March 31, 2017
RFP #QTA0015THA3003

General Services Administration

Enterprise Infrastructure Solutions (EIS)

Submitted to:
Mr. Timothy Horan
FAS EIS Contracting Officer
1800 F St NW
Washington DC 20405-0001

Volume 2

Management

Final Proposal Revision

MICROTECH

8330 Boone Blvd. Suite 600 Vienna, VA 22182
703-891-1073 (Phone) | 703-891-1074 (Fax)
proposals@microtech.net
DUNS Number: 145454182

This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used, or disclosed—in whole or in part—for any purpose other than to evaluate this proposal. If, however, a contract is awarded to this offeror as a result of—or in connection with—the submission of this data, the Government shall have the right to duplicate, use, or disclose the data to the extent provided in the resulting contract. This restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction.

TABLE OF CONTENTS

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

LIST OF FIGURES

1.0 MANAGEMENT RESPONSE

1.1 Contract Administration Data

Team MicroTech ensures an OCO or an authorized official has the required DPA prior to processing Task Orders (TOs) and we obtain this information from GSA Systems.

1.1.1 *Approach and Capability to Provide User-Friendly, Compliant and Efficient Support Systems*

Team MicroTech provides a contract management approach to meet the requirements set out in each TO, including developing and adjusting baselines, tracking milestones, regular reporting, and standard project reviews. We keep open communication with GSA stakeholders to ensure we meet all standards and expectations.

By focusing on quality, process, and continual improvement, we successfully manage, deploy, and sustain services. We build flexibility into our management structure and have multiple chances for course correction and re-direction.

Team MicroTech fuses the agility and innovation of a small company with the expertise of a highly-competitive established business, translating into a low-risk solution for GSA. Since our inception, we have created and maintained IT services that simplify processes, save time, and expand capabilities.

Team MicroTech refined a disciplined approach to management that emphasizes effective communication and takes maximum advantage of leading practices, methodologies, tools, and lessons-learned to meet client needs and objectives. [redacted] delivery of the EIS Program Tasks is also based [redacted]

[redacted] for a robust approach to manage the technical requirements of multiple tasks at multiple locations.

Our Task Order Management Plan provides proven management control systems, automated tools, quantifiable performance metrics, sound personnel practices, and disciplined administrative processes we use throughout the contract lifecycle.

Team MicroTech meets acquisition objectives by focusing on commercial and standards-based practices. Our integrated approach to business acquisition, staffing, training, and contract administration efficiently applies [redacted] practices across all task orders.

1.1.1.1 Ordering

Team MicroTech's relationships with hardware and software vendors allow us to quickly order any parts required for equipment repair. [redacted]

Delivery Order Process: Team MicroTech applies our established and proven processes to respond and support delivery orders for GWACs and large IDIQs similar to EIS. For this contract, we have a team of professional, trained sales personnel poised to respond to large volumes of RFQs, as we have for contracts such as [redacted] Our delivery order (DO) management process, automated tools, and highly skilled staff enable us to provide a rapid and complete response to GSA customers. **Figure 1** shows our process involves reviews and quality checks at each stage. With our PM as oversight, we resolve issues quickly if they arise, and conduct a post-order review to ensure the customer has received all deliverables within schedule.

[redacted]

Figure 1: MicroTech Delivery Order Process. *Team MicroTech evaluates and responds promptly to all DOs.*

Team MicroTech accepts orders via telephone, fax, e-mail, in person, GSA Advantage, or any other CO requested method. [redacted] We ensure all ordering against this BPA complies with FAR 8.405-3(c) (2).

[redacted] Team MicroTech is prepared to report order status through GSA Advantage, or the agency-specific portal for orders placed through these sites.

GSA equipment purchased under this BPA are shipped F.O.B. destination in accordance with the EIS contract, with evidence of delivery for CONUS and OCONUS locations or as specified in individual delivery orders. [redacted]

Shipping takes place within 30 calendar days or as specified under the GSA Contract from the date an order is received by the Contractor, or as otherwise agreed to by Team MicroTech and the ordering agency. Partial shipments and partial payments are allowed under the BPA, unless otherwise specified in the individual orders.

Team MicroTech agrees to work with GSA on all Task Orders to meet and comply with all ordering requirements.

Team MicroTech understands the Ordering Process and agrees to only accept orders from entities listed in OGP 4800.2I Eligibility to use GSA Sources of Supply and Services.

We agree to follow the following ordering process when making any and all orders.

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

Team MicroTech brings a highly qualified team, a large pool of exceptionally qualified and trained personnel, and a proven management approach that offers a low-risk, best-value solution to meet both current and future challenges. Our approach is outcome-based within a framework that incorporates quality assurance practices into every phase of a task order.

We work with GSA to define performance standards on the contract and adhere to the standards in meeting task order metrics and providing efficient, timely delivery of high-quality work products and professional services. Team MicroTech will comply with the processes, data, and systems requirements to support and maintain TOs as described in Section J.2.3, including the submission of TO summary data and pricing tables, and copies of the complete TO to GSA.

1.1.1.1.1 Fair Opportunity Process

Team MicroTech understands the Fair Opportunity process and agrees to work with the OCO to ensure compliance with the process. Team MicroTech is experienced in competing for and fulfilling Task Orders, as we have for contracts such as NASA SEWP IV, FAA SAVES, USAF NETCENTS, and Army CHESS ITS-SB.

1.1.1.1.1.1 eBuy

Team MicroTech is registered on eBuy and experienced in its use. We monitor, view, and respond to solicitations as necessary or required.

1.1.1.1.2 Task Orders

Team MicroTech is aware that effective Task Order management is critical to the success of this contract, and understands the processes, data, and system requirements necessary to support and maintain Task Orders as described in Section J.2.3. We work with the OCO to comply with the processes of each Task Order.

1.1.1.1.2.1 Ordering

Team MicroTech complies with the Task Order Data Management requirements as contained in RFP Section J.2.3 to include:

- The submission of summary data and pricing tables in original and forwarded copies of complete TOs
- Comply with the processes, data, and systems requirements to support and maintain TOs in accordance with RFP Section J.2.3.

1.1.1.1.2.2 Task Order Award

Team MicroTech understands the role of the OCO as it relates to Task Order awards. The Task Order is not modified after award except by a TO Modification. We adhere to this policy.

1.1.1.1.2.3 Task Order Modification

Team MicroTech understands all Task Order modifications must be executed in accordance with FAR Part 43 and we agree to comply with this regulation. MicroTech complies with RFP Section J.2.3 and reports TO modifications to GSA.

1.1.1.1.2.4 Protests and Complaints

Team MicroTech understands GSA maintains compliance with the FAR in terms of protests with the exception of protests made on the grounds that the order increases the scope, period of performance or maximum value of the contract or if the order is valued in excess of $10 million. We ensure compliance with all protest requirements and understand that complaints, if any, are transacted through the GSA ombudsman. We are familiar with this FAR provision since we are on NETCENTS-2 NetOps ID/IQ, which also operates under the same protest regulations.

1.1.1.1.2.4.1 Fair Opportunity Notice of Protest

In the event Team MicroTech determines it is necessary to protest a fair opportunity decision, we agree to comply with GSA provisions and provide a full un-redacted copy of that protest to the GSA CO within 3 business days of the protest date. In the event of a need to file a FOIA request, Team MicroTech understands a redacted copy must be provided to the GSA CO.

1.1.1.1.2.5 Customer of Record

Team MicroTech fully understands the ordering process established by GSA and supports the three roles GSA serves when customers place orders: 1. GSA acting as customer of record on behalf of another agency; 2. The agency itself acting as customer of record; and 3. GSA acting as an OCO for an agency with the agency remaining as the customer of record.

1.1.1.1.2.6 Authorization of Orders

Team MicroTech understands we may only respond to requests for CBSAs for which we have priced all its required mandatory services or until that time in which said mandatory services have been added to its contract. For optional services, Team MicroTech understands we may respond to a requirement if accompanied by a modification for inclusion of the missing CBSA in accordance with established GSA guidelines. In the event all mandatory services or optional services are not possible, we include a clear notice of the pending modification in our response to the solicitation.

In the event a catalog item is not available, Team MicroTech understands we cannot accept a TO or service order or provision catalog items until the items and discount class are added to the catalog through the submission of a modification proposal to GSA.

1.1.1.1.3 Ordering Services

Team MicroTech agrees to accept orders for service incorporated directly within the TO or placed separately after the issuance of the TO. If an order for service incorporated directly within the TO is missing required data, with the exception of the data required in the TO as specified in Section 1.1.1.1.2, we will accept supplemental information to complete the order.

1.1.1.1.3.1 General Requirements for Ordering Services

Team MicroTech adheres to GSA’s general requirements for ordering services as outlined below in the following sub sections.

1.1.1.1.3.1.1 Agency Hierarchy Code (AHC)

Team MicroTech will reject any order submitted without an Agency Hierarchy Code (AHC) for each line item. We will meet and comply with the AHC requirements as described in in Section J.2.4.1.2.

1.1.1.1.3.1.2 Auto-Sold CLINs

If Team MicroTech's solution to an agency requirement includes services with one or more auto-sold CLINs, as described in Section B.1.2.11, we agree to include those CLINs in the proposal or quote as though they had been expressly requested and ensure they are on the TO. Team MicroTech understands all auto-sold CLINs are listed in all notifications and deliverables associated with an order. Such newly added auto-CLINs will not be applicable to any previously issued TOs unless specifically added via TO modification. After completion of each service provisioning, Team MicroTech will submit a Service Order Completion Notice (SOCN) as described in Section J.2.4 of the Solicitation.

1.1.1.1.3.1.3 Customer Want Date

Team MicroTech makes every reasonable effort to satisfy the Customer Want Date and comply with the requirements regarding Customer Want Dates. We comply with the requirements for SOCN issuance, and that these are not issued nor billing commenced unless specifically authorized.

1.1.1.1.3.1.4 Service Order Completion Notification (SOCN)

Team MicroTech submits a SOCN after completion of each service. We understand all revisions are made through the use of an administrative change order.

1.1.1.1.3.2 Order Types

Team MicroTech follows established procedures for the order types outlined below.

1.1.1.1.3.2.1 Orders for New Services

We understand orders for new services are defined as orders for services not currently provided.

1.1.1.1.3.2.2 Orders to Change Existing Services

Team MicroTech follows procedures for orders to change existing services as outlined below.

1.1.1.1.3.2.2.1 Move Orders

Team MicroTech removes existing services or SREs from one location and re-installs at another location.

1.1.1.1.3.2.2.2 Feature Change Orders

Team MicroTech understands feature change orders are defined as orders that require changes to the features of an existing service as described in Section B, and which fall into two categories: those that require a change to the CLIN being billed and those that do not require a change to the CLIN being billed.

1.1.1.1.3.2.2.3 Disconnect Orders

Team MicroTech understands disconnect orders are defined as orders that require the removal of currently provided services (CLINs). Team MicroTech will accept disconnect orders from agencies at any time. We comply with established procedures for equipment sanitization, as well as waiving the SLA for that service on an order when the time between the order and the customer’s desired disconnect date is greater than the defined provisioning interval for the service as described in Section G.8.2.2. Team MicroTech will stop billing for the disconnected services on the completion date in the SOCN and within the provisioning intervals for disconnects as specified in Section G.8 of the Solicitation. We understand the government automatically stops payment on these orders based on the stated disconnect date and that equipment related to disconnect orders shall be removed within 45 days after the termination of services. In the event 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), Team MicroTech notifies the customer of the full list of associated Unique Billing Identifiers (UBIs) and requests clarification of the customer's intent to only disconnect the specified service. If the customer provides instructions indicating that the list, in whole or in part, is intended for disconnect, we accept this as an order update.

1.1.1.1.3.2.2.4 Administrative Change Orders

Team MicroTech accepts administrative changes to previously provisioned orders. After updating the system, we provide the updated information to GSA as described in Section J.2.4, and understand that changes to administrative data associated with existing services can only occur based on an administrative change order. We understand that administrative data is limited to data provided by the government that does not impact service delivery or pricing. We accept administrative changes to previously provisioned orders. After updating our system, we provide the updated information to GSA as described in Section J.2.4, and that changes to administrative data associated with existing services can only occur based on an administrative change order. We understand administrative data is limited to data provided by the government that does not impact service delivery or pricing.

1.1.1.1.3.2.3 Updates to In-Progress Orders

As an experienced contractor to the federal government, Team MicroTech is accustomed to various change orders across the full spectrum of IT government procurement. Our familiarity with all types of change order requests ensures that we are compliant and responsive when updates to in-progress orders occur. We make revisions to these orders according to the situations listed below and we comply with all update requirements for orders.

1.1.1.1.3.2.3.1 Cancel Orders

Team MicroTech understands the fluid nature of business. We accommodate all necessary cancel order requests at any step of the ordering and delivery process, provided they are received prior to SOCN. We recognize the ever-fluctuating needs of the government, which is why our resource and team panel includes room for error from the government. Our expertise as leading-edge IT product and service providers for the government allows our fully-trained team to serve the government as IT solution experts. [redacted]

[redacted] This minimizes risk for the government [redacted] therefore not losing time in getting products and services to the agency on our schedule.

In the particular case of network access orders for CONUS and OCONUS locations, Team MicroTech understands and accepts that we will not charge any agency for network access orders if the cancellation order was placed 30 or more days before the CWD in the initial order or the firm order commitment date. [redacted] In the event the government's cancellation request does not meet the timeframe and requirements above, we would accept and require a non-recurring charge (NRC). Team MicroTech tries to accommodate all cancellations and makes every attempt and opportunity to wave this fee if our network providers can appropriate the schedule to another contract without loss of funds.

1.1.1.1.3.2.3.2 Location Change Updates

We at Team MicroTech understand the dynamic nature of customer environments that create the need for location changes. As an example, Base Realignment and Closure (BRAC) is just one example of a major source of location changes for the DoD. Team MicroTech is accustomed to procedures which require location change updates. We understand the need for communication, coordination, and synchronization which ensure customer missions are not negatively impacted by a location change. We understand the intricacies of split-base operations and other forms of location change. To minimize redundant operations, we work closely with EIS customers to affect a smooth handover. For location changes that involve significant quantities of services, complex engineering requirements or high priority customers, [redacted]

Impacting LEC Provisioning. In the event a change in service delivery location impacts the LEC provisioning for the network at the locations specified in the change, [redacted]

[redacted] If the new location is serviced by the LEC of another EIS contractor, [redacted]

Not Impacting LEC Provisioning. In the event the service delivery location does not impact the LEC provisioning, Team MicroTech and teammates accommodate the change update with no change in the service delivery or uptime standards.

1.1.1.1.3.2.3.3 Feature Change Updates

In the event an agency requires a feature change to an existing service which does not require a change to the CLIN originally ordered, MicroTech updates the purchase order as necessary, with comments and dates such that the features of the service are enabled at the location and by the date and time agreed upon in the original purchase order. In the event the requested feature change does require a change to the original order CLIN, Team MicroTech does our best to amend the original purchase order and product/service delivery due date. In the event this is not possible, due to substantial feature changes, we may follow our cancel process and re-issue a new purchase order with a priority delivery, thereby reducing changes to the delivery date and time.

1.1.1.1.3.2.3.4 Customer Want Date Change Updates

Team MicroTech understands there are times when agencies request Customer Want Dates (CWD) which essentially denote a priority on a delivery time or order. Team MicroTech makes every attempt to deliver the order updates at or before the CWD, especially if they are within reason and agreed upon timeline for each type of product or service delivery. In the event that the ordering agency delays the CWD prior to receiving the Firm Order Commitment Notice, we do not issue the SOCN and begin billing prior to the new CWD, unless the change is requested less than 14 days before the CWD in the initial order or the firm order commitment date, as specified for each CLIN.

1.1.1.1.3.2.3.5 Administrative Data Change Updates

Team MicroTech's purchase orders allow for the addition or change of administrative data for in-progress orders. For instance, the agency purchaser name or address or phone number may be updated in the BSS and order portal at any time. This administrative data is limited to data which does not impact the delivery location or pricing of the order.

1.1.1.1.3.3 Special Order Handling

1.1.1.1.3.3.1 Telecommunications Service Priority (TSP) Orders

Team MicroTech meets and complies with the requirements for telecommunications service priority orders and follows the telecommunication service priority levels.

1. Provisioning Priority
2. Restoration Priority
3. Restoration of service
4. Expedited service

1.1.1.1.3.3.2 Rapid Provisioning Orders

Team MicroTech acknowledges there are orders in which rapid provisioning of hardware, software, network components, and services are readily available for rapid acquisition and procurement. [redacted] Consistent with the requirements in Section G.3.3.3.2 of the Solicitation, if Team MicroTech proposes specific services for rapid provisioning, we will also propose additional KPIs and SLAs. The rapid provisioning of network availability, or other EIS products and services are within the scope of work identified in the RFP. During our BSS training, Team MicroTech discusses what types of orders and services apply to rapid provisioning.

1.1.1.1.3.3.3 Task Order Projects

At the agency's discretion, on award of the TO, Team MicroTech will prepare a Task Order Project Plan (TOPP). We will 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, Team MicroTech provides the OCO with a single point of contact for service implementation. This ensures 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. We coordinate with the OCO, customers, subcontractors, vendors, and other service providers during the service implementation. We inform the OCO and the LGC on the order when activities, including installation and cutover testing, are scheduled at a building. If we change the installation or activation date, we notify the OCO and provide a revised date.

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

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

- ○ Interim and final configuration to include hardware (type, manufacturer, model), software, special circuit arrangements, environmental and electrical requirements, equipment room layouts, Main/Intermediate Distribution Frame / riser cable diagrams (if needed), and any special design requirements.
- ○ Numbering plan and dialing plan. Identify blocks of telephone numbers, if any that will have to change.
- ○ Interface equipment for CPE, including identification and location of special systems integration requirements.
- ○ A site-specific cutover test plan that describes the contractor's general approach to cutover testing and pass/fail criteria for each service during service implementation as described here and in Section E Inspection and Acceptance.

