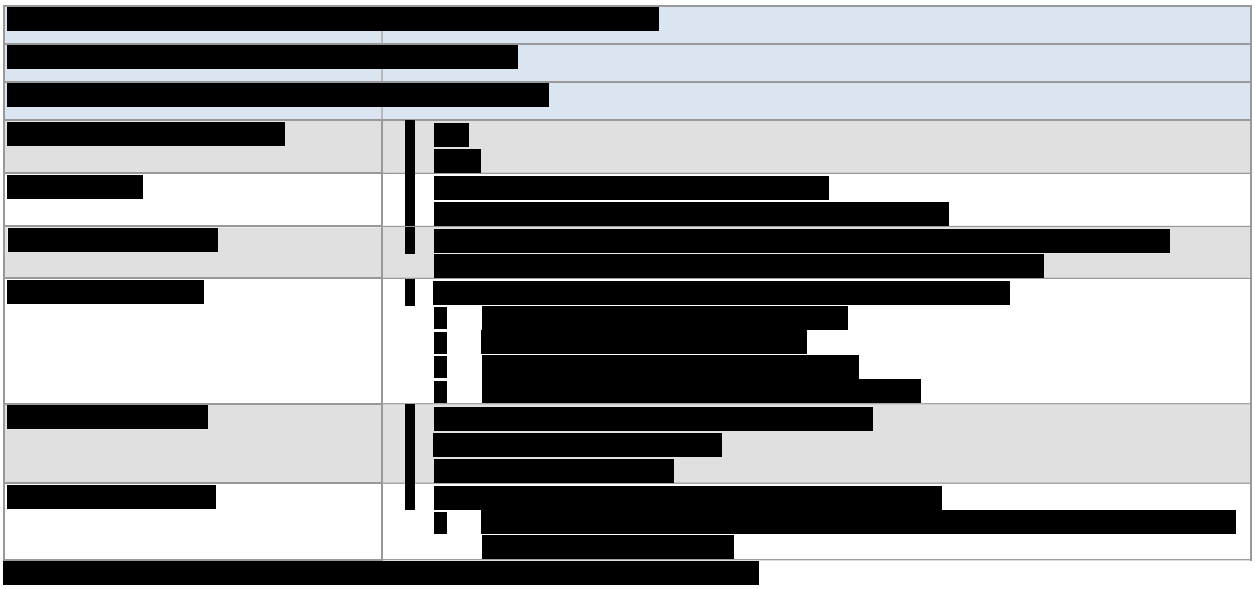
No test data reduction is anticipated as each result will be printed out as if it were from real customers requesting real services.

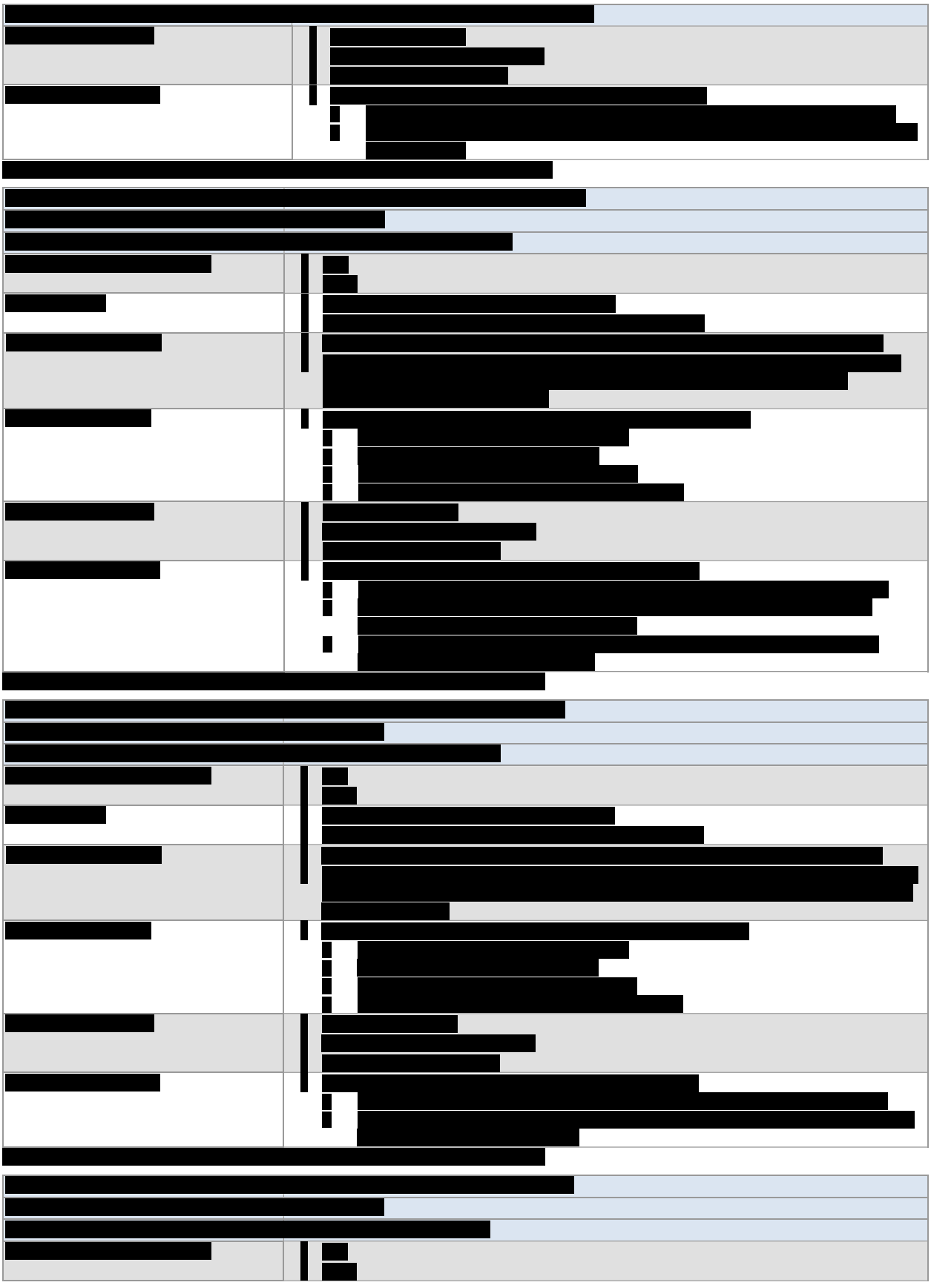
TEST DESCRIPTION for EIS Verification using CTI's BSS.

3.4.10.6.2.1 BSS-TS01-01: New EIS Service Order via Web Interface









[redacted]

3.4.10.6.4 Termination

Tests and testing will terminate when adequate testing results are achieved, or in case of errors or incomplete testing, the testing will terminate is no adequate solutions have been found or errors resolved in which case the specific test will be noted and returned to CTI for resolution.

3.4.11 EIS TEST PLANS SPECIFIC TO PROPOSED SERVICES [RIN: MMC0020-DI, MMC0021-DI]

3.4.11.1 Virtual Private Network Service Test Plan

[redacted]

Test Objectives

The primary objectives for this test are as follows:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

T	

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

[redacted]

[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	[redacted]
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	

[redacted]

[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	[redacted]
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	
[redacted]	

[redacted]	
[redacted]	
[redacted]	

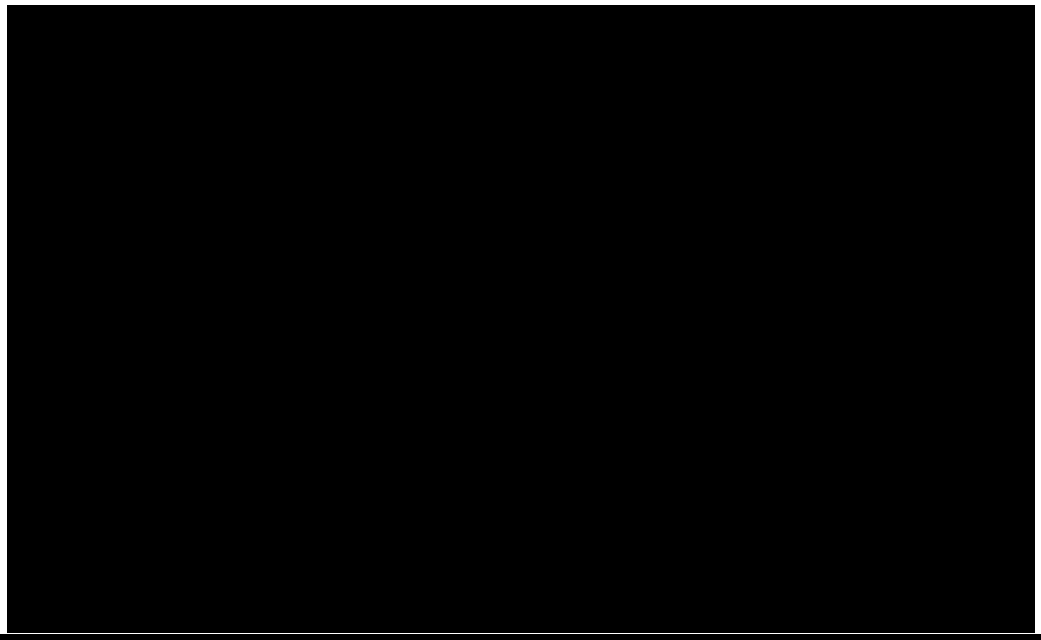
3.4.11.1.1 VPNS Test Plan Fallback

Upon any test failures, CTI will inspect every aspect of the service, and correct any issues. CTI will then perform a full retest of the system, and will continue this until all test failures have been resolved and the service is ready for acceptance.

3.4.11.2 Ethernet Transport Service Test Plan

[redacted]

[redacted]



[redacted]

The network configuration test consists in sequentially testing each service. It validates that the service is properly provisioned and that all specific KPIs or SLA parameters are met.

The service test simultaneously validates the quality of all the services over time. All services are generated at once at their CIR and all key performance indicators are measured for each service.

The following table provides a list and explanation of the other main test applications used in Ethernet testing.

	performance of networks. EXFO's offering concentrates on the four fundamental subtests; namely, the

3.4.11.2.1 ETS Test Plan Fallback

Upon any test failures, CTI will inspect every aspect of the service, and correct any issues. CTI will then perform a full retest of the system, and will continue this until all test failures have been resolved and the service is ready for acceptance.

3.4.11.3 Internet Protocol Voice Service Test Plan

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3.4.11.3.1 IPVS Fallback

Upon any test failures, CTI will inspect every aspect of the service, and correct any issues. CTI will then perform a full retest of the system, and will continue this until all test failures have been resolved and the service is ready for acceptance.

3.4.11.4 Circuit Switched Voice Service Test Plan

CTI will perform [redacted] testing on all Circuit Switched Voice products that CTI is offering under EIS. [redacted]

[redacted]

[redacted]

3.4.11.4.1 CSVS Test Plan Fallback

Upon any test failures, CTI will inspect every aspect of the service, and correct any issues. CTI will then perform a full retest of the system, and will continue this until all test failures have been resolved and the service is ready for acceptance.

3.4.11.5 Infrastructure as a Service Test Plan

Testing cloud services such as Infrastructure as a Service (IaaS) will be unique to each application and hardware platform that is implemented. However there is a standard test methodology that CTI has developed to ensure quality, reliability and performance of its cloud service offerings. [redacted]

3.4.11.5.1 IaaS Test Plan Fallback

Upon any test failures, CTI will inspect every aspect of the service, and correct any issues. CTI will then perform a full retest of the system, and will continue this until all test failures have been resolved and the service is ready for acceptance.

3.4.11.6 Audio Conferencing Service Test Plan

CTI's Audio Conferencing Service offerings combine aspects from several other different offerings previously discussed. VoIP, Ethernet transport, Cloud Services (IaaS, PaaS), and circuit switched voice circuits.

[redacted]

3.4.11.6.1 ACS Test Plan Fallback

Upon any test failures, CTI will inspect every aspect of the service, and correct any issues. CTI will then perform a full retest of the system, and will continue this until all test failures have been resolved and the service is ready for acceptance.

3.4.11.7 Access Arrangements Test Plan

[redacted]

3.4.11.7.1 AA Test Plan Fallback

Upon any test failures, CTI will inspect every aspect of the service, and correct any issues. CTI will then perform a full retest of the system, and will continue this until all test failures have been resolved and the service is ready for acceptance.