1.1.1.1.4 Testing and Acceptance of Services Ordered

Team MicroTech complies with all requirements of the testing and verification methodology, which includes the development of an EIS Test Plan with established test scenarios and test cases and providing and EIS Service Verification Testing Report to demonstrate the successful completion of testing. We understand that for the government to approve the test results we must provide FedRAMP certification if cloud services are included in the TO and EIS Testing Report showing each service provisioned works properly according to the KPIs defined in Section C.2 and the acceptance criteria defined in the EIS Test Plan. For each KPI, Team MicroTech will meet specified Acceptable Quality Limits (AQLs) as defined by the government. We will measure and report the KPIs for each unique instance of a service defined at the most granular level to which the KPI is applicable but never at a level higher than that defined by the UBI service grouping (see Section J.2.10.1.1.2). Once verification testing is completed successfully the government may complete acceptance testing based on the acceptance criteria defined in the EIS Test Plan, and the government reserves the right to perform additional tests to confirm proper operation of a delivered EIS service as defined by the TO.

1.1.1.1.5 Performance Management

Team MicroTech complies with all requirements for service provisioning intervals. We will measure the provisioning interval for orders 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.

Team MicroTech acknowledges that for associated services ordered together and assigned UBIs with the same service group ID, the SLA will be governed by the longest-running interval.

Team MicroTech will complete orders within the provisioning intervals defined in the table below (and also shown in Section G.8.2.2.1.1 of the Solicitation) and acknowledges that failure to complete the provisioning of service within the specified timeframes will 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
▪ DS 3 < PLS < OC3	120
VPN Service	45

1.1.1.1.5.1 Individual Case Basis Provisioning SLAs

Team MicroTech understands and acknowledges that certain service provisioning tasks do not have predefined SLAs (see list below). For these services, the performance objective will be defined on an individual Case Basis (ICB) with the required delivery schedule established in the TO. We further understand that failure to complete the provisioning of service within the timeframe specified in the TO will constitute a failure to meet the SLA for that provisioning incident.

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

▪ Web Conferencing (WCS)	

1.1.1.1.5.2 Project Provisioning SLAs

Team MicroTech understands and acknowledges that for project orders (orders that require special treatment by Team MicroTech 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 Team MicroTech at the time orders are placed and confirmed by Team MicroTech. We further understand that, for these services, the performance objective will be defined on an ICB with the required delivery schedule established in the TO and that failure to complete the provisioning of the services within the timeframes specified in the TOPP will constitute a failure to meet the SLA.

1.1.1.1.5.3 Bandwidth on Demand

As more fully described in Section C.2.1.2 of the Solicitation, Team MicroTech will support bandwidth increments and decrements on demand, as agreed between Team MicroTech and the customer agency. Unless otherwise agreed by the agency and Team MicroTech on a case-by-case basis, the provisioning SLA for Ethernet Transport Services: Bandwidth on Demand Changes interval will be 24 hours, measured from the service order to the SOCN.

1.1.1.1.5.4 Service Provisioning SLA Credit Formulas

For each failed SLA, Team MicroTech will apply the associated credit in accordance with Section G.8.4 of the Solicitation using the following formula:

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

1.1.1.2 Billing

MicroTech proposes to invoice in accordance with the following performance billing milestones. Equipment invoiced upon delivery; partial invoicing is acceptable. Enhanced Warranty are billed in arrears. These milestone events are reflected as separate line items in any resulting order. System Integration are invoiced upon completion of milestones. MicroTech submits all invoices electronically for billing to the COR no later than 120 days following the project completion date.

MicroTech will submit accurate billing that meets the performance standards for Billing Accuracy for each TO as defined in Section G.4. We acknowledge that failing to meet the accuracy standards defined in that section constitute failing to meet the Billing Accuracy SLA. If MicroTech fails this SLA, we will apply the associated credit in accordance with Section G.8.4 using the following formula:

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

MicroTech has proven success in billing methods and complying with the requirements of a program. As a recent example, [redacted] included the following key tasks:

- Responsible for providing on-call production support for the organization's billing application.
- Gathered data from multiple systems to analyze quantify and report production issues, primarily issues impacting billing.
- Responsibilities included investigating job failures, fixing the breaks within time frame specified, liaison with support persons within and outside the organization; Responded to user queries, scheduled runs of jobs with the operations staff and worked on systems documentation.
- Participated in 24x7 on call rotation during weekends and evening hours as scheduled.

1.1.1.2.1 Billing Prerequisites

1.1.1.2.1.1 Billing Cycle

MicroTech complies with the Government's billing period running from the first through the last day of each calendar month. We bill the Government in arrears at the end of every month after providing services. All billing is rendered based on calendar month cycles.

1.1.1.2.1.2 Billing Start Date and End Date

MicroTech submits the SOCN to the government prior to billing for the associated service. We agree to comply with all billing start to end date requirements. Unless otherwise specified in the TO, the NRC price billed by MicroTech will be that which is in effect at the time the service order was placed and the MRC will be that which is in effect for the billing month.

1.1.1.2.1.3 90-Day Billing Requirement

MicroTech submits a proper billing invoice for all services up to 90 days after issuance of SOCN including both initial invoicing and billing adjustments. We understand we do not receive payment for a single billing charge or portion of a billing change invoiced after 90 days. We understand the OCO has the authority and discretion to waive the 90-day billing requirement, which applies to both initial invoicing and all billing adjustments, on a case-by-case basis.

1.1.1.2.1.4 Unique Billing Identifier

MicroTech creates and includes a unique billing identifier for each bill and bill components submitted.

1.1.1.2.1.5 Agency Hierarchy Code

MicroTech will meet and comply with the Agency Hierarchy Code (AHC) requirements as described in Section J.2.4 of the Solicitation. MicroTech includes an AHC on all invoices, for each line item in all billing. We understand only those bills that include said AHC are paid by the Government.

1.1.1.2.1.6 Agency Service Request Number

Whenever the Government provides an Agency Service Request Number, MicroTech includes that number in billing throughout the lifecycle of the program. In addition to the billing deliverables described in Section J.2.5 of the Solicitation, MicroTech will input invoice summary data into a designated government system.

1.1.1.2.1.7 Electronic Billing

MicroTech will not submit and we understand that the government will not accept paper invoices except as authorized by the OCO. MicroTech supports the following methods of electronic billing.

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

1.1.1.2.2 Direct Billing

MicroTech bills the agency directly for all charges incurred by an agency and sub agencies in accordance with the TO. We understand the bill is paid by the agency directly to MicroTech, who collects and remits the AGF in its totality, to GSA via EFT, no later than the 15th business day of the following month.

1.1.1.2.3 Billing Functional Requirements

MicroTech complies with the functional requirements listed below and agrees to respond within 7 days of billing inquiry. In addition to the billing functional requirements described herein, Team MicroTech will meet and comply with the processes, data, and systems interface requirements described in Section J.2.5 of the Solicitation.

1.1.1.2.3.1 Adjustments

In the event it is necessary to adjust a bill, MicroTech follows the adjustment process described in Section J.2.5 Billing. We agree to the adjustment to the next available bill, and in the event of a dispute, Team MicroTech understands the established Billing Disputes process applies.

1.1.1.2.3.2 Monthly Billing Informational Memorandum

MicroTech provides a Monthly Billing Informational Memorandum to coincide with the monthly delivery of billing files. The Monthly Billing Informational Memorandum is a list of information that includes items that explain changes in billing, changes to data formats, and new services added to the billing, as well as any issues pertaining to balancing charges.

1.1.1.2.4 Disputes

MicroTech understands the dispute process applies when:

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

MicroTech understands that the GSA CO, OCO, or authorized official may submit a dispute notice to us. We accept and process the government’s disputes and complies with procedures established in Section J.2.6 Billing & Inventory Disputes.

1.1.1.2.4.1 Billing Disputes Resolution

To expedite the resolution of a dispute, MicroTech agrees to follow these steps:

1. MicroTech will resolve billing disputes with the agency that submitted the dispute.
2. MicroTech resolves disputes within 180 days of the dispute notice.
3. In cases where a complete resolution is not forthcoming, MicroTech submits partial resolutions (less than the total amount in dispute) to the agency for acceptance or rejection. Accordingly, the OCO responds within 14 days to the contractor's proposed resolution. Either party may escalate the dispute at any time to the OCO. In cases where MicroTech 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 not resolved within 180 days of the dispute notice or the approved extension time are escalated to the OCO.
5. Disputes escalated to an OCO are resolved in accordance with FAR 52.233-1 (Disputes).
6. Once a dispute is resolved, MicroTech processes 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. MicroTech provides a monthly Dispute Report (DR) in accordance with Section J.2.6 Billing & Inventory Disputes.
8. Upon dispute resolution, MicroTech will submit corrected billing on the next available bill.

1.1.1.2.5 Payment of a Bill by the Government

MicroTech understands the importance of following the ordering, billing and payment procedures and we are only paid for items and services issued, delivered, and accepted in accordance with ordering, billing and payment procedures established in Section H.32. MicroTech understands at the expiration of the contract or TO we submit a final billing invoice within 90 days unless granted an extension in writing by the OCO.

1.1.1.2.6 Associated Government Fee

MicroTech agrees to collect the associated government fee monthly throughout the lifecycle of the project, and remits the same to GSA via EFT no later than the 15th business day of the following month.

1.1.1.2.7 Electronic Funds Transfer

MicroTech accepts payment via Electronic funds transfer and provides all necessary information to facilitate said payments.

1.1.1.2.8 Government Purchase Card Payments

MicroTech accepts payment via government purchase cards authorized by the Government for telecommunications purchases under this contract and establishes all necessary financial procedures with our financial institution. MicroTech will coordinate with our bank to obtain the appropriate Standard Industrial Classification code for the services provided under the contract and establish our Government Purchase Card financial procedures with our financial institution to ensure acceptance of such payments for billing.

1.1.1.2.9 Rounding of Charges for Billing and AGF

MicroTech rounds all billing in accordance with GSA established procedures.

1.1.1.2.10 Proration of Monthly Charges

MicroTech supports the following proration types:

- Month-Length Proration, as defined in Section J.2.5.1.5.1.1 of the Solicitation
- Normalized 30-Day Month Proration, as defined in Section J.2.5.1.5.1.2 of the Solicitation.

MicroTech will select the proration type in the TO. If the TO does not specify a proration type, we will implement Month-Length Proration. We will implement and use the selected proration type for each TO at no cost to the Government.

1.1.1.2.11 Taxes, Fees and Surcharges

1.1.1.2.11.1 <u>Separate Billing of Taxes, Fees and Surcharges</u>

MicroTech separates billing of taxes, fees, and surcharges, and these are included as individual components or amount on the BI, whether and original charge or an adjustment. If an agency decides to request prices inclusive of these items in its solicitation, we bill the prices proposed, accepted, and included in the TO.

1.1.1.2.11.2 Aggregated Taxes

MicroTech includes the aggregated tax for each line item in the billing invoice and provides detail of the aggregated tax deliverable in accordance with GSA established procedures.

1.1.1.2.12 Billing Performance Objectives

MicroTech submits accurate billing that meets the following objectives:

- All applicable data elements are included on the BI in accordance with Section J.2.10 Data Dictionary.
- The BI have an associated SOCN for each order.
- The information on the BI are consistent with that on the SOCN.
- There are no duplicate records within the BI.
- There are no records within the BI that represent charges being billed more than 90 days after the issuance of the SOCN unless waived (applicable to both initial invoicing and all billing adjustments).
- The price matches the price(s) on the contract or TO.

1.1.1.2.12.1 Billing Data Accuracy Key Performance Indicator

MicroTech maintains the acceptable quality level of billing key performance indicator for Billing Data of 95%.

1.1.1.2.12.2 Billing Charges Accuracy Key Performance Indicator

MicroTech maintains the acceptable quality level of billing key performance indicator for billing charges of 95%.

1.1.1.3 Business Support Systems

1.1.1.3.1 Overview

In today’s business environment, one cannot afford to spend time worrying about communications service issues–nor to wait for customer service when issues arise. Team MicroTech helps maximize productivity and avoids unnecessary downtime by providing responsive personal support and answers to all account questions from a dedicated Service Assurance Manager to a dedicated and prepared team. We provide planned service events through proactive monitoring. We provide our very best in personalized communications service and support and including direct access to a highly skilled customer support team.

1.1.1.3.2 Technical Requirements

1.1.1.3.2.1 Web Interface

Team MicroTech's platform provides [redacted]

1.1.1.3.2.1.1 Web Interface Functions

Team MicroTech's platform provides [redacted] At a minimum, Team MicroTech's web interface will support the following functions (see Section G.5.4 of the Solicitation for function explanations and references):

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

Team MicroTech understands that the government highly desires all other functions described in Section G.5.4 of the Solicitation. Though not required, we will add as many Section G.5.4 functions as possible for the government's convenience and ease of use.

[redacted]

1.1.1.3.2.1.2 Technology Standards

Team MicroTech's web interface [redacted] We support the following products.

- Microsoft Internet Explorer/Microsoft Edge (desktop and mobile).
- Google Chrome (desktop and mobile).
- Mozilla Firefox (desktop and mobile).
- Apple Safari (desktop and mobile).

1.1.1.3.2.1.3 Accessibility

[redacted] We will 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. We will also identify the technical standards applicable to all products proposed. Team MicroTech will clearly indicate the location(s) where this list of technical standards and full details of compliance can be found (e.g., an exact webpage location). We will ensure that this list is available on Team MicroTech's website(s) within 30 days of Notice to Proceed (NTP).

Team MicroTech will ensure all EIT products that are less than fully compliant are offered pursuant to extensive market research, which ensures that they are the most compliant products available to satisfy the solicitation's requirements. If any EIT product proposed is not fully compliant with all the standards, we will 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.

Team MicroTech will make the BSS Voluntary Product Accessibility Template (VPAT), as contained in ITIC website, available on our website and will directly address compliance with Section 508 with the following deliverables:

- BSS Development and Implementation Plan
- BSS Verification Test Plan

- BSS Verification Test Results

1.1.1.3.2.2 Direct Data Exchange

Team MicroTech's platform provides simultaneous transaction data to required destinations and delivers reporting to secure/definable sites. The system is [redacted] Team MicroTech's BSS will include secure, automated mechanisms for direct transfer of detailed transaction data to GSA Conexus. We understand this data will cover all elements detailed in Section G.5.4 of the Solicitation.

1.1.1.3.2.2.1 Direct Data Exchange Methods

Team MicroTech's platform provides simultaneous transaction data to required destinations and deliver reporting to secure/definable sites. Our BSS will accept data transfers from the government and submit data to the government in the formats specified in Section J.2.9 of the Solicitation. The system is [redacted]

1.1.1.3.2.2.2 Direct Data Exchange Formats

Team MicroTech's platform accepts and submits data transfers via email, GSA systems, attachment via direct data exchange, our web interface, or other methods agreed to or required by the task order.

1.1.1.3.2.2.3 Direct Data Exchange Governance

Team MicroTech does not make any changes to the data exchange formats or methods without government approval and we agree to follow established change processes.

1.1.1.3.2.3 Role Based Access Control (RBAC)

Team MicroTech collects user registration and RBAC information from the customer. We will use this information to setup access control on the BSS in accordance with Section J.2.3 of the Solicitation.

1.1.1.3.2.4 Data Detail Level

Team MicroTech submits reports in both Human Readable and Machine Readable formats. We will ensure that all data provided by the BSS will be sufficiently detailed to provide all data elements relating to the services listed in Section G.5.4 as addressed in Section J.2 of the Solicitation.

1.1.1.3.3 BSS Component Service Requirements

MicroTech complies with all BSS Component Service Requirements as listed in G.5.4.1.

1.1.1.3.4 BSS Development

MicroTech has included our BSS Development and Implementation plan in Section 3.0. We provide upgrades to it at no additional cost to the Government as upgrades become available.

1.1.1.3.4.1 BSS Change Control

MicroTech provides 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 notify the Government as soon we discover a change is required.

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

- Obtain government approval before implementing the change.
- Use industry-standard change control procedures.
- Train government personnel if required.
- Retest with the government to ensure functionality continues to meet requirements.
- Update all relevant service documents and information posted on our website(s) as necessary, at no additional cost to the government and within 7 days of completing the change.

1.1.1.3.5 BSS Security Requirements

Team MicroTech ensures security requirements are met in accordance with our BSS System Security Plan. We will support the Government’s efforts to verify that these standards are being met.

1.1.1.3.5.1 General Security Compliance Requirements

Team MicroTech complies with all current security requirements and regulations. To date, we have not encountered any security lapses within the regulations identified within the solicitation. Team MicroTech will comply with Federal Information Security Management Act (FISMA) guidance and directives to include Federal Information Processing Standards (FIPS), NIST Special Publication (SP) 800 series guidelines,

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

GSA IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of government IT.

1.1.1.3.5.2 GSA Security Compliance Requirements

Team MicroTech complies with all GSA security requirements and regulations. We submit our BSS System Security Plan in accordance with NIST SP 800-37.

1.1.1.3.5.3 Security Assessment and Authorization (Security A&A)

Team MicroTech maintains a valid security A&A and understands that not doing so is grounds for termination of the contract. We conduct a new security A&A at least every 3 years, or when there is a significant change that impacts the system's security posture.