3.4.11.8 Service Related Equipment Test Plan

CTI will test all Service Related equipment to the manufacturers recommended specifications[redacted].

3.4.11.8.1 SRE Test Plan Fallback

Upon any test failures, CTI will inspect every aspect of the service, and correct any issues. CTI will then perform a full retest of the system, and will continue this until all test failures have been resolved and the service is ready for acceptance.

3.4.11.9 Cable and Wiring Test Plan

CTI will prepare a Test Plan in accordance with approved industry and OEM procedures that outline, sequence and indicate qualifications for system acceptance.

[redacted]

[redacted]

[redacted]

[redacted]

3.4.11.9.1 CW Test Plan Fallback

Upon any test failures, CTI will inspect every aspect of the service, and correct any issues. CTI will then perform a full retest of the system, and will continue this until all test failures have been resolved and the service is ready for acceptance.

3.4.11.10 Services Not Requiring Testing

CTI has identified that all the services that are being proposed from Section C.2 require a test plan and fallback approach, thus deeming that there are no services for which testing is not applicable.

3.5 CLIMATE RISK MANAGEMENT PLAN [L.30.2.5]

The global focus and strong level of interest to ensure environmental sustainability, that industry and governments alike are demonstrating, is a growing phenomenon and has quickly become one of the defining issues of our time. Core Technologies, Inc. (CTI) is a company that readily understands the need to make informed and responsible decisions to employ environmental sustainability initiatives and, at the same time, consider the implications on our future plans.

In meeting the Section L.30.2.5 RFP requirement, CTI is providing this Climate Risk Management (CRM) Plan as Appendix E to our Volume 2 Management Proposal. This CRM Plan demonstrates CTI's compliance with the climate change adaptation conditions described in Executive Orders and other applicable laws, regulations, and directives.

3.5.1 CLIMATE CHANGE ADAPTATION, SUSTAINABILITY AND GREEN INITIATIVES [G.12]

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.

The goal of Executive Order (EO) 13693, which is titled: "Planning for Federal Sustainability in the Next Decade", is to maintain Federal leadership in sustainability and GHG emission reductions. For the EIS program, CTI is ready to support this goal as we progress with our commitment to environmental sustainability and change adaptation in service design and operations and risk management strategies.

The Government Accountability Office (GAO) has, since 2013, identified the changing climate as one of the 30 most significant risks facing the federal government. President Obama established adaptation as a prominent part of his Climate Action Plan in June 2013. The November 2013 Executive Order 13653, Preparing the United States for the Impacts of Climate Change, directed agencies to undertake vulnerability assessments and planning for adaptation. The Administration aimed efforts at reducing agencies' own

risks, taking advantage of “no-regrets” adaptation opportunities, and actions that promote resilience to climate changes.

[redacted]

[redacted]

[redacted]

3.5.1.1 Climate Change Adaptation [G.12.1] [RIN: MMR0095-DN]

CTI will incorporate strategies in addressing climate change adaptation aspects into our risk-management programs to reduce vulnerabilities to our property, infrastructure, and supply chain. These strategies will be utilized in the design and operations of the services that CTI is offering under EIS. Appropriate climate change adaptations can result in minimizing negative impacts and/or allow enterprises to take advantage of new opportunities presented by changing climate conditions.

[redacted]

[redacted]

[redacted]

Key Performance Indicators (KPIs)

In this area, CTI will focus on matching the environmental KPIs to our specific business strategy targets, and we will develop standardized processes to make sure the KPI data is as useful as possible to facilitating Climate Change Risk Management. [redacted]

Comply with Executive Order 13693

Executive Order (EO) 13693 was signed on March 19, 2015. This EO introduces new requirements and expands upon requirements established by EO 13514, EO 13423, the Energy Policy Act of 2005 (EPAct 2005), and the Energy Independence and Security

Act (EISA) of 2007. CTI will comply with the climate change adaptation conditions described in Executive Order 13693 and other applicable laws, regulations, and directives. CTI will comply with the climate change adaptation conditions described in EO 13693, especially as they pertain to Scope 3 conditions. Scope 3 pertains to GHG emissions from sources not owned or directly controlled by an agency but related to agency activities such as vendor supply chains, delivery and transportation services, and employee travel and commuting.

We will prepare and update, as needed, this Corporate Climate Risk Management Plan. We will make this plan available for agency use in support of their efforts to develop their Agency Adaptation Plans. Agencies incorporate adaptation strategies into their planning to ensure that resources are invested wisely and that their services and operations remain effective to meet current and future conditions.

Conducting Corporate Sustainability Reporting

CTI will subscribe to the Global Reporting Initiative (GRI) and the Carbon Disclosure Project (CDP) to conduct our corporate sustainability reporting. GRI is the official reporting portal for some 8,700+ organizations. Its framework uses a rigorous stakeholder approach to standard development with participants drawn globally from business, civil society, labor, and professional institutions. GRI's reporting methodology is free and available for anyone to view, as are the reports companies publish using the framework.

Notification to GSA Contracting Officer

CTI will notify the agency and the GSA CO immediately if conditions arise where the Climate Risk Management Plan is not in compliance with the Executive Orders, laws, regulations, and directives.

3.5.1.2 Sustainability and Green Initiatives [G.12.2]

[redacted]

[redacted]

CTI will notify the agency and GSA COR immediately if conditions arise deemed to be out of compliance with the EIS RFP's list of Executive Orders, laws, regulations, and directives.

When CTI opts to offer Energy Star-certified, low standby power, or Electronic Product Environmental Assessment Tool (EPEAT) registered products, we will identify, by model, which products offered are Energy Star-qualified/certified, meet Federal Energy Management Program (FEMP) low standby power levels, and/or are EPEAT-registered. If the product is EPEAT-registered, it will be identified by a registration level of bronze, silver, or gold.

[redacted]

3.5.1.2.1 Electronic Product Environmental Assessment Tool [G.12.2.1]

[redacted]EPEAT is a method used to evaluate the effect of a product on the environment and it rates products as gold, silver, or bronze based on a set of environmental performance criteria. Products are rated Bronze, Silver, or Gold based on how many of the 28 optional criteria they meet, as follows:

Below 50% - Bronze	50% - 74% - Silver	75% or more - Gold

[redacted]

[redacted]

3.5.1.2.2 Energy Efficient Products [G.12.2.2]

In compliance with FAR Clause 52.223-15, CTI will 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,

FEMP provides resources and tools to help agencies purchase energy- and water-efficient products. [redacted]

3.5.1.2.3 Data Centers and Cloud Services [G.12.2.3]

[redacted]

[redacted]CTI has verified that our Data Center [redacted]uses Industry-leading solutions in containment and track power usage effectiveness (PUE) metrics, which determine the energy efficiency of a data center.

[redacted]

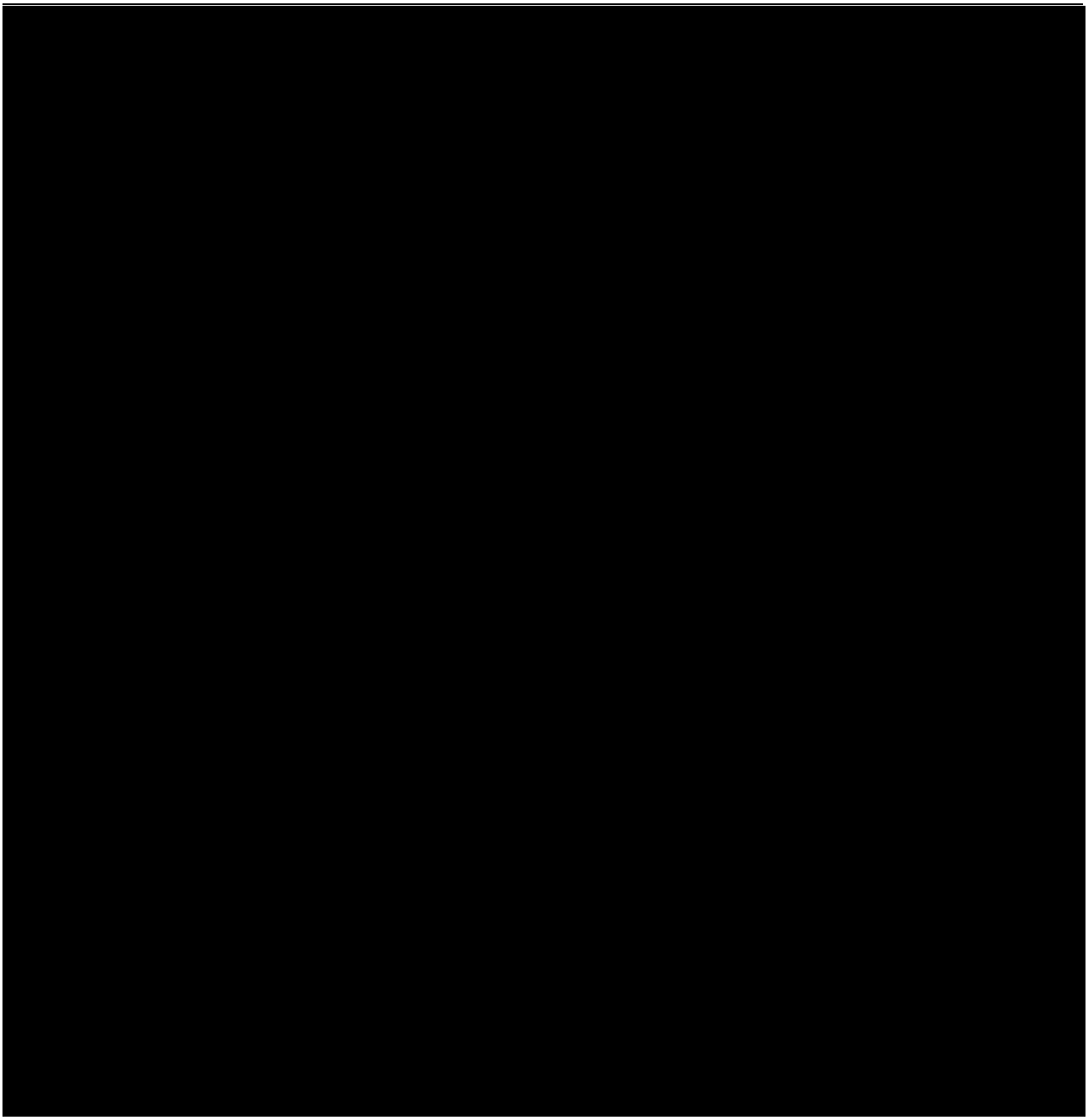
[redacted]

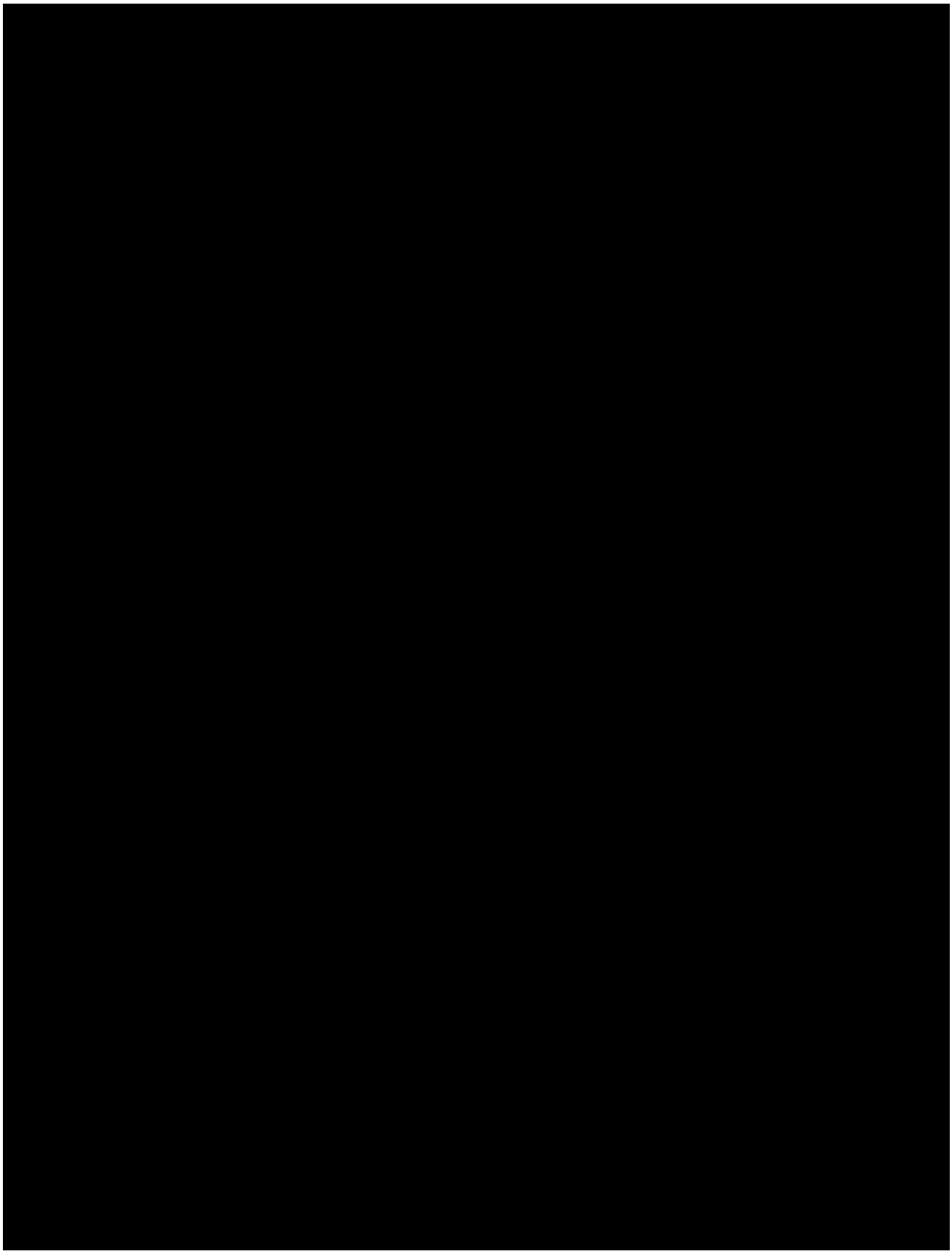
3.6 FINANCIAL MANAGEMENT REPORT [L.30.2.6; G.9.5; H.7]