1.1.1.3.5.4 BSS System Security Plan (BSS SSP)

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

- Security Assessment Boundary and Scope Document (BSD)
- We develop and maintain Interconnection Security Agreements (ISA) in accordance with NIST SP 800-47.
- We develop and maintain a GSA NIST SP 800-53 R4 Control Tailoring Workbook. Column E of the workbook titled "Contractor Implemented Settings" will document all Team MicroTech-implemented settings that are different from GSA-defined settings, and where GSA-defined settings allow Team MicroTech to deviate from the same.
- We develop and maintain a GSA Control Summary Table for a Moderate Impact Baseline as identified in GSA IT Security Procedural Guide 06-30, "Managing Enterprise Risk."
- We develop and maintain a Rules of Behavior (RoB)

- We develop and maintain a System Inventory that includes hardware, software and related information as identified in GSA IT Security Procedural Guide
- We develop and maintain a Contingency Plan (CP) including Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA) completed in agreement with NIST SP 800-34.
- We develop and maintain a Contingency Plan Test Plan (CPTP)
- We test the CP and document the results in a Contingency Plan Test Report (CPTR)
- We perform a Privacy Impact Assessment (PIA)
- We develop and maintain a Configuration Management Plan
- We develop and maintain a System(s) Baseline Configuration Standard Document
- We develop and maintain System Configuration Settings
- We develop and maintain an Incident Response Plan (IRP)
- We test the IRP and document the results in an Incident Response Test Report (IRTR)
- We maintain system security through continuous monitoring of security controls of the our system and its environment of operation
- We develop and maintain a Plan of Action and Milestones completed in agreement with GSA IT Security Procedural Guide 06-30, “Plan of Action and Milestones (POA&M).”
- All FIPS 199 Low, Moderate and High impact information systems complete an independent internal and external penetration test and provide an Independent Penetration Test Report documenting the results of vulnerability analysis and exploitability of identified vulnerabilities with the security assessment package and on an annual basis
- All FIPS 199 Low, Moderate, and High impact information systems conduct code analysis reviews in accordance with GSA CIO Security Procedural Guide 12-66 using the appropriate automated tools (e.g., Fortify, Veracode, etc.) to examine for common flaws, and document results in a Code Review Report to be submitted prior to placing system into production, when there are changes to code and on an annual basis.
- The government provides the Security/Risk Assessment and Penetration Tests. We allow GSA employees (or GSA-designated third-party contractors) to conduct security

A&A activities to include control reviews in accordance with NIST SP 800-53 R4/NIST SP 800-53A R4 and GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.”

- All identified gaps between required 800-53 R4 controls and Team MicroTech implementation as documented in the Security/Risk Assessment Report (SAR) are tracked.
- Team MicroTech mitigates all security risks found during the security A&A and continuous monitoring activities.
- We deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26, “FISMA Implementation.”
- Team MicroTech develops and keeps current all policy and procedures documents, as outlined in the specified NIST documents as well as appropriate GSA IT Security Procedural Guides.
- Team MicroTech will develop and maintain a System Inventory that includes hardware, software and related information as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk”
- Team MicroTech will develop and maintain a Contingency Plan Test Plan (CPTP) completed in agreement with GSA IT Security Procedural Guide 06-29, “Contingency Planning Guide”
- Team MicroTech will provide a CPTP for the information system with the initial security A&A package to include annual updates.
- Team MicroTech will test the CP and document the results in a Contingency Plan Test Report (CPTR), in agreement with GSA IT Security Protocol Guide 06-29, “Contingency Planning Guide”.
- Team MicroTech will provide a CPTR for the information system with the initial security A&A package to include annual updates.
- Team MicroTech will perform a Privacy Impact Assessment (PIA) completed as identified in GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk”.
- Team MicroTech will provide a PIA for the information system with the initial security A&A package to include annual updates.

- Team MicroTech will develop and maintain a Configuration Management Plan (CMP) (Reference: NIST SP 800-53R4 control CM-9; NIST SP 800-128; GSA CIO-IT Security 01-05).
- Team MicroTech will provide a CMP for the information system with the initial security A&A package to include annual updates.
- Team MicroTech will develop and maintain a System(s) Baseline Configuration Standard Document (Reference: NIST SP 800-53 R4 control CM-2; NIST SP 800-128; GSA CIO-IT Security 01-05).
- Team MicroTech will provide a well-defined, documented, and up-to-date specification to which the information system is built.
- Team MicroTech will provide the System Baseline Configuration for the information system as a part of the CMP and will submit the same with the initial security A&A package to include annual updates (Reference: NIST SP 800-53 R4: CM-9)
- Team MicroTech will develop and maintain System Configuration Settings (Reference: NIST SP 800-53 R4 control CM-6; NIST SP 800-128; GSA CIO-IT Security 01-05).
- Team MicroTech will establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements.
- Team MicroTech will configure systems in accordance with GSA technical guides, NIST standards, Center for Internet Security (CIS) guidelines (Level 1), or industry best practices in hardening systems, as deemed appropriate by the AO.
- Team MicroTech will include system configuration settings as part of the Configuration Management Plan and will update and/or review same on an annual basis.
- Team MicroTech will develop and maintain an Incident Response Plan (IRP) (Reference: NIST SP 800-53 R4 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”).
- Team MicroTech will provide an IRP for the information system with the initial security A&A package to include annual updates.
- Team MicroTech will test the IRP and document the results in an Incident Response Test Report (IRTR) (Reference: NIST SP 800-53 R4 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02 “Incident Response”).

- Team MicroTech will provide an IRTR for the information system with the initial security A&A package to include annual updates.
- Team MicroTech will develop and maintain a Continuous Monitoring Plan to document how continuous monitoring of the information system will be accomplished.
- Team MicroTech will provide a Continuous Monitoring Plan for the information system with the initial security A&A package to include annual updates.
- Team MicroTech will perform all scans associated with the POA&M as an authenticated user with elevated privileges.
- Team MicroTech will manage and mitigate vulnerability scanning results in the POA&M and will submit the results together with the quarterly POA&M submission. We will ensure that scans include all networking components that fall within the security accreditation boundary.
- Team MicroTech will provide a POA&M for the information system as part of the initial security A&A package followed by quarterly updates.
- Team MicroTech will ensure that all identified gaps between required 800-53 R4 controls and our implementation as documented in the Security/Risk Assessment Report (SAR) are tracked by Team MicroTech 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).
- Team MicroTech will mitigate all critical and high-risk vulnerabilities within 30 days and all moderate risk vulnerabilities within 90 days from the date vulnerabilities are formally identified.
- Team MicroTech will provide updates on the status of all critical and high vulnerabilities that have not been closed within 30 days. This report will be provided on a monthly basis.
- Team MicroTech will verify and review the following documents during the initial security assessment and provide updates to the GSA COR/ISSO/ISSM biennially:
  - Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1).
  - Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1).
  - Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1).

  - Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1).
  - Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1).
  - Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1).
  - Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1).
  - Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1).
  - System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1).
  - Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1).
  - Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1).
  - Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1).
  - Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1).
  - Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1).
  - Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 R4: SA-1).
  - System and Communication Protection Policy and Procedures (NIST SP 800-53 R4: SC-1).
  - System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1).

1.1.1.3.5.5 Additional Security Requirements

Team MicroTech is responsible for these privacy and security safeguards:

- We do not publish or disclose in any manner, without the CO’s written consent, the details of any safeguards either designed or developed by Team MicroTech under this contract or otherwise provided by the government (except for disclosure to a consumer agency for purposes of security A&A verification).
- We provide the government logical and physical access to our facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request.

1.1.1.3.5.5.1 Personnel Security Suitability

All personnel with access to government information complete a background investigation.

1.1.1.3.6 Data Retention

Team MicroTech complies with FAR Subpart 4.7 (48 CFR 4.7) to maintain an archive of all records for 3 years after final payment under the contract. Where appropriate, Team MicroTech 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.

1.1.1.4 Service Assurance

MicroTech’s reliable, high quality, customer-driven technical support staff consistently deliver innovative technology, technical services solutions, and excellent customer service. We provide flexible, effective solutions that exceed our clients’ expectations. MicroTech’s adherence to structured quality management methodologies ensures we manage large tasks while maintaining the flexibility and rapid decision-making of a small business. MicroTech has a proven record of accomplishments and repeat customers who rely on our consistent record of delivering solutions on-time, within budget, and at the highest quality standards.

Since our inception, MicroTech has created and maintained IT services that simplify processes, save time, and expand capabilities. We understand GSA systems and goals. Insights gained from working on previous initiatives inform our culture and enhance our capabilities, creating a process that is focused and innovative.

MicroTech is experienced in setting up and running customer support offices. For instance, MicroTech currently has a customer support office for the [redacted] [redacted] We provide customer service support from 8:00 a.m. to 8:00 p.m. EST, Monday through Friday, by staff familiar with and knowledgeable of the [redacted] We can expand our customer service infrastructure to provide support to GSA under this procurement and we are prepared to do so.

MicroTech currently supports the approximately 200 users of the [redacted] through a broad range of technical services and support. MicroTech leads efforts to create requirements and specifications for complex or highly technical Web applications. We research, analyze, and create application designs for complex web projects. We assist in estimating programming resource requirements, project planning, and scheduling. We code, develop, and test web applications using standard toolsets, and robust edit and error checking processes. We design and develop projects with professional level standards for site performance, usability, scalability, browser compatibility, and reliability. We review designs, maintaining compliance with application and infrastructure architecture and security. We provide technical expertise in evaluating, designing, integrating, and managing computer hardware, system software, operating systems, database management systems (DBMS), and customized software products. We perform overall web design, application development, and integration of web sites. We manage and support Oracle and SQL database administration, Microsoft Windows, and web server administration.

Our customer service approach is collaborative, cohesive, and fully focused on the GSA and its customers. Team MicroTech communicates often with GSA to provide unparalleled program support through its established program management office. Our Program Management Office (PMO) quickly and effectively responds to and supports each customer request. MicroTech employees assigned to the PMO are knowledgeable in Federal Government purchase procedures in general and specifically in processes tailored to the GSA and this BPA.

MicroTech knows how to manage major programs and is prepared to implement the same administrative processes and functions to support the GSA EIS program. These functions include resource management, communications management, financial management, risk management, and quality management, which we use successfully on other programs.

1.1.1.4.1 Customer Support Office

MicroTech identifies the structure of the Customer Support Office. The CSO supports the sales, service and implementation activities with the government. The CSO is set up to communicate with government users of the contract around the world using common means of communications including toll-free number, email, and collaboration tools.

The CSO provides tech support and training as required and makes sure Customer Service Representatives are available to users for requirements planning or billing reconciliation.

1.1.1.4.2 Customer Support Office and Technical Support

Team MicroTech maintains a Customer Support Office including a main toll-free telephone number and primary email address. We have all functional areas of the CSO fully operational within 30 days of NTP. Services provided by our CSO include:

- Facilitate the government's use of the contract.
- Provide contact information for each functional area of the CSO.
- Respond to general inquiries.
- Provide information regarding available products and services, respond to service inquiries, and accept orders.
- Provide training registration and scheduling information.
- Respond to inquiries via the same method the user used to access the CSO, unless otherwise specified by the user.
- Provide a main US toll-free telephone number through which all CSO functional areas can be accessed.
- Provide the capability for non-domestic users to contact the CSO without incurring international charges and minimize, to the extent possible, the different CSO contact numbers required to support non-domestic users.
- Provide hot-links from the contractor's public EIS website(s) to CSO functional area email addresses.
- Provide Telecommunications Device for the Deaf (TDD) access to the CSO for government representatives who are hearing impaired or have speech disabilities.
- Deal effectively with the geographical distribution of EIS subscribing agencies, GSA's Program Management Offices (PMOs) in the GSA regions, and GSA international activities.
- Provide responses to user inquiries of a general nature such as the contractor's established administrative and operational procedures, contractor points of contact, and user forum information.
- Provide information on available training classes as well as guidance and assistance with registration for training classes. Training requirements are described in G.10 Training.

- Provide technical support to agencies and the PMO regarding the services the contractor delivers to the government.
- Answering questions related to how users can obtain functions designed into the services we provide via the contract.
- Advising users on the capabilities incorporated into services features.
- Providing technical support to assist either our technicians or the agencies or other organizations or personnel in the timely resolution of troubles.
- Notifying users of new services and features that are planned or that have recently been added to the contract.
- Providing ordering and tracking support services.
- Providing support to help resolve billing issues.

1.1.1.4.3 Trouble Ticket Management

We respond to trouble calls for our clients within 15 minutes of the report(s). [redacted] We analyze and repair or report as non-functioning all inventory items. [redacted] We update inventory. In coordination with the Government, we track the status and location of items under warranty, and place them back into a ready status within 24 hours of the item's return and test.

We maintain accurate computer-related software and hardware trouble logs in electronic format, using the client's preferred ticketing system. MicroTech provides records to the Government's SharePoint site within 2 days of repair completion. By maintaining processes and updating trouble call documentation, we track the inventories of spare parts, note trends in repairs, faults, and failures, and proactively test and replace parts to reduce failures during training activities.

When a trend suggests an avenue for improvement, we document the analysis for review and action. For example, MicroTech's PM at the [redacted] conducted an extensive trend analysis to determine ways daily operations could run more efficiently. [redacted]

Team MicroTech uses industry best practices to perform trouble ticket management.

1.1.1.4.3.1 Trouble Ticket Management General Requirements

Team MicroTech understands the government's priority for online real-time access to trouble ticket areas for service issues. Our trouble ticket management system operates like any of our multitude of Help Desk trouble ticket contracts operating on a 24x7x365 basis. As with all technology, service issues occur. At the onset of discovered service issues, whether they be caused by weather or other forms and types of outages, we create a trouble ticket on our online trouble ticket portal, which may be accessed 24x7x365. Our finalized procedures for creating and responding to trouble tickets are approved by the government on award and as we approach roll-out of products and services. However, we offer this example as a demonstration: Once a trouble ticket is entered into the system, we implement our practiced and proven response methodologies. [redacted]

1.1.1.4.3.2 Reporting Information

Team MicroTech provides 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. We deliver archived trouble and complaint report data within 5 days of the request for such information.

1.1.1.5 Inventory Management

1.1.1.5.1 Inventory Management Process Definition

Team MicroTech maintains an ongoing and accurate inventory and we 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.

1.1.1.5.1.1 <u>Inventory Management Functional Requirements</u>

Team MicroTech meets the requirements of the EIS program to manage our inventory and we agree to populate the records of the EIS services within 1 business day of the issuance of SOCNS for services.

1.1.1.5.1.2 <u>EIS Inventory Maintenance</u>

Team MicroTech maintains and updates the EIS inventory for all customer services as well as the current view so as to indicate all additions, deletions, and changes within 1 business day of the issuance.

1.1.1.5.1.3 <u>EIS Inventory Data Availability</u>

Team MicroTech complies with all government requirements for Inventory Data availability. We ensure the government users have secure electronic access to the current view and monthly snapshots of our inventory.

For queries regarding the EIS inventory, Team MicroTech provides options to select a user choice of online viewing, data file downloading and we provide and maintain a web interface line for secure electronic access to our inventory information. We also support common industry standard formats and file structures and there is no limit on the number of records.

Older monthly snapshots of the EIS inventory are available within 5 days of a government request and we retain the monthly snapshots and provide them upon request for 3 years following the end of the contract. Team MicroTech does not place any use restrictions for three years following the end of the contract.

At no expense to the Government, Team MicroTech provides copies of records, monthly snapshots, inventory records in the format requested by the Government.

1.1.1.5.1.4 EIS Inventory Data Discrepancies and Accuracy

1.1.1.5.1.4.1 EIS Inventory Data Discrepancies

Team MicroTech investigates any EIS inventory discrepancy and makes necessary corrections within 10 days of query. In the event there is a disagreement regarding the correction, we advise the Government and work to resolve the discrepancy and escalate to the CO for resolution as necessary to the Government's satisfaction. When Team MicroTech 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, we will 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.

1.1.1.5.1.4.2 EIS Inventory Data Accuracy

Team MicroTech institutes internal verification and audit procedures to ensure that the EIS inventory is complete and correct. If we discover an inventory data discrepancy, or an error in the EIS inventory data elements in the SOCN issued to the government, we generate a government report of the discrepancy and will issue a corrected SOCN or a new correct SOCN that clearly references the original error at no additional cost to the Government.

If the EIS inventory data elements result in a billing error in the BD deliverable issued to the Government, we issue, at no additional cost to the Government, a Billing Adjustment (BA) deliverable. We agree to correct data discrepancies as they occur within 10 days.

1.1.1.5.1.5 EIS Inventory Reconciliation

Team MicroTech provides the monthly IR deliverable as defined in Section J.2.7.

1.1.1.6 Service Level Management

Team MicroTech will be responsible for meeting all SLA requirements, and measuring each SLA, as defined in Solicitation Section G.8.3.2. We will measure each SLA in accordance with its definition provided in Section G.8.2. We will describe procedures for measuring and sampling in the quality assurance section of the Program Management Plan, described in Section G.9.4. MicroTech designates a single interface for Service Level Management and resolves all issues such as missing data, data reporting in incorrect format, timeliness of submission, including those pertaining to subcontractors as defined in Section G.9.2. We describe procedures for measuring and sampling in the quality assurance section of the Program Management Plan (Section 2.6). We use service level management to align business needs with IT services with a goal of successfully delivering and improving services. We have considerable experience working under SLAs. In many cases we introduced and established new SLAs with our customers as an integral component of our [redacted] We report on the Networks, Groups, Servers, and Functional Units performance against the prescribed SLAs in the contract. All SLAs are entered into the service desk and tracked continuously and reported weekly. Team MicroTech provides SLA reports on SharePoint to keep management apprised of trends and activities with drill-down capability. We will provide SLA Reports that comply with requirements in accordance with Section G.8.5, and unless otherwise specified, Team MicroTech will ensure each report is TO-specific and addresses only those actions and metrics applicable to the TO in question. As specified in Section G.5, we will submit all reports electronically via our web interface and via direct data exchange.

1.1.1.6.1 Report Definitions

1.1.1.6.1.1 <u>Service Level Agreement Report (SLAR)</u>

Team MicroTech will generate a Service Level Agreement Report (SLAR) that documents monthly SLA performance covering all aspects of service including incident-based SLAs, service-specific SLAs, service-provisioning SLAs, and billing accuracy SLAs. Report content will be as defined in Section J.2.8 of the Solicitation. Team MicroTech will deliver this report on the 15th day of each month.

1.1.1.6.1.2 <u>SLA Credit Request (SLACR) Response</u>

Team MicroTech will document our response to a government request for SLA credits through a SLA Credit Response (SLACR). Our Response contents are defined in Section J.2.10 of the Solicitation. We will deliver this report to the government within 30 days after the receipt of an SLACR. In those cases where MicroTech does not meet the defined contractual or TO SLA, MicroTech will provide credits and/or adjustments to the government agency of record or GSA.

1.1.1.6.1.3 Trouble Management Performance Summary Report

Team MicroTech will document trouble management performance by summarizing the number of trouble reports opened and resolved during the reporting period. Unless otherwise specified by the TO, we will use our standard commercial report format that will contain the specified information. We will deliver this report to the government within 14 days after the end of each FY quarter.