3.6.1 INTRODUCTION

CTI will provide the monthly Financial Management Report to the PMO. The report will include the following information:

- The total billed charges for all agencies during the monthly reporting period
- The total dollar activity broken down by the service types and services,
- The remaining amount of unspent dollars under the maximum contract dollar limitation





3.7 BBS RISK MANAGEMENT FRAMEWORK PLAN (L.30.2.7, G.5.6)

3.7.1 HOW BSS RISK MANAGEMENT FRAMEWORK PLAN ADDRESS SYSTEM SECURITY [L.30.2.7; G.5.6; J.8; C.6.6; I]

The Business Support Systems (BSS) Risk Management Framework plan is a framework for the BSS System Security Plan (SSP), which is designed to provide an overview of the security requirements of the system in use and which describes the controls in place or planned for meeting those requirements. Our system security plan delineates responsibilities and expected behavior of all individuals who access the system, both internally to the Core Technologies, Inc. (CTI), our Team members, and externally, from those federal agencies and organizations expected to interact with the BSS itself. [redacted] All federal systems and many large commercial concerns have some level of sensitivity and require protection as part of good management practices. Within the commercial sector, besides industry best practices, all commercial applications that deal with interstate transactions must deal, at some level, with federal mandates and security practices – either mandated or accepted as industry best practices and/or accreditation standards. Therefore, the protection of a system must be documented in a system security plan and CTI's BSS SSP shall meet the stipulations contained in Section G.5.6 by adhering to government regulations concerning development of such plans.

The completion of system security plans is a requirement of the Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Resources," and "Title III of the E-Government Act", entitled the Federal Information Security Management. [redacted]

[redacted]

3.7.1.1 General Security Compliance Requirements [G.5.6.1] [RIN:]

[redacted].

All information systems in our inventory are categorized using FIPS 199 as a first step in our system security planning activity. FIPS 199 is a mandatory standard used by all federal agencies to categorize all information and information systems collected or

maintained by or on behalf of each agency based on the objectives of providing appropriate levels of information security according to impact.

Security categorization standards for information and information systems provide a common framework and understanding for expressing security that, for the federal government, promotes: (a) effective management and oversight of information security programs, including the coordination of information security efforts throughout the civilian, national security, emergency preparedness, homeland security, and law enforcement communities; and (b) consistent reporting to the Office of Management and Budget (OMB) and Congress on the adequacy and effectiveness of information security policies, procedures, and practices.

[redacted]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.”

In addition to complying with the requirements identified in the government policies, directives and guides specified above, CTI 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 2100.1(I).
- 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,” April 2007.

3.7.1.1.1 Compliance with GSA Policies, Directives, and Guides

[redacted]

[redacted]Compliance includes compliance with the following Federal documents, which in turn have sub-set GSA documents as denoted within this section.

- Federal Information Security Management Act (FISMA) of 2002.
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.).
  - Clinger-Cohen Act of 1996 also known as the “Information Technology Management Reform Act of 1996.”
  - 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.
  - OMB Circular A-130, “Management of Federal Information Resources,” and Appendix III, “Security of Federal Automated Information Systems,” as amended.
  - OMB Memorandum M-04-04, “E-Authentication Guidance for Federal Agencies.”

- OMB Memorandum M-05-24, “Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors.”
- 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).
- OMB Memorandum M-14-03, “Enhancing the Security of Federal Information and Information Systems.”
- 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.”

In addition to complying with the requirements identified in the government policies, directives and guides specified above, CTI shall comply with the current GSA policies, directives and guides listed below:

GSA Information Technology (IT) Security Policy, CIO P 2100.1(I).

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,” April 2007.

3.7.1.2 GSA Security Compliance Requirements [G.5.6.2]

CTI’s BSS SSP adheres to GSA Security Requirements through the development of their SSP in accordance with FIPS 199 as stated in the prior section, and which should be in compliance, and in accordance with NIST SP 800-18 and 37 at the Moderate level. Our approach for the BSS Risk Management Framework Plan is to use the specific guidelines established in NIST 800-18 R1. [redacted]

[redacted]

[redacted]

[redacted]

3.7.1.3 Security Assessment and Authorization (Security A&A) [G.5.6.3]

[redacted]

3.7.1.4 BSS System Security Plan (BSS SSP) [G.5.6.4]

As part of its BSS SSP approach CTI shall comply with all security A&A and shall have a BSS that can pass the formal approval process. Compliance also infers compliance with all federal laws, directives and policies including making available any documentation, physical access, and logical access needed to support the government's requirements.