1.1.1.6.1.4 Trouble Management Incident Report

Team MicroTech will document our trouble management incident-level performance by describing each trouble report issued during the reporting period. The report will contain our trouble report number; agency; and AHC, UBI, time opened, and time resolved. Unless otherwise specified by the TO, we will use our standard commercial report format that will contain the specified information. We will deliver this report to the government within 14 days after the end of each FY quarter.

If Team MicroTech does not meet specified service levels, we will issue specified credits as defined in any contract arising out of this Solicitation. In cases where Team MicroTech does not meet the defined contractual or TO SLA, we will provide credits and/or adjustments to the government agency of record or GSA.

1.1.1.7 Training

Team MicroTech offers our understanding and ability to meet the training requirements for the EIS BSS Web portal. The paramount importance is that the government fully understands the functionality of the EIS BSS Web portal, and how to navigate that portal for order submission, trouble ticketing, inventory management, billing processes, electronic billing/Web Vendor, and invoice processing platform, billing disputes and resolution, and billing entry and submission forms.

Below, we outline the various methods by which we conduct EIS BSS Portal Training, such as: instructor led classroom training, distance learning, online web-based/self-paced learning, and interactive video. Additionally, we outline our Draft Training plan, curriculum, and training evaluation methodologies. We provide training at no additional cost to the government.

1.1.1.7.1 Instructor Led Classroom Training

MicroTech HQ Training: MicroTech, headquartered in Vienna, VA, has a state-of-the-art training center located in a LEED-Silver certified building with an Energy Star Score of 86, Wired-certified Silver. The building was awarded an Energy Star label in 2015 for its operation efficiency. This means the government accesses training and equipment in a facility which provides equipment with high energy ratings. We offer these energy ratings at no additional cost to the government, and without any network or technical degradation while on site. We provide training in our HQ facility for 40-50 personnel. In the event of large training (40+) requiring secured access, we permit these on a rotating basis, in coordination with the government. If a training does not require secured access, our building provides space to tenants, which holds 100+ participants. In the event of an extremely large training, 100+, we provide a staggered training approach. The reduction of class size assists in our ability to answer questions and promote a dialogue with the trainers and participants. When training is offered at MicroTech's HQ (whether it be in our official training room or on-site room), we provide all training materials, available by our secure server or secured hot spot for the day(s) required. We allow plenty of bandwidth (notwithstanding streaming video or audio for individual attendants). Our training center has an overhead projector and interactive screen, allowing for dynamic learning environments. Our technical team, financial team, and business team are all in attendance for the BSS training. Our EIS training, equipment, and environmental/network support is offered at no cost to the government.

Government Site Training: As the situation may arise, Team MicroTech personnel are available to attend any government-provided training center or location with the same training curriculum or customized brown-bag on or relating to our BSS. We take the opportunity one day prior to training to troubleshoot the rooms and equipment with the agency Help Desk professionals such that on-site training runs smoothly and with reduced delay to government personnel.

1.1.1.7.2 Distance Learning

In the event on-site training is not permissible, we have VTC capabilities at our HQ with web cameras, which allow for participants with end-user networks compatible of streaming video to "attend" the live training at anywhere in the world. Similar to our other VTC ventures, our Training moderators can screen questions from the Web from people attending the class and submitting questions to the demonstrators.

1.1.1.7.3 Online Web-based Training/Self-paced Training

Team MicroTech is experienced in Online Web-based Training and Self-paced Training. For instance, our HR department launches at a minimum, company-wide self-paced training with interactive modules and questions with forms and regurgitation of information such that information is dispersed to the end-user and available for completion within a certain timeframe. Our training has cross-browser compatibility on Microsoft Internet Explorer/Microsoft Edge, Google Chrome, Mozilla Firefox, and Apple Safari. Our QA process on these browsers is ongoing. If there is an issue, these are reported to us and we fix them as they arise.

1.1.1.7.4 Interactive Video

Similar to the See Something, Say Something IA Training through Department of Homeland Security (http://cdsetrain.dtic.mil/itawareness/), we enable interactive video training through recorded videotaping of our first few trainings and then supplementing the video with quizzes throughout the segments, ensuring the information is understood by our end-users. These segments in between the video portions are 508 compliant, as required by the GSA.

1.1.1.7.5 Other Remote Training Methodologies

Team MicroTech provides other training methodologies, such as Brown Bag Meetings, where new hires or small group demonstrations require instruction on a particular element of the portal, back-to-basics, or when a new feature or iteration requires a short, or informational training, which takes place over a period of hours as opposed to a full training. We can meet at our HQ or on government facilities. Brown Bag Training allows us to delve into a particular issue with a set of people at an agency. By having a smaller dynamic (~15 participants), we can answer more questions and offer more personalized training.

1.1.1.7.6 Other Methods Specified by the Government

In the event other training demonstrations are required by the government, such as an annual EIS BSS Portal Refresher training, we accommodate by repurposing our coursework materials and custom tailoring a type or topic of training to any audience, as specified by the government. We're readily available to provide any coursework or materials which best meet the governments' needs.

1.1.1.7.7 Draft Customer Training Plan

Team MicroTech's proposed draft training plan affects all users of the EIS BSS Portal and resulting services: COs and CORs, end-users of services, government trainers, and government executives. Our Draft Customer Training plan (once finalized) is available on our portal throughout the entire life of the contract. In the event there are multiple iterations of the portal (given updated technology, or purchase methods, etc.) these documents are revised and the newest iteration is available on our portal.

The curriculum for the trainings covers full scope and use of the EIS BSS Portal. Upon the notice to proceed, Team MicroTech provides the government full documentation for comments and approval, and the revised/final Training Plan within 15 days after the comments are received.

Our Training Mangers, technical designers/developers, and other training personnel work with an in-house technical writer and a graphics specialist to develop our training materials and course PowerPoints/interactive materials for the EIS BSS Portal. We create curricula based on other topic-oriented trainings we have completed.

Once we have the go-ahead from the government, we enroll all members requiring training into our queue, and add their user names to the back end of our portal such that when our rollout training occurs, we are able to have the trainings across the organization as soon as the site is live. We concurrently offer in-person training as well as Webinars and Demonstrations through our FAQ/Training page on the Portal such that those unable to attend training due to any project issues, might still be able to receive the content. Everyone using the portal is required to attend at least one type of vital training to reduce risk to the government and ensure an even-footing across agencies. If there is a reason someone cannot attend or complete any training, we request (although it is not a requirement) that their direct supervisor is made aware of the absence and make other arrangements for another form of training.

1.1.1.7.8 Training Curriculum

Team MicroTech has deep familiarity with GWACs and GWAC portals, as we have decades of combined experience with the Portals on [redacted] among others. Our Portal is built off the best practices from these portals and mimics their layout and design, while removing or reworking the elements which do not work or are unnecessary to meet GSA's needs.

BSS Portal Overview and Customer Management. General walk-through is provided of username and password, changing password, user or password reset, user interface, and other general portal home page navigation items. We allow computers at each of our trainings such that members can create their user name and password and orient themselves as we continue the portal walk through. We walk through our trouble management steps so as to address easily resolvable issues that may arise. We discuss the search function tool which is enabled for keyword as well as product number.

Obtaining Price Quotes for Services and Features. Our training manual takes a walkthrough of the product and service catalog. We demonstrate a dynamic pricing to order option, where items may be selected and added to a quote, as well as "favorited" items capability. Additionally, we walk attendants through placing order electronically to add, change, cancel, or disconnect services.

Billing. Our billing training course includes a step-by-step breakdown of the billing management area on the portal. We demonstrate how our billing management process occurs, along with the dispute claim resolution, SLA credit management, and payment tracking for In-Process orders.

Order Submission and Tracking. We demonstrate how to submit a complete order form on the GWAC Portal and how-to track the end delivery. In addition, we demonstrate accepting or rejecting part or all of an order.

Network Performance and Changing Services. We allow time to walk through accepting or rejecting an order or part of an order, or adding or changing the features, calling privileges, telephone number or other line attributes that can be changed via "soft" reconfigurations.

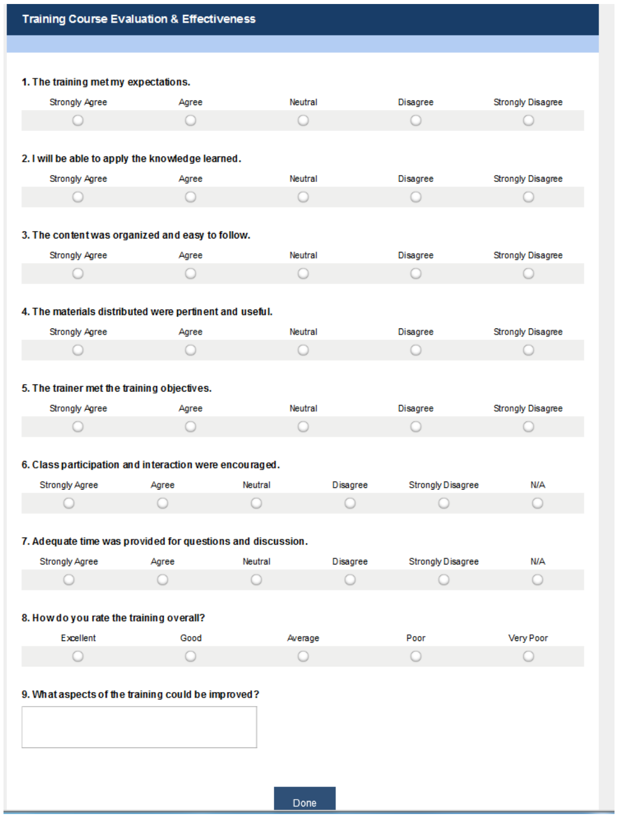
Trouble Ticketing. Team MicroTech's EIS BSS Portal trainers offer a trouble ticketing section of the training such that comprehensive knowledge of any difficulties during the purchasing process are addressed.

SLA Reports. Per the EIS Solicitation, being able to call SLA reports by-the-minute, and placing and tracking trouble reports for routine and emergency troubles, are both features of the Portal.

Inventory Management. Team MicroTech's EIS BSS Portal offers Inventory Management, where current inventories and lifecycles are known. These are refreshed as frequently as possible, we push updates to the inventory tracker at least once every 72 hours, including weekends and holidays.

1.1.1.7.9 Training Evaluation

As MicroTech conducts on intra-office affairs, and develops and employs at federal agencies, we rebrand our preexisting automated/online survey query at the end of each class, for students to evaluate the instructor, effectiveness, course objectives and applicability of the course material, training facilities/method, and offer written comments to the instructor. We use a combination of survey questions, which include: Dichotomous Questions (yes/no), Level of Measurement, such as a Likert Response Scale (see **Figure 2**). We provide these questions across all elements of the training, including but not limited to: the instructor(s), training effectiveness, course objectives, and applicability of the course material, training



Training Course Evaluation & Effectiveness

1. The training met my expectations.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
○	○	○	○	○

2. I will be able to apply the knowledge learned.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
○	○	○	○	○

3. The content was organized and easy to follow.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
○	○	○	○	○

4. The materials distributed were pertinent and useful.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
○	○	○	○	○

5. The trainer met the training objectives.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree
○	○	○	○	○

6. Class participation and interaction were encouraged.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	N/A
○	○	○	○	○	○

7. Adequate time was provided for questions and discussion.

Strongly Agree	Agree	Neutral	Disagree	Strongly Disagree	N/A
○	○	○	○	○	○

8. How do you rate the training overall?

Excellent	Good	Average	Poor	Very Poor
○	○	○	○	○

9. What aspects of the training could be improved?

Figure 2: Training Questionnaire Partial Sample Example.

Team MicroTech's Example of a Likert Response Scale and written comments.

facilities/method(s), and also offer a place for written comments. Team MicroTech offered VTC surveys for the [redacted] at the completion of a VTC session, the requestor is provided with an automated survey requesting their feedback. We provide a daily review of all returned surveys to include follow-up with the customer if there is a perceived issue, generation of Trouble Ticket for any equipment issues, direct contact with customer for any scheduling issues, follow-up training if required, and reporting to government within 2 weeks following the survey close. For example, on contract with the [redacted] Our personnel perform highly visible and highly successful work for [redacted] executive leadership including a large number of special projects. Our customer response to our performance is overwhelmingly positive as evidenced by 80% of quality survey respondents giving us Excellent or Very Good ratings. Team MicroTech is accustomed to automatic and online survey response collections.

Our questionnaire offers a larger breadth of questions across all areas such that course attendants provide feedback on all areas of the training, per our [redacted]

In the event a portion, or an entire training is found unacceptable by the government, Team MicroTech's PMO plan and RMF plans are enacted to immediately and thoroughly correct these issues. We understand that the CO/COR will notify the appropriate personnel. Following this action, we obtain as much information as possible from the government and then immediately re-work the materials and concepts taught in the course which were amiss in the training, reposition our trainers, and offer the training as quickly as possible such that the information disparity is corrected. Team MicroTech accepts this responsibility as we believe our burden on this contract is to provide training on our BSS and ensure the knowledge transfer is complete and correct, such that a working relationship is established and built upon during contract duration.

1.2 Capability to Provide Customers with Web-Based Access to Support Systems

Team MicroTech is experienced in developing web-based support systems. It has an existing platform that allows administrators to develop a support tool with multiple engagement methodologies for web-based access to support systems. These capabilities range from FAQ information and support ticket submissions to self-help search and presentation environments, as well as customer capabilities (where appropriate) to handle support tasks (password reset, administrative functions, access grants, and administrator determined provisioning tasking).

The Team MicroTech platform is highly flexible and allows for support system capabilities to be determined by permission and privileges governed by pre-log-in and post log-in within the “Customer Portal” environment as well. Communication access threading to support system personnel is also permission and privilege managed by administrators with the ability to extend “Email, Chat, and Call” functionality based upon customer, customer access level, time of day, day of week, as well as customer defined “employees” or “access granted” personnel.

The portal’s Administrators also have the ability to customize the support access experience on the Web-Based systems – therefore the customer experience for accessing the support system is customizable as deemed prudent by each customer based on input received by the customer. These customizations run from access management to content provided by the Administrator or the End Customer (if provided). [redacted]

The web based support system customization and support system access deployment is immediate and dynamically customizable within the administrator interface.

The web-based access was built to assimilate multiple levels of communication transportation based upon the requested “support” (i.e. tickets, chat request, email requests, and call requests can be transported to the correct support personnel – transparently to the end customer). Additionally the open architecture allows for the system to be integrated into existing support environments as deemed prudent by the end customer (i.e. end customer can direct support requests to their personnel or systems that have already been established, or direct support requests to multiple destinations or providers they have already established or desire to establish).

The following figures provide visual depictions of the support platform’s access and customization capabilities available to each individual customer as determined by the administrator/end customer requests and input.

[redacted]

Figure 3: One representative theme depicting multiple engagement threads to the web-based support structures.

“Support Line”, Support Customized Access via drop down to FAQs, Self-Help Configuration, Video Library for Self-Help, as well as Contact Us (email, chat, phone). **Figures 4–7** present the drop down individual destinations points represented within **Figure 3** (FAQ, Self-Help, Videos, Contact Us).

[redacted]

Figure 4: FAQ (Addition Table of Content Sub-Categories available)

[redacted]

Figure 5: Self-Help

[redacted]

Figure 6: Helpful Videos

[redacted]

Figure 7: Contact Us (Email / Chat)

Figures 8–13 show the ability to extend a Single User Interface w/ability to manage multiple customer accounts or extend multiple customer access instances.

[redacted]

Figure 8: Ability to Load an Account (My Account) or Load a Customer Account by Administrator or Support Personnel Assisting the End Customer

[redacted]

Figure 9: Ability to Load a Customer Account w/Contextual Search

[redacted]

Figure 10: Ability to extend access capabilities to End Customer with User/Pass Registration. [redacted]

[redacted]

[redacted]

Figure 11: Presents the End-Customer sub-capabilities for self-administration and support following their registration and permission based access to the pre-determined "Action" privileges.

[redacted]

Figure 12: Presents the ability to interface into the customer portal single click access to support management (Chat, Email, Ticketing, Phone)

[redacted]

Figure 13: Presents the destination click of the single click access. [redacted]

Figures 14–18 present the administration capabilities of the platform to manage the web support capabilities of the platform. These figures represents the ability to control the Help Tab at the bottom of the presented page (We can help!") as well as the link to any support environment, either Internal (shown as "Help" within the blue), or external [redacted]

[redacted]

Figure 14: Administration Capabilities.

[redacted]

Figure 15: Ability to extend or not extend self-help functions to the customer (Customer Options: [redacted]

[redacted]

Figure 16: Internal Help Environment. [redacted]

[redacted]

Figure 17: Multi-tier capabilities presented [redacted]

[redacted]

Figure 18: Content Management System. [redacted]

1.3 Inspection and Acceptance

GSA and the Agencies conduct inspection and acceptance to insure our delivered EIS services meet specified requirements and quality levels. Team MicroTech facilitates government quality assurance by providing transparent access to our verification processes that include inspection and testing results and processes. We provide access to our facilities and our data to support the government's processes in the most efficient and effective manner. We conduct verification testing, a standard process whereby we assure that EIS services meet or exceed the required Key Performance Indicators (KPIs) prior to service delivery. We assure that our services (complete with all capabilities and features) as well as our business support systems conform to technical requirements and service level agreements. Our test plans and processes are comprehensive since they test components as well as solutions and end-to-end performance. We also provide a historical record of testing and provide that to GSA upon request.

1.3.1 *Business Support Systems (BSS)*

In accordance with the Solicitation requirements, our Test Methodology follows the Verification and Acceptance procedures outlined in Sections E.2.1.1 through E.2.1.5. Team MicroTech delivers the Final Test Plans 30 days after notice to proceed. Our test plan will assure that all of the required functions such as ordering and invoicing function as required. We understand and acknowledge that the Government has 21 days from receipt of the Final Test Plan to accept or reject the plan. If rejected, we request 14 days to correct the plan's deficiencies based on the Government's comments. We understand the Government may offer contractors an opportunity for pre-award testing of their primary security features, but this testing does not take the place of the formal BSS testing following contract award. If the Government offers the opportunity for pre-award testing, the contractors must agree to specific terms and conditions, including acknowledgement that the system available may not be the same system used for formal testing.

1.3.2 *EIS Services*

Team MicroTech verifies that EIS services meet or exceed required KPIs by following our Verification Test Plan. Our plan follows commercial best practices for verification testing procedures. We coordinate with customers for facility access where required to conduct testing. We also coordinate with the customer to afford them the opportunity to observe our verification testing or if directed we support customer acceptance testing. We will rerun verification tests, in whole or in part as directed by the GSA or the agency.

If the customer experiences problems during their acceptance testing, we will correct the problem and repeat our verification testing prior to seeking acceptance.

1.4 Contractor Data Interaction Plan

Team MicroTech leverages the Communications Industry standard operating model to manage the business and interaction between MicroTech, GSA, and the end customers. [redacted] has created a standard business process framework enhanced [redacted] which Team MicroTech will leverage to manage the U.S. Government business.

Team MicroTech utilizes the [redacted] framework to:

- Create a common language for use across departments, systems, external partners, and suppliers, to reduce the costs and risks of system implementation, integration, and procurement.
- Adopt a standard structure, terminology, and classification scheme for business processes to simplify internal operations and maximize opportunities to partner within and across industries.
- Apply disciplined and consistent business process development enterprise-wide, allowing for cross-organizational reuse.
- Understand, design, develop, and manage IT applications in terms of business process requirements so applications will better meet business needs.
- Create consistent and high-quality end-to-end process flows, eliminating gaps and duplications in process flows.
- Identify opportunities for cost and performance improvement through re-use of existing processes and systems.

Team MicroTech modifies the [redacted] model to accommodate and manage the task orders and other requirements specific to the needs of GSA. [redacted] MicroTech leverages all Best in Class technologies managed in a dedicated and approved Government Cloud environment using its current and former partners such as [redacted]

Team MicroTech manages our business leveraging an enterprise Program Management Office (ePMO). The ePMO manages all task orders on which we bid and projects awarded to Team MicroTech. While we have a current OSS/BSS solutions stack/portfolio we plan to leverage, we are prepared to invest in and adopt a common technology infrastructure. The company is also prepared to leverage the common API methodology and approach.

1.4.1 *Common Data Interaction Requirements*

Team MicroTech is prepared to comply with the requirements outlined in Common Data Interaction Requirements (J.2.2) section of this RFP.

1.4.2 *Task Order Data Management*

Team MicroTech leverages our BSS solution stack to manage all key components of the GSA and end customer experience. We leverage secure APIs to transmit data to GSA and comply with all requirements outlined in Sections J.2.3.1 and J.2.9 of the Solicitation.

Data Set	Frequency	Transfer Mechanism
Access Circuit Type	As required	Secure FTP
Access Framing	As required	Secure FTP
Access Jack Type	As required	Secure FTP
Access Provisioning	As required	Secure FTP
Account Type	As required	Secure FTP
Active Inactive	As required	Secure FTP
Adjustment Outcome	As required	Secure FTP
Adjustment Reason	As required	Secure FTP
Agency Bureau Code	As required	Secure FTP
Allowable Tax	As required	Secure FTP
Authoritative System	As required	Secure FTP
Bandwidth	As required	Secure FTP
Charging Frequency	As required	Secure FTP
Charging Unit	As required	Secure FTP
Contract	As required	Secure FTP
Country	As required	Secure FTP
Data Transaction Type	As required	Secure FTP
Delivery Type	As required	Secure FTP
Dispute Reason	As required	Secure FTP
Dispute Status	As required	Secure FTP
KPI AQL Operator	As required	Secure FTP
KPI Location Qualifier	As required	Secure FTP
KPI Measurement Unit	As required	Secure FTP

Data Set	Frequency	Transfer Mechanism
KPI Service Level Qualifier	As required	Secure FTP
KPI Unit Type	As required	Secure FTP
Line Coding	As required	Secure FTP
LOA Dependencies	As required	Secure FTP
Location	As required	Secure FTP
Order Rejection	As required	Secure FTP
Order Type: Header Level	As required	Secure FTP
Order Type: Line Item Level	As required	Secure FTP
Primary Interexchange Carrier	As required	Secure FTP
Service	As required	Secure FTP
True/False	As required	Secure FTP
Yes/No	As required	Secure FTP

1.4.3 *Ordering*

Team MicroTech leverages our Order Management system and complies with all requirements outlined in section J.2.4 of the RFP.

1.4.4 *Billing*

Team MicroTech leverages our Billing solution and complies with all requirements outlined in section J.2.5 of the RFP.

1.4.5 *Disputes*

Team MicroTech leverages our Billing solution and complies with all requirements outlined in section J.2.6 of the RFP. We will work with the government to resolve any disputes and agree on an appropriate credit award in accordance with Section G.4.4.

1.4.6 *Inventory Management*

Team MicroTech leverages our Billing solution and complies with all requirements outlined in section J.2.7 of the RFP. We will fully populate the EIS inventory with the data elements of the IR as defined in Section J.2.7 of the Solicitation.

1.4.7 *SLA Management*

Team MicroTech leverages our Billing solution and complies with all requirements outlined in section J.2.8 of the RFP.

In accordance with Section G.8.4 of the Solicitation, Team MicroTech understands if we fail to meet the performance objectives specified in the SLAs defined in Section G.8.2, the government is entitled to receive credit within two billing cycles. For each failed SLA, we will apply the associated credit in accordance with Section G.8.4. We will calculate the amount of credit as specified in the applicable portion of Section G.8.2.

In accordance with Section G.8.2.1.1.2, Team MicroTech will calculate the credit based on the number of times a particular SLA is failed during a rolling 6-month window from service acceptance using the following formulas:

- For the first month missing a particular SLA during the 6-month window: Service-Specific Credit = 12.5%of the Monthly Charge for a service. This Monthly Charge is either the Monthly Recurring Charge (MRC) for the affected service or the Usage Charge for usage-based services.
- For the second month missing the same SLA during the 6-month window: Service-Specific Credit = 25% of the Monthly Charge for the affected service. This Monthly Charge is either the Monthly Recurring Charge (MRC) for the affected service or the Usage Charge for usage-based services.
- For the third (or any subsequent) month missing the same SLA during the 6-month window: Service-Specific Credit = 50% of Monthly Charge for the affected service. This Monthly Charge is either the Monthly Recurring Charge (MRC) for the affected service or the Usage Charge for usage based services.

The agency may also choose to cancel the affected service without penalty.

Team MicroTech understands that the GSA CO, OCO, or authorized ordering official may submit a SLA Credit Request (SLACR) as defined in Section J.2.8 and that the GSA CO or OCO may designate, in writing, additional personnel or systems authorized to submit SLACRs to Team MicroTech and further that additional credit management requirements may be defined in the TO. We will respond to any such request within 30 days by submitting a SLACR response and issue the credit within two billing cycles of this response unless we choose to reject the request.

Time to Restore (TTR)

Team MicroTech will calculate Time to Restore (TTR) using the following method:

- Find the elapsed time between the time a service outage is recorded in the trouble ticketing system and the time the service is restored.
- Subtract time for any scheduled network configuration change or planned maintenance.

- Subtract time, as agreed to by the government, that the service restoration of the service cannot be worked on due to government-caused delays. Examples of government-caused delays include:
  - The customer was not available to allow the contractor to access the Service Delivery Pont or other customer-controlled space or interface
  - The customer failed to inform the contractor that a security clearance was required to access the SDP or customer-controlled space
  - The government required service at a remote site and agreed that a longer transit time was required

For each incident-based SLA, Team MicroTech will meet the AQL for the matching KPI associated with the service affected by the incident. For each failed SLA, we will also apply the associated credit in accordance with Section G.8.4 using one of the following formulas based on the nature of the service in question:

- Routine Service TTR Credit = 50% of the MRCe for the affected service
- Critical Service TTR Credit = 100% of the MRC for the affected service

1.4.8 *Data Transfer Mechanisms*

Team MicroTech complies with all requirements outlined in section J.2.9 of the RFP.

1.4.9 *Data Dictionary*

Team MicroTech complies with all requirements outlined in section J.2.10 of the RFP.

2.0 PROGRAM MANAGEMENT PLAN

Team MicroTech is ready to meet the responsibilities and challenges of the GSA Enterprise Infrastructure Solutions (EIS) contract. We implement a proven, tested management methodology to process orders and track them to delivery for maximum benefit to the GSA and its customers. Our program management approach is collaborative, cohesive, and focused. We have proven processes and skill in team and vendor management, delivery fulfillment, and quality control. We complete work on time, while meeting or exceeding expectations. We know the value of good recordkeeping and frequent reporting, which make operations seamless and more effective.

MicroTech's senior management includes [redacted] who have an in-depth understanding of Government processes, policies, and requirements, abbreviating the contract start-up learning curve. They have experience from the agency perspective purchasing and implementing transition from previous contracts such as [redacted] The details of our program management approach are detailed in the following paragraphs.

2.1 Contract Management Requirements

Team MicroTech provides a contract management approach to meet the requirements set out in the EIS RFP and subsequent contract. Our approach [redacted] Our approach relies [redacted] Some of our management efforts include [redacted] We keep open communication with GSA stakeholders to ensure we meet all standards and expectations.

Team MicroTech's proposed structure for managing the EIS program creates close communication. Our lean organization responds quickly to TOs and programmatic communications. By focusing on quality, process, and continual improvement, we successfully manage, deploy, and sustain services. We build flexibility into our management structure and have multiple chances for course correction and re-direction.

Team MicroTech fuses the agility and innovation of a small company with the expertise of a highly-competitive established business, translating into a low-risk solution for GSA. Since our inception, we have created and maintained IT services that simplify processes, save time, and expand capabilities.

Team MicroTech has refined a disciplined approach to management that emphasizes effective communication and takes maximum advantage of leading practices, methodologies, tools, and lessons-learned to meet client needs and objectives. [redacted]

[redacted]

[redacted]

- Comply with GSA guidelines and follow ISO processes
- Quickly tailor our approach to the requirements of each task
- Proactively manage cost, schedules, and risks
- Align and integrate our processes and personnel with each task.

We focus our management objectives on creating a responsive partnership with GSA. Our management approach provides a low-risk, reliable solution with vendors and subcontractors integrated into a unified team.

2.2 Description of Service Solution

Team MicroTech's service management solution is based on ecommerce and communications services best practices. At the heart of our service solution is [redacted]

[redacted] The primary method of procuring Team MicroTech EIS services is through our website, the functioning of which is detailed in Section 1.2 of this volume. In addition to the website, our customer support representatives provide support via phone and email and can support the same operations normally performed on the website via means best suited to customer needs. Regardless of the communication means, the Team MicroTech EIS website is the platform for service ordering, billing, inventory management as service management as detailed below.

- Service Ordering. Customers place orders for individual services or service packages designed to ease the ordering of commonly combined services. [redacted] Once the order is placed, the customer can track the order status through to service operation. This interface also provides the customer with the opportunity to modify or cancel the order prior to the start of engineering. [redacted] The customer can access a listing of open and closed service orders. [redacted]
- Billing. Customers can access upcoming, current, and past bills via the same website. Customers can download current and past bills as well as exporting bills in common formats for their own analysis. Items ordered, but not yet billed are reflected as upcoming and can be viewed individually as well as exported. This screen provides the customer with the opportunity to get more information about a bill or billed item with a single click.
- Inventory Management. As Service Orders are fulfilled, these line items appear in the customer's inventory listing. The customer can sort or search this listing according to their needs to export some or all of the items using common formats. The customer

can also export the listing to PDF or print. The inventory management process [redacted] as best suits the customer's needs.

- Service Management. The customer is able to conduct the majority of service management via service ordering and inventory management processes. [redacted]
- Coordination and Communication. Team MicroTech will manage the customer relationship, including, but not limited to:
  - ○ Government-MicroTech communications
  - ○ Resolving trouble reports and complaints
  - ○ Resolving issue calls
  - ○ Resolving billing disputes and inquiries
  - ○ Resolving schedule issues
  - ○ Resolving reporting discrepancies

MicroTech will answer questions and address issues from the EIS PMO regarding our network management activities, especially those that have not been resolved to the satisfaction of the government through our standard trouble handling process per Section G.6.4.1.

Team MicroTech has the capability and 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 service level management requirements as contained in Section G.8
- Help resolve billing queries and reconciliation issues
- Support NS/EP requirements
- Provide the EIS PMO with information on customer requirements and customer demographics

Team MicroTech's service solution is designed to facilitate the customer's effectiveness and efficiency as well as GSA's oversight of execution. As with all of our services, our EIS website and included processes are part of our [redacted] Our website provides multiple means for customer feedback. We incorporate this feedback as well as input from our operations and transition staff and GSA to continually improve the quality of service and the quality of the customer experience.

2.3 Draft Program Management Schedule

Team MicroTech's program management schedule is geared to gather inputs, affect actions, and produce reports that lead to the effective execution of the program and accurate and efficient oversight by GSA as well as transparency to our agency customers. Our program level reports depict the operations and effectiveness of the program while summarizing task order level actions and providing a strategic view of overall delivery. The vast majority of our Risk Management Framework requirements are delivered within 15 to 30 days of notice to proceed and most are updated annually. Those deliverables associated with the Security Assessment and Authorization (A&A) are primarily updated on a biannual basis. We have noted key deliverables that fall outside these annual/biannual windows.

On notice to proceed we take the following actions and deliver the following program deliverables within the first 30 days:

- Activate the CSO and the website
- Post our points of contact list to the website that provides contact information for, at a minimum, the following functions:

  - 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
- Post our online catalog
- Post the Voluntary Product Accessibility Template to our website indicating our Section 508 compliance
- Post the redacted copy of our contract to the website
- We are prepared to update the Customer Training Plan within 15 days of receiving comments from the COR
- Provide our financial status report to the CO

Monthly:

- Post an updated copy of our redacted contract to the website by the 12th of the month
- Provide billing invoices, tax details to agency CORs and to GSA via Conexus
- Provide the AGF Detail, AGF EFT Report and Inventory reconciliation to GSA via Conexus
- Provide the Service Level Agreement Report to GSA via Conexus and to the OCO and agency COR

Quarterly:

- Review our Plan of Action and Milestones (POA&M) from our Security A&A package. We update the GSA ISSO and CO with our progress toward achieving milestones associated with reducing risk
- Provide our Trouble Management Performance Summary Report and Trouble Management Incident Performance Report to the agency COR

- Provide Quarterly Program Status Reports to the GSA PMO and Lead Quarterly Management Review (QPMR) Meetings. The Quarterly Status Reports include the status of such items/issues as:
  - Project Plan for program management activities
  - Base contract modifications
  - TOs and modifications
  - Projects
  - Orders entered and completed
  - Backlog
  - Aging
  - Pipeline of orders
- Billing disputes
- Summary of trouble reports
- Issues and resolution
- Root cause analysis:
  - Identification of measures failing SLAs
  - Root cause of failures
  - Corrective action to remedy
- Technical accomplishments and future plans

Semi-Annually:

- Report our State and Local Taxes, Fees and Surcharges to the CO

Annually:

- Update our FISMA report and provide to the GSA COR/ISSO
- Update our Supply Chain Risk Management Report and provide to GSA CO/COR
- Update our NS/EP Functional Requirements Implementation Plan and provide to GSA COR
- Update our Climate Change Adaptation, Sustainability, and Green Initiatives Report and provide to GSA CO/COR and OCO
- Update our Power Utilization Efficiencies (PUE) Report and provide to OCO

While these reports and activities reflect only a portion of the myriad of actions and interactions associated with delivering EIT, they do reflect our understanding of the criticality of prompt, accurate communication and compliance with contract requirements.

2.4 Draft Transition Management Approach

Team MicroTech understands that one of the most important activities for EIS providers is the ability to ensure seamless network "Transition on" (the transfer of service from a Networx contract or GSA Local Services Agreement (LSA) to EIS providers) or "Transition off" by leveraging past experience and having proven policies and procedures in place that ensure effective management of this complex and mission-critical process.

Per C.3.1.2, Team MicroTech delivers all services transitioning onto EIS and disconnect those transitioning off EIS as required and specified.

Team MicroTech has a thorough understanding of the needs and the expertise to provide Government Agencies with efficient network Transition. MicroTech has years of experience transitioning complex projects. As an example, for the [redacted] the objective of MicroTech's transition process was to ensure seamless and undisrupted [redacted] The key to a smooth transition was developing a partnership with the [redacted] keeping distractions to a minimum, but applying rigor to address everything needed. We kept the [redacted] informed of progress and offered recommendations on how to improve the knowledge transfer effort if roadblocks existed. Our Project Manager transferred [redacted] knowledge from the existing [redacted] infrastructure, Application Support, and Engineering teams to our team. Our Program Manager focused on supporting non-transition related activities.

Our overarching transition objectives were to:

- Ensure the Government did not experience any lapse in service.
- Maximize the retention of human resources the Government had identified as critical.
- Capture, organize, and maintain all existing documentation produced by the incumbent.
- Document and manage all undocumented incumbent knowledge, and
- Identify transition risks before they became issues and mitigate these through Risk Management Strategy.

[redacted]

For EIS Transition projects, we provide planning, staffing, execution and control of all aspects of transition activity, including special project management attention to certain projects based on priority. Furthermore, we are committed to working closely with the GSA and the individual Agencies to ensure that all Transition projects are executed in the most effective and efficient manner possible. [redacted]

Team MicroTech understands clearly the oversight role of the Government in Transition Projects per C.3.1.1 and work cooperatively with the GSA to ensure that Agencies receive the services they have ordered. Likewise, we work closely with the Agencies, whether they are comprised of one entity or multiple entities, to obtain required telecommunications information about the sites, to coordinate with Agency service providers, and to coordinate the date of scheduled activities with users and other contractors.