3.7.1.4.1 Security Assessment Boundary and Scope Document (BSD)

CTI, as part of its BSS SSP, shall also complete and maintain a Security Assessment Boundary and Scope Document (BSD) using the template in Section J.8 and will submit same within 15 days of the NTP and update it on an annual basis. The BSD will be used to determine the actual security assessment boundary. CTI will cooperatively work with the federal government to establish and/or change information system security (ISS) boundaries.

3.7.1.4.2 Interconnection Security Agreements (ISA)

CTI shall, as part of its BSS SSP and security A&A package, create, develop and maintain Interconnection Security Agreements (ISA) developed in accordance with NIST SP 800-47. The ISA's will be compiled and kept with the overall BSS SSP and be updated on an annual basis.

3.7.1.4.3 Control Tailoring Workbook

CTI, as part of its BSS SSP, security A&A package, and ISA will also develop and maintain a Control Tailoring Workbook as identified in GSA IT Security Procedural Guide 06-30 and in accordance with the template in Section J.8. This Control Tailoring Workbook shall document all contractor-implemented settings that are different from GSA-defined settings, and where GSA defined settings allow a contractor to deviate. CTI will provide this CTW with the initial security A&A package and update it annually.

iv.

3.7.1.4.4 GSA Control Summary Table for a Moderate Impact Baseline

CTI, as part of its BSS SSP, security A&A package, and ISA will also develop and maintain a GSA Control Summary Table as identified in GSA IT Security Procedural Guide 06-30 in accordance with the template in Section J.8. CTI shall provide the Control Summary Table with the initial security A&A package and update annually.

v.

3.7.1.4.5 Rules of Behavior (RoB)

CTI, as part of its BSS SSP, security A&A package, and ISA shall also develop and maintain a Rules of Behavior (RoB) for information system users as identified in GSA IT Security Procedural Guide 06-30 and GSA Order CIO 2104.1. CTI will provide the RoB for our BSS along with the initial security A&A package and update annually.

3.7.1.4.6 System Inventory

The CTI's BSS application provides the team an all-in-one solution that is scalable and highly available, platform independent, open and extensible. The system provides features that match the needs of the GSA EIS vehicle in terms of GSA IT Security Procedural Guide 06-30. It features a tightly integrated monitoring and billing system that demonstrates specialization in usage-based billing. It enables CTI to offer out-of-the-box solutions for inventory control, bandwidth billing, ticket-time billing, power billing and resource-based cloud billing. For our customers the system can be mapped to represent all applicable data centers and connections, the Device Manager offers easy-to-configure network and power monitoring, switch management, server metrics and reboot controls. The CTI Team will provide a System Inventory for our BSS along with the initial security A&A package and update annually.

vi.

3.7.1.4.7 Contingency Plan (CP)

CTI shall develop and maintain a Disaster Recovery Plan (DRP), Contingency Plan (CP) and Business Impact Assessment (BIA) in accordance with NIST SP 800-34 as part of a standard BSS SPP and submit it with the initial security A&A package and update it annually.

vii.

3.7.1.4.7.1 Disaster Recovery Plan (DRP)

CTI shall provide and maintain a Disaster Recovery Plan (DRP), Contingency Plan (CP) and Business Impact Assessment (BIA) in accordance with NIST SP 800-34 as part of our standard BSS SPP and submit it with the initial security A&A package and update it annually.

3.7.1.4.7.2 Business Impact Assessment (BIA)

CTI shall provide and maintain a Business Impact Assessment (BIA) in accordance with NIST SP 800-34 as part of our standard BSS SPP. CTI will provide the BIA with the initial security A&A package and update it annually.

3.7.1.4.8 Contingency Plan Test Plan (CPTP)

CTI shall provide and maintain a Contingency Plan Test Plan (CPTP) in accordance with NIST SP 800-53 and in agreement with GSA IT Security Procedural Guide 06-29 as part of our standard BSS SPP. CTI will provide the CPTP with the initial security A&A package and update it annually.

3.7.1.4.9 Contigency Plan Test Report (CPTR)

CTI shall test the CP and document the results in a Contingency Plan Test Report (CPTR) in agreement with GSA Security Procedural Guide 06-29 and in accordance with NIST SP 800-53 as part of a standard BSS SPP. CTI shall provide a CPTR for the information system with the initial security A&A package and update it annually.

viii.

3.7.1.4.10 Privacy Impact Assessment (PIA)

CTI will perform a Privacy Impact Assessment (PIA) and complete it as identified in GSA IT Security Procedural Guide 06-30 and in accordance with NIST SP 800-53 R4: AR-2, AR-3, and AR-4 as part of our standard BSS SPP. CTI will provide a PIA for the information system with the initial security A&A package and update it annually.

ix.

3.7.1.4.11 Configuration Management Plan (CMP)

CTI shall develop and maintain a Configuration Management Plan (CMP) in accordance with NIST SP 800-53 R4 control CM-9; NIST SP 800-128; GSA CIO-IT Security 01-05 as part of our standard BSS SPP. The CMP for our BSS will be provided along with the initial security A&A package.

x.

3.7.1.4.12 System(s) Baseline Configuration Standard Document

CTI shall develop and maintain a System(s) Baseline Configuration Standard Document (BCSD) in accordance with NIST SP 800-53 R4 control CM-2; NIST SP 800-128; GSA CIO-IT Security 01-05 as part of our standard BSS SPP. CTI shall provide a well-defined, documented, and up-to-date specification to which the information system is built. CTI shall provide the SBC for the information system as part of the CMP and shall submit it with the initial security A&A package, including annual updates.

xi.

3.7.1.4.13 System Configuration Settings

A BSS System Configuration Settings in accordance with NIST SP 800-53 R4 control CM-6; NIST SP 800-128; GSA CIO-IT Security 01-05 as part of a standard BSS SPP, shall be developed and maintained by CTI. This document will establish mandatory configuration settings for IT products employed within CTI's BSS that will reflect the most restrictive mode consistent with operational requirements. Our current system complies with federal guidelines, requirements and directives and is industry certified per the Payment Application Data Security Standard (PA-DSS) certification. These system configurations may be viewed at any time by an authorized government official and shall be updated/reviewed by the CTI CIO on an annual basis.

xii.