The rest of this section highlights Team MicroTech's policies and procedures and tools for network "Transition on" and "Transition off", including:

- Transition Project Management
- Agency Solicitations
- Customer Support
- Interconnection Plan
- Communication and Reporting
- Transition Contingency Plan

Ultimately, Team MicroTech's process and procedures are established to make the transition as transparent as possible to the users and to reduce the overall cost to the Government. Team MicroTech has significant experience in migrating traffic from one network to another. Team MicroTech does this by using effective project management processes, scheduling with the Agency appropriate times for the transitions, and using highly skilled individuals on our project team of Engineers and Field Technicians who understand and appreciate the need for business continuity on behalf of the end users. Team MicroTech understands the importance of managing work to schedule and budget. It is from this foundation that we built our own business and will do no less for the Agency.

2.4.1 *Transition Organization*

Team MicroTech has developed a robust ability to manage and operate large and complex programs and we will use this experience to ensure Government success under the EIS contract. Our established EIS Program Management Office (PMO), located in our Vienna, VA office under the leadership of [redacted] Program Manager (PM) processes all transition orders in their entirety including planning, notifying the Government, executing, and reporting all transition activities to the Government. Our EIS Transition Manager, oversees these efforts, pulling corporate resources as needed to ensure a smooth transition with no loss of service. We provide management, planning, and field personnel sufficient in number and qualifications to ensure that transition activities are completed as ordered.

The Transition team(s) for each project work closely with the PMO. Team MicroTech has identified a Transition-in Management Team (TMT) to plan, coordinate, and implement a seamless transition for operations. **Figure 20** highlights the key personnel, responsibilities required to support each Transition Project. These teams have access to the same information systems allowing clear, consistent communication between all internal groups to provide a seamless customer service solution to the Government.

[redacted]

Figure 20: Transition Team Authorities and Responsibilities Overview

2.4.2 *Transition Project Management*

2.4.2.1 Transition On

Team MicroTech's approach and methodology to "Transition on" and "Transition off" encompasses four aspects as shown in **Figure 21**.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Figure 21: Transition Approach

2.4.2.1.1 Contract-Wide Planning and Implementation

[redacted]

[redacted]

2.4.2.1.2 *Agency-Specific Planning and Implementation*

Team MicroTech recognizes that each Agency may have unique requirements in terms of how and when they will want their services transitioned as well as how we need to communicate to the site contacts during this work. An understanding of the technical requirements as well as the non-technical needs of each Agency is a major part of our planning process. [redacted]

[redacted]

2.4.2.1.3 Inventory

Ordering. Team MicroTech has significant experience in the processing of service request orders for the requisite Government service types, and assists Agencies in the ordering process to expedite all orders for a smooth Transition. Generally speaking, most of the orders will follow a similar process for the management of the orders.

As part of the order process flow there are check points and communications points which will be tracked individually and as a collective group. These will be used as project metrics for reporting and project control.

Team MicroTech understands the complexities of transitioning live network traffic. The technical considerations for the various network services will need to be taken into account.

2.4.2.2 Transition Off

[redacted] While we operate according to GSA's guidance and contractual requirements, we also apply lessons-learned from our experience transitioning in. Team MicroTech views the quality of the transition off every bit as important as the transition on. Our performance not only impacts customer missions, but also their opinion of us and we value their opinions.

2.4.2.2.1 Planning and Implementation

Team MicroTech partners with GSA and the follow-on contractor to minimize transition time and effort and ensure that customer missions are not negatively impacted. [redacted]

2.4.2.2.2 Inventory

An accurate inventory is a key component of a successful transition off. [redacted]

2.4.2.3 Processes, Procedures and Tools Unique to Transition

Team MicroTech draws on its experience managing billing, service ordering, trouble reporting and customer service processes to offer unique transition solutions.

2.4.2.4 Coordination with Incumbent Providers

Successful Transition Projects require coordination with all impacted parties. [redacted] These notices will be distributed as shown in **Figure 22.**

[redacted]

Figure 22: Distribution of Transaction Notices

2.4.2.5 Risk Assessment

Team MicroTech's Program Manager is responsible for risk management. [redacted]

[redacted]

[redacted] **Figure 23** presents those risks with Team MicroTech's mitigation approach.

[redacted]

Figure 23: Potential Transition Risks and MicroTech's Mitigation Approach

2.4.2.5.1 Reporting

The Transition Project team maintains communication and project status.

The types and subjects of scheduled reporting follow GSA's requirements but will be augmented or tailored in consultation with the agency customer upon initiation of the transition project and will be adhered to by Team MicroTech's project management staff. Some of the key types of reports MicroTech has found to be instrumental in maintaining project status include:

- **Weekly Service Report**: [redacted]
- **Monthly Transition Status Report:** [redacted]

Additionally, MicroTech complies with any reporting and requirements identified in an approved Transition Plan. Representatives of MicroTech meet with Government representatives when requested by GSA to report the contractor's progress in completing ordered transitions. MicroTech coordinates all meetings requested by the Government and establishes an agenda if requested by the Government.

2.4.3 *Agency Solicitations*

MicroTech understands the complex needs of the Government Agencies from our current work with both large Government and commercial customers. We know it takes multiple experts from a variety of different functional departments to provide the support our customers need. We designed our team to allow the agency customers to select the best service at the best price from the partners within Team MicroTech.

[redacted] These telecommunications and customer support experts will come together as a team for the duration of the program. [redacted] The account teams will work directly with the Government entities to provide personalized service; thereby, ensuring customer satisfaction.

The PMO account teams ensure that personal support is provided through a dedicated Government toll-free number.

Team MicroTech's PMO is designed to fully meet the Government's requirements at all organizational levels during the contract life cycle by providing:

- Strong executive management commitment and involvement from all levels within MicroTech Communications
- Clearly defined lines of program responsiveness and responsibility
- Carefully selected, fully trained, and highly professional management and technical teams
- Cutting edge network management capabilities, tools, and support systems
- Clearly defined interfaces between MicroTech, the GSA, and the Agencies.

Team MicroTech's PMO is devoted to ensuring complete customer satisfaction throughout the contract and service life cycle and understands the importance of the EIS program and the need for high-level visibility throughout the organization. GSA and all Government Agencies will enjoy the benefit of a dedicated organization that has the necessary authority and the management and operational expertise to fulfill EIS requirements. They coordinate other MicroTech departments and subcontractors to ensure successful delivery and maintenance of end-to-end services.

2.4.3.1 Pre-sales Technical Support

[redacted]

[redacted] See **Figure 24.**

[redacted]

Figure 24: Support Role of Sales Management and Engineering

2.4.4 *Customer Support During Transition*

Team MicroTech provides our customers with unrivaled customer support as shown above with our Account Teams. By emphasizing healthy innovation in both customer support and new services, the Government is assured that Team MicroTech achieves the vision and the mission of the EIS Program.

Team MicroTech understands that the success of the EIS contract ultimately depends on superior customer support, which necessitates commitment, visibility, and communication at the highest management levels. Team MicroTech is perfectly sized to support the EIS contract—large enough to provide the requisite technical and management resources, yet sized to be nimble and responsive to each Agency's unique needs and requirements.

2.4.4.1 Transition Handbook Outline

Team MicroTech provides EIS customers with a handbook that describes the process of transition and the roles and responsibilities of the parties involved. [redacted]

[redacted]

2.4.5 *Interconnection Plan*

As Team MicroTech has a deep and robust team comprised of multiple nation-wide telecommunication and data carriers, [redacted] This type of arrangement allows Team MicroTech to offer the customer a customized solution across multiple carrier networks that offers extremely flexible solutions. This design does not constrain us to one individual network but utilizes the best connectivity options from multiple local and national networks. Interconnection to government private networks will be made using the same arrangement described above.

The primary goal of Team MicroTech's interconnection plan is to provide minimal impact to customer's operations. The detailed implementation plan will provide for installation and testing of connectivity prior to transitioning services to our network. [redacted] This allows for the least amount of customer impact. [redacted]

2.4.6 *Transition Contingency Plan*

Team MicroTech maintains continuity and quality of existing services to Agencies throughout transition and migration activities. Implementation of new services ordered by Agencies during transition or implementation does not disrupt transition or migration activities or affect the planned schedule.

[redacted]

2.4.6.1 Transition Contingency Approach

[redacted]

We ensure adequate management and planning staffs and the field personnel staffs are on-hand as needed to complete transition activities.

[redacted]

2.5 Resource Plan

Our Resource Plan includes financial resources, human resources, and equipment. Team MicroTech has a comprehensive plan to budget and track costs to limit expense to the Government. Our Human Resource Plan describes how we identify and retain highly qualified personnel and make effective use of their skills and the details are explained below. As a part of our resource plan, Team MicroTech details how equipment is maintained, and hardware and software assets are managed.

2.5.1 *Financial Resources*

Team MicroTech's management approach to cost control, tracking, and budgeting for EIS is based on an [redacted] (**Figure 25**). This framework is a strategic approach for designing, delivering, managing, and improving the way information technology and telecommunications services are used within an organization. The framework employs methodologies and processes that are compatible with and produce deliverables that integrate into all aspects of services management, including accounting and cost management.

[redacted]

Figure 25: [redacted]

The goal of Team MicroTech's use of the [redacted] is to ensure that the right processes, people, and technology are in place so that the Government organization can meet its business goals. The [redacted] ensure that services are provided in a focused, client-friendly and cost-optimized manner. With these processes, all services are clearly defined, success can be measured with regards to the service provision, and targeted improvement measures can be introduced where necessary.

Team MicroTech has both service and product contracts on the [redacted] so we have extensive experience controlling costs to the Government. We employ our [redacted] framework to guide EIS services. Our [redacted] implementation:

- Decreases costs
- Improves resource utilization
- Provides services that meet GSA requirements
- Provides the Key Performance Indicators (KPIs) we use to support performance measurements

[redacted]

Team MicroTech uses [redacted] and other systems to track resources, manage costs, and provide timely reports to the contracting office. [redacted] interfaces with the accounting system to provide real-time data to the project management team.

2.5.2 *Human Resources*

GSA benefits from attracting and retaining a permanent, highly-qualified workforce in all specified labor categories. We build strong teams of experienced and engaged personnel. We fill supervisory positions with experienced personnel charged with providing the leadership, direction, functional understanding, control, and accountability needed to ensure we support all areas in keeping with GSA requirements.

We staff non-supervisory positions with functional specialists with exemplary subject matter knowledge and performance. We select and reassign individuals from our existing teams, as much as possible, to provide proven performers whose skills have been successfully demonstrated on other assignments under our direct control. In addition, we always seek and capture new talent and innovative thinkers.

Measures we take to fill critical positions include:

[redacted]

2.5.2.1 Recruitment Sources

[redacted]

As Affirmative Action employers, MicroTech provides job vacancy announcements to several organizations that assist in locating qualified minorities, women, veterans, and workers with disabilities. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted] [redacted]

2.5.2.2 Successful Incumbent Capture, a Recruiting Methodology

MicroTech ensures a smooth and efficient staff transition and maximum knowledge transfer retaining valued incumbent staff to capitalize on and maintain institutional knowledge. Our successfully proven process is explained. [redacted]

Screening. [redacted]

Interview. [redacted]

Offer Letter/Start Date. [redacted]

2.5.3 *Equipment*

MicroTech uses software as our primary method for managing hardware and software assets.

[redacted] The asset management system enables MicroTech to monitor, control and account for all property transactions. Asset activity is easy to record, simple to retrieve, and completely auditable.

The system has many capabilities such as:

[redacted]

[redacted]

MicroTech manages all hardware and software on receipt. During the receiving process documentation will be created to establish custody and accountability. [redacted]

[redacted]

All supporting documents collected during the receiving process are scanned and attached to each property record when the record is created in the asset management system.

2.6 Quality Control Program

Team MicroTech operates in compliance with our [redacted]. These standards, and our corporate commitment to quality which motivated us to implement them, mandate we develop a quality assurance plan containing items such as project metrics collection, analyses and reporting, risk management, strong data management and reporting structures, and QA/QC. The impact and result of these items is less overall risk to the project and DOL operations. The QAP is provided to the CO/COR/COTR for approval prior to the start of the contract. [redacted]

All team partners follow the same processes, procedures, policies, and the same quality management system. Where necessary, Team MicroTech provides training prior to contract start for all personnel to ensure consistent quality services and management of each contract. The PM is responsible for all program quality and conducts peer walkthroughs, management reviews, quality assessment reviews, and testing. Each Task Lead is responsible for implementing all project-level quality control procedures. MicroTech’s corporate Quality Assurance Department [redacted] This provides independent oversight for al quality controls within the program. The following are other elements of our QMS:

[redacted]

- [redacted]

[redacted]

[redacted] All MicroTech employees are made aware of all SLAs and SLA elements prior to any service implementation.

To ensure the continuation of compliance of service-specific and incident-based SLAs and elements therein, MicroTech's [redacted]

Our service management page provides customers access to known service disruptions that may affect services in their inventory. Additionally, customers can monitor service availability and utilization for given services or groups of services. The service management function alerts customers to services meeting or exceeding subscription levels or where the service provider has not met SLAs for specific services per TO. SLA failure will have details on what constituted the reported failure. The portal also allows for the placing and tracking of trouble tickets by the customer, by the network monitoring tools, or by the Customer Service Office. SLA non-compliance is tracked continuously and made available in near real time on the Service Management Portal/page.

Team MicroTech will generate a Service Level Agreement Report (SLAR) that documents monthly SLA performance covering all aspects of a service provided, including incident-based SLAs, service specific SLAs, service-provisioning SLAs, and billing accuracy SLAs. Report content will be as defined in Section J.2.8 of the Solicitation. MicroTech will deliver this report on the 15th of each month. MicroTech will generate a SLACR for any credit request. Our response contents are as defined in Section J.2.10 of the Solicitation. We will deliver this report to the government within 30 days after receipt of a credit request. In those cases where MicroTech does not meet the defined contract or TO SLA, MicroTech will provide credits or adjustments to the government agency of record or GSA.

2.7 Key Personnel and Organizational Structure

2.7.1 *Key Personnel*

Team MicroTech's Program Manager (PM) serves as the single point of contact for the EIS contract and is responsible for overall delivery and contract performance. He manages our highly skilled personnel in the complex EIS environment. He formulates and enforces work standards, assigning schedules, reviewing work discrepancies, tracking service deliverables, and communicating policies, purposes, and goals of the organization to subordinates. He coordinates regular quality reviews with the teammates through "Team Health Check" meetings.

The PM is responsible for all deliverables related to the management of the contract (i.e., budget reports, technical progress reports, invoices, etc.). Ultimately, our PM is accountable to the government for performance and problem resolution on this contract.

He has the full support of MicroTech leadership and the resources of our corporate office. The PM ensures contractor personnel perform EIS management duties as assigned to include: tracking projects, monitor project progress, resources, and communicating project information to the government with presentations and reports. The PM provides support and updates to the client by identifying and managing critical success factors for projects and contract expectations.

[redacted]

Summary of Qualifications

[redacted]

2.7.2 *Substitutions and Additions of Contractor Key Personnel*

Team MicroTech is very proud of our personnel. We attract and retain the highest quality employees using our Human Resources Plan as described in Section 2.5.2. Should any substitutions of our personnel be necessary, we will submit a written request to the GSA CO and abide by the established terms and conditions.

During the first 180 days of contract performance, Team MicroTech makes no key personnel substitutions except in the unfortunate situations including illness, injury, death, disciplinary action, demotion, termination of employment, or other exceptional circumstances approved by the GSA CO. Should any of these events occur, we promptly notify the GSA CO and provide the information required including a detailed explanation of the circumstances requiring the proposed substitution or addition; a complete resume for each proposed substitute or addition, and any other information requested by the GSA. We certify that the proposed replacement is better qualified than, or at least equal to, the key personnel to be replaced.

In the case that substitutions in key personnel are necessary after the initial 180-day period, proposed substitutions and additions are submitted to the GSA CO in writing 15 days (30 days if security clearance is to be obtained) prior to the anticipated effective date of the proposed change.

2.7.3 *Organizational Structure*

Team MicroTech's proposed organizational structure provides clear lines of authority and reporting to ensure an orderly work flow and responsiveness (**Figure 26**).

[redacted]

Figure 26: Organizational Structure. *MicroTech's streamlined organizational structure empowers and provides clear escalation abilities when necessary.*

Team MicroTech believes that hiring and retaining qualified personnel is vital to a service contract's success. We propose candidates with the most current and applicable experience, who familiarity with GSA systems and regulations, and who hold the requisite security and technical qualifications to work on this program.

Team MicroTech's organizational structure contributes to the planning and execution of work requirements by establishing clear lines of communication and authority between our corporate-level management, the Program Manager, Project Manager, Sr. Analyst, and our project team, as we have successfully established on current work. Our structure provides centralized, overall program management, financial and contract data management, and a direct interface to the CO and COR. Our approach delivers the entire range of corporate resources to assist the PM with the required support from a staffing, business, and contractual perspective, as well responding to contract requirements. Shown in **Figure 26**, MicroTech's lean management structure streamlines communication and responsiveness to customer requests and requirements. MicroTech confirms management and staff names and contact information for the government during the kickoff meeting and/or during transition.

MicroTech has executive reachback to our partners on this effort, as shown in **Figure 27**. [redacted]

[redacted]

[redacted]

Figure 27: Executive Organization Support.

Using [redacted] The PM oversees the project team.

2.8 Risk Management

Risk management is a continuous, forward-looking process that is an important part of our business and technical management processes. Team MicroTech uses a systematic and disciplined risk management approach to identify potential risk and apply proven, clearly identified solutions across the entire lifecycle to mitigate adverse impacts on performance to achieve requirements. This plan provides overall guidance to the Team Leads and will be updated as project teams identify additional risks.

2.8.1 *Risk Management Process*

The purpose of risk management is to identify potential problems before they occur so that action may be taken to avert them or reduce their impact on achieving objectives. Risk management starts during the beginning stages of project planning and continues throughout the life of the project. Team MicroTech will identify risks and manage them effectively to allow GSA to make informed decisions. Risks will be identified during the development of the technical approach for each Task Order.

Team MicroTech has an established iterative risk management process that identifies and mitigates risks as well as evaluates the effectiveness of the risk mitigation strategy and manages potential shortfalls. [redacted]

2.8.1.1 Roles

The primary roles associated with this process are listed below.