3.7.1.4.14 Incident Response Plan (IRP)

An Incident Response Plan (IRP) is part of CTI's Disaster Recovery Plan (DRP), that is created and maintained in accordance with NIST SP 800-53 R4 control IR-8; NIST SP 800-61; and GSA CIO Security 01-02 as part of our standard BSS SPP. CTI will provide the IRP with the initial security A&A package and update it annually.

xiii.

3.7.1.4.15 Incident Response Test Report (IRTR)

An Incident Response Test Report (IRTP) is part of CTIs Disaster Recovery Plan (DRP), and part of the IRTR that is created and maintained in accordance with NIST SP 800-53 R4 control IR-8; NIST SP 800-61; and GSA CIO Security 01-02 as part of our standard BSS SPP. CTI test the IRP and document the results in the above IRTR and will provide it with the initial security A&A package, including annual updates.

xiv.

3.7.1.4.16 Continuous Monitoring Plan

CTI's Managed Security Services (MSS) provides continuous monitoring and protection of endpoints, email, web, and networks, and includes capabilities such as authentication, anti-virus, anti-malware/spyware, intrusion detection, and security event management. CTI shall provide a Continuing Monitoring Plan (CMP) in accordance with NIST SP 800-53 R4: CA-7 as part of the BSS SSP initial security A&A package, including annual updates.

CTI's MSS comprises the following underlying functions:

- Managed Prevention Service
- Vulnerability Scanning Service
- Incident Response Service

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

XV.

3.7.1.4.17 Plan of Action and Milestones

CTI shall develop and maintain a Plan of Action and Milestones (POA&M) in agreement with GSA IT Security Procedural Guide 06-30. All scans will be performed per the processes outlined in the BSS SSP. Results of scans will be mitigated and managed in the POA&M and submitted together with the quarterly POA&M submission. Scans using

the software in our MSS include all networking components that fall within the security accreditation boundary and will be submitted with the initial security A&A package. An annual information system user certification and authorization review shall be annotated on the POA&M in accordance with the template provided in Section J8. All identified gaps between required 800-53 R4 controls and CTI's implementation shall be tracked for mitigation in a POA&M document completed in accordance with GSA IT Security Procedural Guide 09-44. CTI shall provide a POA&M for our BSS along with the initial security A&A package.

xvi.

3.7.1.4.18 Independent Penetration Test Report

[redacted]The service tests for vulnerabilities by comparing scanned information to data contained in a database, which is updated as new threats are discovered. VSS can also simulate a real intrusion in a controlled environment, in order to gauge a network's susceptibility to attacks. The service performs external scans by remotely probing a network for vulnerabilities that generally come from the outside; and internal scans which detect flaws originating from the inside. While the VSS is part of the overall MSS, CTI will coordinate independent testing through the GSA Office of the Chief Information Security Officer (OSISO) Security Engineering (ISE) per NIST SP 800-53 R4; CA-5 and RA-5. The independent testing authority will provide an Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities. CTI understands that GSA will provide for the scheduling and performance of these penetration tests with the security assessment package and on an annual basis in accordance with GSA CIO-IT Security Guide 11-51.

xvii.

3.7.1.4.19 Code Review Report

[redacted]

[redacted]

xviii.

3.7.1.4.20 Security/Risk Assessment and Penetration Tests

CTI shall allow GSA employees to conduct security A&A activities as requested and in accordance with NIST SP 800-53 R4 / NIST SP 800-53A R4 and GSA IT Security Procedural Guide 06-30. We understand that all scans must be performed as an authenticated user with elevated privileges.

3.7.1.4.21 Plan of Action and Milestones (POA&M) [G.5.6.4]

All identified gaps between required 800-53 R4 controls and the CTI's implementation as documented in the Security/Risk Assessment Report (SAR) will be tracked by CTI 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)."

xix.

See Section 2.8.4.17 Plan of Action and Milestones

3.7.1.4.22 Risk Mitigation Status Update Report

If a security risk is discovered during monitoring activities it shall be immediately reported through CTI's chain of command and to the government point of contact. CTI will mitigate all critical and high-risk vulnerabilities within 7 days and all moderate risk vulnerabilities within 14 days from the date the vulnerability is formally identified. We understand that the government will determine the risk rating of vulnerabilities. CTI shall provide status updates on a monthly basis on all critical and high-risk vulnerabilities that have not been closed within 30 days.

3.7.1.4.23 Annual FISMA Assessment Report

CTI shall deliver the results of our annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, "FISMA Implementation." CTI understands that each fiscal year the annual assessment will be completed in accordance with

instructions provided by GSA and CTI will work in conjunction with GSA to ensure the assessment report goes smoothly.

3.7.1.4.24 Policy and Procedures Documentation [G.5.6.4]

CTI will 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 will 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).

The CTI Team currently keeps all identified documents updated.

3.7.1.5 Additional Security Requirements [G.5.6.6]

CTI will 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 C.6.6 will 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 will be encrypted. Certified encryption modules will be used in accordance with FIPS PUB 140-2, “Security Requirements for Cryptographic Modules.”

Where appropriate, CTI will 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.”)

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

1. CTI will not publish or disclose in any manner, without the CO’s written consent, the details of any safeguards either designed or developed by CTI 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 CTI. CTI will provide the government

logical and physical access to it's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits will include, but are not limited to, the following methods:

a. Authenticated and unauthenticated operating system/network vulnerability scans
b. Authenticated and unauthenticated web application vulnerability scans
c. Authenticated and unauthenticated database application vulnerability scans
d. Internal and external penetration testing
e. 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 CTI 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 will be approved by the government. In addition, the results of contractor-conducted scans will be provided, in full, to the government.

CTI shall follow all additional security requirements and shall have each employee sign an affidavid stating that he/she shall be responsible for the security safeguards as stipulated in this section per the RFP.

3.7.1.5.1 Personnel Security Suitability [G.5.6.6.1]

CTI shall follow all personnel security suitability requirements and shall have each individual, as required, complete a background investigation IAW Homeland Security Directive-12, OMB guidance M-05024m M-11-11 and as specified in GSA CIO Order 2100.1I and GSA Directive 9732.1D. CTI understands that background investigations are the responsibility of each CTI Team member.

Data Retention

CTI shall maintain data records for 3 years after final payment under the contract.