[redacted]

[redacted]

2.8.1.2 Tools and Templates

[redacted]

2.8.2 *Risk Categories*

As risks are identified, they are categorized into groups. Some risks may fall into more than one category. For instance, a risk that the schedule will be extended is likely to also affect cost.

- Technical – Technical risks affect the effectiveness and usefulness of the proposed technical solution and the likelihood that it will meet GSA requirements.
- Schedule – Schedule risks impact current project milestone completion dates.
- Cost – These risks adversely affect the project budget.
- Safety – Safety risks have the potential to jeopardize human life; they can appear in processes, hardware, software, or the environment.
- Quality – These risks compromise project operating standards or the final deliverables.
- Scope – Increasing scope likely creates other risks in other categories such as cost or schedule; decreasing scope impacts future business goals.

Once risks are analyzed, based on their likelihood and impact, risk mitigation strategies and contingency plans are developed and presented to the CO or COTR during regularly scheduled status meetings. Team MicroTech's Program Manager and the CO or COTR review significant risks and the progress of mitigation strategies during weekly and monthly status meetings; the results of these discussions are documented in the Monthly Status Report.

2.8.3 *Independent Risk Identification*

Team MicroTech supports GSA by taking a proactive action in identifying risks. We encourage every team member, regardless of position, to identify risks as early as possible. Once identified the MicroTech PM evaluates the risk and works with other key team members and GSA to resolve or mitigate the risk as quickly and as early as possible. Team MicroTech's Directorate Lead tracks identified risks and their associated mitigation plans, makes recommendations to the Deputy PM for affirmation and approval. The status of these risks is updated in the Program Monthly Report to the Government.

The Team MicroTech Deputy PM ranks risks as Low, Medium, or High and assign them to an appropriate risk owner. The risk owner is responsible for the re-assessment of risk, risk handling, planning, and execution. [redacted]

2.8.4 *Process Steps*

MicroTech's proposed risk management process complies with the [redacted] Risk Management process area.

[redacted]

Figure 28: Risk Management Process. *We use best practice standards to identify and solve potential risks*

We have identified activities that represent risks with the potential to impact the fulfillment of mission critical task orders. The table below summarizes some of those risks and MicroTech's recommended mitigation strategies.

[redacted]

[redacted]

2.8.5 *Risk Identification and Mitigation*

Team MicroTech has identified the following common risks and plans to mitigate them throughout the performance of the contract:

[redacted]

Some of the risks GSA may experience in the future would be those arising from the continuing realignment of GSA missions and responsibilities due to new budgetary constraints. Such limitations would impact programs in a wide range of activities, some of which are listed below.

[redacted]

2.9 Information Systems

Team MicroTech understands that one of most important features of the BSS, right after security, centers on the end-user experience. The back-end capability of any system is virtually meaningless if the end user is unable to easily and intuitively use the system interface to extract the most benefit from it. Team MicroTech has years of experience designing web-based solutions from the ground up and will use that knowledge to design user-friendly web pages that are both secure and intuitively laid out.

The core capabilities that will initially be available within the BSS include: Order Submission using a Pricing Catalog, Billing and Payment Management, Inventory Management, and a Trouble Ticketing capability. This initial core set of functions will be part of 5 functional modules that will allow for future enhancements to be added to the BSS in a systematic and organized way. Team MicroTech will work closely with EIS stakeholders, to add additional feature sets to the BSS Roadmap that will improve the functionality and capability of the system. [redacted]

[redacted] Additional capabilities can also be included as the needs of the user community change.

Knowing the BSS will need to serve a wide variety of customers, it will be designed with maximum accessibility in mind. Using common industry standards that are Section 508 compliant, the BSS user interface will accommodate standard browsers (IE, Edge, Chrome, Firefox, and Safari). [redacted]

In addition, the BSS will include support for bidirectional, secure, direct data exchange APIs to facilitate XML over HTTPS using SOAP calls along with SFTP transfers for file based bulk data exchange. NIST compliant mutual authentication and encryption of data will be accomplished through x.509 digital certificates, in keeping with current industry standards. To ensure only authorized users with appropriate permissions are able to access data and information though the BSS, users will need to register for access to the system. Using the registration information, the appropriate role based access controls can be applied to restrict access; including but not limited to, the ability to place orders and research order, billing, inventory, and performance information. Users of the system will have the ability to view and download (exchange) data and information in several formats that will be compliant with government requirements for both content and format. Adjustments to data exchange formats, schemas, methods and level of detail will be at the discretion and control of the government. Changes to data exchange elements can be developed and implemented through coordination and negotiation with the government.

Over time, the BSS will be subject to changes, updates, and patching to maintain optimal security, functionality, and reliability. Changes that impact or change the Web interface user experience relative to 508 compliance or functionality that requires additional training will be coordinated and approved by the government, regardless of the impact or severity. This also includes changes that impact direct data exchange, the system's ability to meet any specified requirements, or system security. Changes and modifications to a system as large and complex as the BSS requires strict adherence to Change Control and Configuration Control processes. Team MicroTech follows industry best practices for Change Control, derived from our [redacted] competencies. This knowledge and experience will directly benefit EIS in the successful implementation and control of the BSS throughout the life of the contract. Consequently, the government will be the approving authority for all changes subject to change control and once approved, any additional training, retesting and compliance validation along with associated documentation updates will all be part of the change control process.

As a government integrator, Team MicroTech has many years of successful and security compliant hardware and software development implementations that span several DoD and Federal agencies. Team MicroTech is very familiar with application of DISA STIGs, FISMA, FIPS, NIST, OMB and GSA IT security directives, policies, publications, and guides. This vast history and knowledge base will provide EIS with a BSS that is fully compliant across the full spectrum of Federal security requirements.

3.0 BSS VERIFICATION TEST PLAN

This Draft BSS Verification Test Plan provides a general overview of the test strategy that Team MicroTech will employ to ensure that testing objectives are met and business risk associated with the approval of our BSS systems is minimized. The plan depicts resources (personnel, environment, equipment, tools, etc.) required and provides an overview of the types/styles of testing that will be performed. Development of the test plan is an iterative process. The test plan is initially drafted during the planning phase and updated and finalized during the execution phase. It has been written in compliance with the EIS RFP and individual system scope documents, but is dependent on system requirements for finalization.

The Draft BSS Verification Test Plan will be finalized and approved prior to the start of test execution. All changes to, or deviations from, the test plan will be documented in the project test report. Updates will not made to the test plan after test execution has started; the baseline test report will be created at the start of test execution to record changes from test plan.

Team MicroTech has developed this Draft BSS Verification Test Plan in accordance with the requirements of Solicitation Section E.2.1, as directed by Section L.30.2.3. This draft plan meets the inspection and acceptance requirements for functional, load, security, and regression testing, with the understanding that regression testing will apply only to system changes and not the BSS developmental systems.

1. We will begin with internal testing of our BSS platform. Our internal test plan will include detailed descriptions of the functions we will test in the system. Examples of these tests include tests of the system’s features that will be accessible to Government users ordering services from Team MicroTech. Features such as the user interface, ordering applications, user commands, and user transactions with the system are included in our tests. Features will be tested under load with multiple users and stress testing of the network. Tests for response times will be done as part of performance testing. We will also conduct security testing using different scenarios to ensure that our security meets the Government’s requirements during live testing.

Team MicroTech’s internal testing of our BSS will use scenarios that emulate what we might encounter in formal Government testing. This approach allows us to correct problems and retest the system multiple times over a period of months. Our network engineers will write test scripts that exercise the systems' features under heavy loads. Multiple test scripts can be started simultaneously and must run long enough to exercise the system's capacity and capabilities.

The GSA's functional testing will verify that the network applications and infrastructure operate correctly under a heavy load. Functional testing will focus on the interactions of the system when multiple users run the same application. This type of testing will closely emulate the real-world production environment.

For the formal Government testing of the BSS, we will be prepared to execute the test cases developed by the GSA, as detailed in Solicitation Section E.2.1.2. We are aware that no testing will be done until both the Government Conexus system and our BSS pass unit testing. All testing will be done on Team MicroTech's proposed BSS; no alternate systems will be allowed. Data transfers will use the mechanism defined in Section J.2 for that data set. All test data will be provided by the GSA and will emulate real-world data sets; no actual customer data will be used in testing. We are aware that some test data sets may include errors to test the error handling capabilities of our BSS.

The GSA will use a tiered testing approach for the BSS. Team MicroTech will be given multiple test cases for test scenarios outlined in Section E.2.1.2. We will incorporate the test cases into the BSS Test Plan, execute them, and document the test results. Certain test cases will use real-world test data, such as a disconnect order, to execute. Team MicroTech understands that functional testing is incomplete until all scenarios are passed; the BSS must properly execute each test case in the scenario to pass. All test cases must properly handle each subcase twice in succession using different data sets; a subcase will not be considered passed until the BSS handles the data sets following a prescribed routine with no errors or warnings.

Although regression testing may not occur as part of the formal BSS testing, it is important to understand its role in the BSS life cycle. Regression testing is done to compare the performance, reliability, and functionality of a new hardware or software release to the current release. It is designed to ensure that new system components don't impact the production network. Most important, regression testing ensures that both the testbed and the test cases emulate the critical components and risks that may appear in the production network. As technology evolves over the life of the EIS contract, there is a high probability that regression testing will be part of the BSS and network life cycle.

Load testing the BSS occurs when running multiple scenarios for different types of orders: new service; disconnects; moves, adds, and changes; orders coming from multiple sources including Web-based and e-mail; as well as orders adding features, TSP orders, bulk orders, and task-order-unique CLINS (TUCs). Team MicroTech will be prepared to handle multiple ordering scenarios as part of BSS load testing. We will demonstrate the system features related to the ordering scenarios, including initial task order set-up and updates. With the help of the Government representatives, we will demonstrate how an authorized Government user can place an order as specified in RFP Section J.2.4, and the correct fields populate in the BSS in accordance with Sections G.3, G.5, and J.2. The system will provide an order acknowledgement or other appropriate CDRLS based on the accuracy of the order.

2. Team MicroTech will demonstrate our BSS management and operational functions related to Ordering, Billing, Inventory Management, Disputes, SLA Management, and Trouble Ticketing in accordance with Solicitation Sections G.3 – G.8 and J.2. Our Ordering procedures are designed to meet the requirements of managing multiple types of orders from different Government sources, including directly on the contract via task orders with simple or complex CLINs ranging from TUCs to Individual Case Basis, to those requesting different feature sets, services, and performance; or orders from eBuy for equipment and services.

Billing can be one of the most demanding tasks on the EIS contract. Team MicroTech will demonstrate the features and functionality of our billing application and system during BSS testing. Our system meets the requirements of RFP Section G.4, which stipulates that the contractors must meet prerequisites related to processing and delivering an accurate Agency bill. The test scenarios relate to inventory reconciliation in which system reference data is loaded onto the BSS. The system must be able to accurately account for inventory for billing purposes. Billing must be accurate and produce the correct inventory usage, remainder, and cost to the Agency.

Usage-based billing test scenarios will take into account monthly minutes called, include the appropriate taxes, and ensure that the service is billed to the correct task order. It must also account for the associated Government fee and identify the CDRLs related to the bill. Government-provided test data will include sample usage data for one or more UBI based on usage based CLIN(s). Billing adjustment scenarios will be included in the test set. The data set from the Government will include a sample adjustment request to modify a billing line item. Both Ordering and Billing scenarios will require accurate results, the necessary CDRLs, and the correct technical aspects to pass the testing. Disputes differ in that they require the BSS to issue a Dispute Report identifying open billing disputes, and a second report listing open and closed disputes. The Government will issue data sets with at least two disputes per set, and a notification to close at least one of the disputes. The acceptance criteria include accurately identifying all required CDRLs, accurate data based on inputs, and again, the correct technical aspects to pass testing.

SLA Management, similar to Disputes, requires an SLA Report. The prerequisites for this test include one or more previously provisioned orders. Inputs to this test are services showing SLAs met or missed. The data set uses UBIs to show whether the SLAs were met or not. Outcomes are identical to those required for Disputes. When testing for an SLA Credit Request, the additional prerequisite of an SLA Report with on SLA missed is required. Inputs to this test include an SLA Credit Request, while the output is an SLA Credit Request Response.

Trouble Ticket Management is a critical function that is fulfilled by tiers of support. Trouble tickets are opened for both customer-reported, and network monitoring tools signifying an issue. Once the ticket is opened, the Government customer will receive regular status updates until the problem is corrected and the ticket can be closed. Team MicroTech will meet the Government’s 24x7x365 trouble monitoring requirements, and also provide real-time on-line status for Agency users of our network. Activities will include complaint collection, entry, tracking, analysis, priority classification, and escalation as appropriate, for all services to ensure that problems are resolved within the timeframes specified in Section G.8 Service Level Management. As our first priority,

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

we will restore any TSP restoration-coded service as quickly as possible. We will escalate problems in accordance with the criteria in our Program Management Plan. Team MicroTech will provide the Government with the ability to query, sort, export, and save in formats such as PDF/CSV or other file formats trouble and complaint records by any field or combination of formatted (that is, not free-form text) fields in each record. We will process credits applicable to the service outage based on this record of information. SLAs and credits are defined in Section G.8 Service Level Management. The contractor shall, upon request from the PMO and agencies, deliver archived trouble and complaint report data within five (5) days of the request for such information.

3. BSS security testing is a critical step in system authorization by the Government. The system must comply with the BSS System Security Plan, as defined in RFP Section G.5.6.4. The BSS must meet FISMA, FIPS, and NIST Special Publication guidance and directives. The system must also meet with current GSA policies and directives, and pass the Federal Government’s Assessment and Authorization process. Direction for completing the A&A process is in NIST SP 800-37, R1 and GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.” Team MicroTech understands that our BSS must have a valid A&A before being placed in service and allowed to carry Government communications traffic. We are aware that failure to maintain a valid A&A is grounds for contract termination. The A&A must be conducted every three years, or when a significant change occurs in the system’s security posture.

4. Team MicroTech has reviewed the test cases in RFP Section E.2.1.3, and will be prepared to engage in the testing of our BSS following contract award. Should the Government offer pre-award testing of the Offerors’ systems, we may avail ourselves of that opportunity to demonstrate the security of our BSS.

5. Our response to Section 3.1, Draft BSS Verification Test Plan, has attempted to address all of the scenarios outlined in RFP Section E.2.1.3. We will be prepared to demonstrate BSS use cases for quality, utility, and customer access features as well.

3.1 Scope

Team MicroTech will meet the Government’s Inspection and Acceptance requirements, including the following:

- Our BSS test results will verify that all functional, regression, and security requirements were successfully met
- Testing included all management and operational systems for Ordering, Billing, Inventory Management, SLA Management, and Trouble Ticketing, in accordance with RFP Sections G and J.2.
- Security testing, based on the requirements of RFP Section G.5.6, and addressed A&A; FedRAMP certification (if required); testing with multiple use cases as defined in RFP Section E.2.1.3; and use cases for quality, utility, and customer access to features.

At the Government's request, we will perform tests each time a new service is offered, or if Team MicroTech modifies the features or functionality of our BSS. Should the Government require this retest, we will provide a BSS Verification Test Results Report, including analysis, within 7 days of performing the test. The Government reserves 14 days to review and accept or reject the results. If rejected, we will retest the changes to the BSS until the Government is satisfied with the results. BSS Verification Testing will be done according to the BSS Test Plan, at a time and date agreeable to the Government.

3.2 BSS Test Scenarios

3.2.1 *Testing Prerequisites*

Before beginning BSS testing, Team MicroTech will provide the Government with written notice that our BSS has passed internal testing and is ready to begin BSS interface testing with the Government. We will provide the final BSS Test Plan that is accepted by the GSA. We understand that verification and acceptance testing is to ensure that our BSS meets the requirements of RFP Sections G and J.2. We will support BSS security and functional testing as detailed in RFP Section G.5.6 and G.2.3.

3.2.2 *Test Scenarios*

We have thoroughly reviewed the list of BSS Test Scenarios, and understand that our BSS must pass the acceptance criteria for the system to be authorized by the Government. We have addressed the test scenarios throughout our response to Section 3 herein, and understand the relevant portions of Section G and J.2. We understand that the scenarios address the relevant data exchange mechanisms and the validation of the data exchanged. We further understand and acknowledge that each Test Scenario is associated with one or more Test Cases presented in RFP Section E.2.1.3.

3.3 BSS Test Cases

Team MicroTech has reviewed the BSS Test Cases, and will incorporate them into the Final BSS Test Plan, and successfully execute them during BSS Testing. We accept the conditions presented in the EIS RFP, as detailed in RFP Section E.2.1.3. MicroTech, as the Prime Contractor for Team MicroTech, takes no exceptions to the Government's Requirements.

3.4 Deliverables

3.4.1 *Verification Test Plan for Contractor's BSS*

Team MicroTech's Draft BSS Verification Test Plan (this document) is submitted in accordance with the Government's timeline.

- Draft: Delivered with our proposal
- Final: 30 days after Notice to Proceed
- Revisions: 14 days after receipt of Government comments

Our BSS Test Plan will:

- Reflect the test methodology defined in RFP Section E.2.1
- Include MicroTech's approach to testing each test scenario and test case
- Include the contractor's timeline and test sequencing.
- BSS testing to occur during normal working hours, 8:00 am – 5:00 pm, Monday – Friday EST.

[redacted]

3.4.2 *Verification Test Results Report for Contractor's BSS*

We will provide a BSS Verification Test Results Report which includes an analysis of the current test results containing the test scenario number, test case number, test data set number, test number, date the test was executed, the test acceptance criteria, and the test Result including a pass or fail status. This report will also include a summary table of all previously submitted results. Team MicroTech will deliver the report within 7 days after performance of the tests. We understand that the Government reserves 14 days to accept or reject the test results, in whole or in part. We will perform retests of test cases with test data sets that failed, until they are accepted by the Government. We will also rerun tests, in whole or in part, as deemed necessary by the Government to verify that the Government's comments on the test results were satisfactorily addressed.