3.8 NS/EP FUNCTIONAL REQUIREMENTS IMPLEMENTATION PLAN INTRODUCTION: [L.30.2.8; G.11]

The CTI Team realizes that information technology/communications national policy requirements such as 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 serve to ensure that telecom services are not disrupted in times of national emergency whether it's related to a national disaster or enemy/terrorist attack. Executive Orders (EO) 12472 and 13618 also pertain which describe telecom continuity to selected principal offices that support the President of the United States. The CTI Team will adhere to all stipulations within the governance policies by proving telecom products and services that can:

- Increase survivability and interoperability of NS/EP telecommunications.
- Provide connectivity augmentation for the public switched network (PSN).
- Develop a NS/EP telecommunications architecture that is responsive to the current and future needs of the Federal government via the GSA EIS vehicle.
- Providing and further developing telecommunications technical and procedural standards, and ensure compliance with standards from our suppliers and partners.
- Provide technical and analytical expertise to any member of the Federal government or telecommunications advisory committees and subordinate groups as required and/or requested.
- Provide planning assistance and technical analysis to the Federal Government as required/requested.
- Perform NS/EP telecommunications network performance analysis through the CTI Team partners.
- Ensure interoperability of the various types of telecommunications provided by the CTI Team.
- Develop emergency operations training and exercises or participate with the Federal government in same.

- Develop and manage NS/EP automated systems and capabilities as part of our normal standard operating procedures and SCRM Plans.
- Work with Federal agencies and commercial organizations to anticipate the impacts of disasters on telecommunications for our customers.
- Provide best business practices by analyzing technological advances such in digital cellular, advanced intelligent networks (AIN), commercial satellite technologies, government and consumer products and technologies, and wireless technologies to identify potential impacts on NS/EP telecommunications.
- Coordinate as required with the National Cybersecurity and Communications Integration Center (NCCIC) which integrates the functions of the National Cyber Security Center (NCSC), U.S. Computer Emergency Readiness Team (US-CERT), National Coordinating Center (NCC), and Industrial Control Systems CERT (ICS-CERT) into a single coordination and integration center and co-locates other essential public and private sector cybersecurity partners as described in Sections 3.1 and 3.2.of the National Cyber Incidence Response Plan.

[redacted]

3.8.1 NS/EP FUNCTIONAL REQUIREMENTS IMPLEMENTATION PLAN [G.11.1 – G.11.3]

[redacted]

[redacted]

3.8.2 NATIONAL SECURITY AND EMERGENCY PREPAREDNESS [G.11.1 – 3]

The CTI Team will notify the government immediately when events arise that may have major consequences to its network. The CTI Team understands that the GSA Contacting Officer will set priorities for restoration; and that the CTI Team will work with the priorities set and be solely responsible for network operations required to restore or continue service during a national emergency.

3.8.2.1 Basic Functional Requirements [G.11.1]

The CTI Team will support the following 14 basic functional requirements for NS/EP telecommunications and IT services, which are 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 will be provided preferential treatment over other traffic using priority coding from CTI Team members, which is part of their normal service provision.
2. **Secure Networks:** Networks will have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate. This includes both physical and software//hardware related protection which is provided in conjunction with corporate and Federal policies and procedures.
3. **Non-Traceability:** Selected users will 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 will be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.

5. **International Connectivity:** Voice and data services will provide access to and egress from international carriers.
6. **Interoperability:** Voice and data services will interconnect and interoperate with other government or private facilities, systems, and networks identified after contract award by the government CO.
7. **Mobility:** The CTI Team will provide voice and data infrastructure to support transportable, re-deployable, or fully mobile voice and data communications.
8. **Nationwide Coverage:** Voice and data services will 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 will 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:** Our service will provide voice band service in support of presidential communications.
11. **Broadband Service:** The CTI Team will provide broadband service in support of NS/EP missions (e.g., video, imaging, Web access, multimedia).
12. **Scalable Bandwidth:** NS/EP users will be able to manage the capacity of the communications services to support variable bandwidth requirements.
13. **Affordability:** The CTI Team will leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).
14. **Reliability/Availability:** The CTI Team services will perform consistently and precisely according to their design requirements and specifications, and will be usable with high confidence.

These products and services are provided by using certified and verified supply chain, having a robust team in place that can provide installation and recovery services - which the CTI Team has in place, and a SCRM Plan that reduces/mitigates the chance that inferior products and services are introduced to the customer that could exacerbate the effects of a cyber-attack, natural or man-caused disaster.

3.8.2.2 Protection of Classified and Sensitive Information [G.11.2]

[redacted]The CTI Team realizes that 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 CTI Team may be provided access to certain classified and sensitive materials above the Secret Clear level required for the planning, management, and operations for NS/EP. That information is in various forms, including hardcopy and electronic media. Once identified as classified, the CTI Team will protect such data in accordance with applicable industrial security regulations (National Industrial Security Program Operating Manual [NISPOM] and NSA-approved standards as applicable for Safeguarding Classified Information).

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

The CTI Team will 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), and Wireless Priority Service (WPS) and, when released, Next Generation Network Priority Services (NGN-PS). The CTI Team, as required, will work with the OEC's Communications Portfolio Management (CPM) Branch that collaborates with the public and private sectors to ensure the NS/EP communications community has access to priority telecommunications and restoration services to enable communicate under all circumstances.

3.8.2.3.1 Government Emergency Telecommunications Service [G.11.3.1] [RIN: MMR0131-DN]

The CTI Team will fully comply and interoperate with the GETS service. The CTI Team is aware that the GETS contract is managed by another contractor and as such we have no direct access to GETS. The Government Emergency Telecommunications Service (GETS) is a White House-directed emergency telephone service provided by the DHS OEC and is covered by several national policies including Executive Orders (EO) 12472 and 13618. 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.

3.8.2.3.2 Wireless Priority Service [G.11.3.2]

The CTI Team will ensure WPS calls 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 and the CTI Team will fully comply and interoperate with the WPS 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.

3.8.2.3.3 Telecommunication Service Priority [G.11.3.3]

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). TSP eligibility is restricted to federal, state, local, tribal and territorial stakeholders, as well as private sector organizations with a supporting NS/EP role. Traditionally, qualified organizations are first responders, health care providers, 9-1-1 call centers, and public utility entities. Non-federal users must be sponsored by a federal agency.

The CTI Team will 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 CTI Team will fully comply and interoperate with any future TSP replacement system.

[redacted]

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.