3.5 BSS Final Contract Acceptance

The General Services Administration has established a time period of 12 months from acceptance of the BSS Verification Test Plan, for the contractors to complete and pass BSS validation testing. If the contractor is unable to pass validation testing in that timeframe, the Government will cancel the contract. The exception to this rule is if the delay in passing the testing is due to the Government. Team MicroTech understands that in the event our BSS does not meet the Government's schedule, we will not receive the Minimum Revenue Guarantee stated in Section H.3, if the contract is cancelled under this clause. We acknowledge that the Government will not accept any financial claim or settlement from the contractor as a result of the contract being cancelled. Team MicroTech understands that BSS validation testing does not include completion of Assessment and Authorization (A&A) as referenced in Section E.2.1.2.2 of the solicitation.

3.6 Draft BSS Development and Implementation Plan

Team MicroTech's technical and management approach, including integration management, emphasizes partnership with our customers in planning and delivery of all aspects of the project. Our approach is based on a foundation of [redacted] Facilitating effective communication and identifying key management reviews is a primary driver of any MicroTech program or project plan. We select our program and project managers based on their communication abilities and understanding of the organizational and operational context or the customer environment.

3.6.1 *Scope*

By the use of this Development and Implementation Plan, Team MicroTech takes responsibility to architect, develop, and support the creation of this BSS utilizing our testing methodology, change control, security compliance, quality control, risk management, and related activities to provide a solution to fulfill the GSA EIS solicitation.

3.6.2 *Identification*

[redacted]

Team MicroTech BSS Architecture

[redacted]

3.6.3 *Relationship to Other Plans*

This Development and Implementation Plan is part of the Team MicroTech support process for enhancement and maintenance of the BSS. The steps in this plan are a prerequisite for modification of the BSS prior to user testing and acceptance.

3.6.4 *Reference*

The list of internal referenced artifacts includes:

- Change Control in this document is found in Section 1.1.1.3.4.1

- Security Compliance in this document is found in Section 1.1.1.3.5
- Testing Methodology in this document is found in Section 1.3.1
- Quality Control in this document is found in Section 2.6
- Risk Management in this document is found in Section 2.8

The list of external referenced artifacts includes:

[redacted]

3.6.5 *System Overview*

Team MicroTech's BSS platform provides the core Order Submission (including Pricing Catalog), Trouble Ticketing, Inventory Management, Billing, and Payment Management to facilitate the GSA acquisition program to meet future federal information technology and telecommunications needs and become the federal government's strategic sourcing center for network based and network-enabled services.

This web based acquisition platform performs security controlled access with flexible business rules to align with the GSA requirement and Team MicroTech's operations requirement to provide a compliant service offering.

Team MicroTech BSS Platform Overview

[redacted]

3.6.6 *Assumptions and Constraints*

- The contract award will happen in October 2016 and the Development and Implementation Plan will start on November 1, 2016
- Equipment

[redacted]

- Scope modifications
- Integration challenges
- Schedule conflicts
- GSA approval time line and/or prerequisites

3.6.7 *Plan Deliverables*

The following deliverables will be produced during the project:

- Business Use Cases
- Business Use Case Survey
- Glossary
- Supplementary Specifications
- Design Briefs
- Navigation Map
- User Interface Prototype
- Use Case Survey
- Data Model
- Design Model
- Database Design
- Software Architecture Document
- Implementation Subsystem
- Test Package
- Change Requests
- Test Summary

3.6.8 *Evolution of the Software Development Plan*

[redacted]

[redacted]

The Development and Implementation plan will be revised for each iteration.

3.6.9 *Project Organization*

3.6.9.1 Organizational Structure

The project team includes:

[redacted]

[redacted]

3.6.9.2 External Interfaces

The Team MicroTech development and implementation project team will work with the Government customer Support and the GSA users to confirm requirements, review business and uses cases, test cases and scenarios and test results to verify the BSS fulfills the plan objectives.

3.6.9.3 Roles and Responsibilities

[redacted]

3.6.9.4 Project Resourcing

The project resources on this project are provided by Team MicroTech. The resources assigned to this project will have appropriate skills. [redacted]

3.6.10 *Management Process*

3.6.10.1 Project Plan

Team MicroTech will conduct development of the plan using a phased approach where multiple iterations occur within a phase. The phases and the relative timeline are shown in the table below:

[redacted]

The milestones that mark the end of each phase can be seen in the table below.

[redacted]

3.6.11 *Iteration Objectives*

[redacted]

3.6.12 *Releases*

At this point in time, one release is planned. After the 30 weeks of development, we will have one release that will be ready for verification testing. Verification testing will be complete 30 days following the roll-out of Release one.

4.0 EIS VERIFICATION TEST PLAN

Team MicroTech's operational experience with secure network management allows us to quickly respond to customer needs with minimal or no impact to voice and data services. We ensure our services through proper designing, testing, and documentation of all customer network solutions. Our management processes ensure coordination with customers for specific requirements on a routine and on demand basis, including all required documentation, government change request forms, and other requirements.

In addition, our team of carriers operate in an agile fashion with continual updates in network administration technologies and information systems, computer security, intrusion detection system, malware and anti-virus support and relational database administration, querying and report generation. This requires a test and evaluation plan for both pre-deployment and routine monitoring of efficiency and effectiveness. For complex and highly secure customer solutions our team conducts penetration testing with our networks in several stressed conditions from bandwidth limitations to traffic anomalies.

Our security planning and controls method is based on our [redacted] and ANSI best practices. We have mapped into the NIST 800-53 controls using a plan derived from NIST 800-171. Team MicroTech will provide test cases for each of the test scenarios defined in Section E.2.2 of the Solicitation. We will provide all the necessary test equipment: data terminals, load boxes, test cables, and any other hardware and software required for testing. We will successfully test all of the test cases defined in the EIS Test Plan using one or more test data sets proposed and provided by Team MicroTech. We will test all services and service features proposed in the TO. We will use test data sets that reflect real-world service conditions and locations and we will address all relevant test cases.

Team MicroTech will complete verification and acceptance testing based on the acceptance criteria defined in the government-accepted EIS Test Plan for any services listed under Section C.2 that is awarded to Team MicroTech. These Test plans will be updated and augmented per the modification proposal should new services be added to the contract in the future. We will not begin billing for services if the government rejects the services within 3 days of receipt of the Service Order Completion Notice (SOCN).

Team MicroTech understands that the service will be accepted if the government does not reject the service within the acceptance period defined above. We further understand that in the event the government rejects the service, it may at its option:

- Direct Team MicroTech to repeat the procedure outlined above;
- Withdraw the service from acceptance testing;
- Direct Team MicroTech to facilitate the return of the services to their original provider (for services transitioned or migrated from another contractor's network);
- Request a replacement of the service (in whole or in part); or
- Cancel the service order without penalty.

In the event the government rejects the SOCN, Team MicroTech will issue a new SOCN for services after correcting the reasons for rejection. If the government exercises any of these options as a consequence of unacceptable acceptance testing results, we understand that all expenses incurred by the government will be borne by Team MicroTech. If the government elects option 1, above, we will immediately initiate corrective actions to remedy the problem reported on the trouble ticket and will keep the government informed of progress. We further understand that in cases when the government cannot successfully complete acceptance testing due to circumstances beyond Team MicroTech's control, we will notify the government of the details surrounding the deficiencies and the steps we have taken to overcome the deficiencies. Team MicroTech further understands that these cases will be discussed between us and the government and that, 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 by the government in those instances when Team MicroTech has demonstrated that the problems encountered are not the fault of Team MicroTech and the government has determined that we have taken all reasonable actions to correct all problems. We understand that the waiver issued by the GSA CO or OCO will specify the grounds for the waiver. We also understand that if the waiver is not granted, we will be obligated to continue to attempt correction of the deficiencies encountered in order to successfully accomplish the acceptance testing.

We will provide an EIS Testing Report, as defined in Section E.2.2.5 of the Solicitation,

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

within 3 days of service installation and testing. We will allow government representative(s) to observe any or all parts of the EIS Verification Testing.

Our test plan focuses on 3 phases: Activation Phase, Testing Phase, and Acceptance Phase. [redacted] These and other measurements are run in a regression table to determine changes in the network. [redacted] All associated test scenarios, test cases, test data sets, acceptance criteria will be customized to meet the individual service, security, and location requirements.

KPI	Test Parameter	Value
Latency (Round Trip Delay)	Trial Duration	120 seconds
	Latency Threshold (ms)	per contract
	Number of Trials	1
Throughput	Trial Duration	120 seconds
	Threshold	Within 1% of EVC Bandwidth
Jitter (Round Trip Delay Variation)	Trial Duration	120 seconds
	Jitter Threshold (ms)	per contract
	Number of Trials	1

Figure 29: Sample Fiber Circuit Performance Metrics

The following sample of our plan is applicable to all services offered. (Service-specific test plan information is provided later in this section).

EIS VERIFICATION AND CONNECTIVITY PLAN (EVCP)

1. Introduction

Infrastructure solutions are vital to {Organization's} mission/business processes; therefore, it is critical that services provided by Team MicroTech are able to operate effectively without excessive interruption. This EIS Verification and Contingency Plan (EVCP) establishes comprehensive procedures to test and verify quickly and effectively EIS service.

1.1 Background

This EVCP establishes procedures to test and verify {service name}. The following plan and objectives have been established:

- Maximize the effectiveness that will be accomplished through an established plan that consists of the following phases:
  - Activation and testing phase to activate the service and testing against KPIs;
  - Acceptance phase to ensure that {service name} is validated through testing and that customer has accepted service performance levels.
- Identify the activities, resources, and procedures to carry out {service name} initialization and testing requirements.
- Assign responsibilities to designated {organization name} personnel and provide guidance for verification of {service name}.
- Ensure coordination with all personnel responsible for {organization name}. Ensure coordination with external points of contact and carriers associated with {service name} and execution of this plan.

1.2 Scope

This EVCP has been developed for {service name}, which is classified as a high-impact system, in accordance with Federal Information Processing Standards (FIPS) 199 – Standards for Security Categorization of Federal Information and Infrastructure solutions. Procedures in this EVCP are for establishment of EIS services and the verification of initialization and performance. This plan does not address requirements that were not addressed in the associated task order such as diverse path, redundancy, and /or unidentified KPIs.

1.3 Assumptions

The following assumptions were used when developing this EVCP:

- {Service name} has been established in accordance with EIS contract procedures.
- Key {service name} personnel have been identified and trained in their roles; they are available to initialize and verify the {service name} verification plan.

2. Concept of Operations

The Concept of Operations section provides details about {service name}, an overview of the two phases of the EVCP (Activation/Testing, and Acceptance), and a description of roles and responsibilities of {Organization's} personnel during the verification process.

2.1 System Description

[redacted]

2.2 Overview of Two Phases

This EVCP has been developed to implement and verify the {service name} using a two-phased approach. This approach ensures that service initialization efforts are performed in a methodical sequence to maximize the effectiveness and minimize system outage time due to errors and omissions.

[redacted]

During validation, the system is tested and validated as operational prior to making it available for use to the task order customer. [redacted] The system is declared operational by services owners upon successful completion of validation testing.

2.3 Roles and Responsibilities

[redacted]

3. Activation/Testing Phase

[redacted]

3.3 Testing Process

[redacted]

3.3.1 Sequence of Testing Activities

[redacted]

3.3.2 Testing Procedures

[redacted]

3.3.2 Test Case Generation

[redacted]

[redacted]

4. Acceptance

[redacted]

4.1 User Acceptance Testing (UAT)

[redacted]

[redacted]

4.2 Validation Data Testing

[redacted]

4.3 Validation Functionality Testing

[redacted]

[redacted]

4.4 Acceptance Declaration

[redacted]

4.5 Notifications (users)

[redacted]

4.6 Completed Documentation

[redacted]

SUGGESTED APPENDICES

[redacted]

APPENDIX A [redacted]

[redacted]

{Service name} **EVCP Key Personnel**

Key Personnel	Contact Information	
EVCP Director	Work	*Insert number*
Insert Name and Title	Home	*Insert number*
Insert Street Address	Cellular	*Insert number*
Insert City, State, and Zip Code	Email	*Insert email address*
EVCP Director – Alternate	Work	
	Home	
	Cellular	
	Email	
EVCP Coordinator	Work	
	Home	
	Cellular	
	Email	
EVCP Coordinator – Alternate	Work	
	Home	
	Cellular	
	Email	
EVCP Team – Team Lead	Work	
	Home	
	Cellular	
	Email	
EVCP Team – Team Members	Work	
	Home	
	Cellular	
	Email	

APPENDIX B [redacted]

[redacted]

APPENDIX C [redacted]

[redacted]

APPENDIX D [redacted]

[redacted]

[redacted]

APPENDIX E [redacted]

[redacted]

APPENDIX F [redacted]

[redacted]

APPENDIX G [redacted]

[redacted]

APPENDIX H [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

The following is a sample of a yearly test and maintenance schedule for a services:

[redacted]

APPENDIX I [redacted]

[redacted]

APPENDIX J [redacted]

[redacted]

APPENDIX K [redacted]

[redacted]

Record of Changes			
Page No.	Change Comment	Date of Change	Signature

Test Plan for Ethernet Transport Services

Team MicroTech will conduct all verification testing related to services and systems for Ethernet Transport Services. We will assure that the services, capabilities, and features provided to an agency conform to the technical requirements for the service defined in Section C.2.1.2 of RFP. Team MicroTech is responsible for all equipment, software, labor, and facilities required for executing the verification testing.

This section contains a Test Plan to verify that the Ethernet Transport Services delivered under the contract meet the requirements of Section C.2.1.2 of the RFP.

Team MicroTech will archive all verification test results for a minimum of 2 years and will deliver any archived test results requested by GSA within 5 business days after receipt of GSA's request.

Prior to accepting service, the agency's designated contact will receive an EIS Services Verification Testing Report (EIS Testing Report) from Team MicroTech that shows successful completion of testing as defined in the EIS Services Verification Test Plan. We will complete verification and acceptance testing based on the acceptance criteria defined in the government accepted EIS Test Plan. For additional detail on accepting service, see EIS contracts Section E.2.2.

Ethernet Service Activation Test Methodology

[redacted]

Scope

[redacted]

[redacted]

Test Equipment Capabilities

[redacted]

Abbreviations and Acronyms

This Recommendation uses the following abbreviations and acronyms:

[redacted]

[redacted]

Ethernet Service Activation Test Methodology:

[redacted]

[redacted]

Figure EVCP-1: High-level Service Activation Test Methodology

Service Configuration test (Test Case)

[redacted]

Service Configuration Test Reporting Format (Test Data Sets)

[redacted]

[redacted]

Service Performance Test (Test Case)

[redacted]

[redacted]

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

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Test Duration

[redacted]

[redacted]

Pass/Fail Criteria

The service must operate at or above the SAC performance levels for the service to be accepted for bringing into service.

[redacted]

Service Configuration Test Reporting Format

[redacted]

[redacted]

[redacted]

[redacted]

Service Performance Test Result Format (illustrative)

[redacted]

[redacted]

Test Plan for IPVS (Internet Protocol Voice Service)

[redacted] These performance measurements are good indicators of network performance for a given geographic footprint. This set of performance measurements [redacted] are intended to demonstrate efficiencies in network design and sufficient levels of resource allocation such that real-time services and other services are maintained with acceptable Quality of Service.

The sampling of these measurements is on [redacted]

The information obtained from this measurement should be used for tracking overall network level performance particularly from the perspective of sustaining desired Quality of Service for all IPVS services.

[redacted]

Transport provided to the customer premise will be managed to the IPVS KPIs outlined in the Solicitation.

[redacted]

Internet Protocol Voice Service (IPVS) will provide voice communications service and telephony features to agencies using VoIP over a managed IP network. [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Features Test

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

All Tests results, as well as pass/fail indicators are provided in a final test report.

Test Plan for Access Arrangements

Access Arrangement Description

Access Arrangements (AAs) connect the SDP at the agency location to a POP on the contractor's network. The range of line speeds and reliability options allows agency users to satisfy their diverse needs to access contractor networks. AAs provide the convention to specify and price the originating and/or terminating access component required to deliver a service. AAs cannot be ordered as a standalone access service and no performance metrics are specified for them, however we do perform acceptance tests on these circuits to ensure the performance of the circuit and its position in the overall service delivered. The following is a general description of test methodology parameters to be measured, the measurement procedure, and the acceptance (pass/fail) criteria.

[redacted]

Test Methodology

[redacted]

[redacted]

[redacted]

[redacted]

Optical Fiber and Ethernet Access Arrangements

For this type of Access Arrangements, refer to section 2.2, Ethernet Transport Services in this section. [redacted]

IntraNet VPN

[redacted]

[redacted]

[redacted]

B. Testing Phase

[redacted]

Results-FAIL

[redacted]

[redacted]

C. Acceptance

Once the Testing Phase is completed, documented and satisfactory, relevant project members will accept the project as complete and validated. All relevant documentation will be finalized and shared amongst authorized project members.

Documentation includes but is not limited to, [redacted]

Remote Client VPN

[redacted]

Results - Pass

[redacted]

[redacted]

Results-FAIL

[redacted]

ExtraNet VPN

[redacted]

Results- PASS

[redacted]

Results-FAIL

[redacted]

[redacted]

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

[redacted]

[redacted]

[redacted]

[redacted]

5.0 SCRM PLAN

Team MicroTech's Supply Chain Risk Management Plan (SCRM-P) creates a framework that will allow the government and Team MicroTech to proactively manage risks inherent in the global supply chain. As a whole, the government recognizes the growing threat to its operational programs and national security. To that end, NIST has developed Special Publication 800-161, DoD Instruction 5200.44 mandates SCRM, and DFARS clause 252.239-7018 ensures the use of SCRM by all subcontractors. This plan seeks to be compliant with current NIST Special Publication 800-161 specifications, DoDI 5200.44, all applicable regulations, and other complimentary, industrial supply chain best practices. The SCRM-P has been developed to ensure the integrity and continuous auditability of the entire spectrum of services and product (HW/SW) as utilized in IT environments which we plan, develop, and sustain. The approach affords visibility into its full supply chain sufficient to ensure the selection and management of suppliers of critical components across the IT and related communications networks lifecycles. The plan encourages consistency and stability through regulation of compliance and integration. Our plan enumerates all known factors and seeks continuous review of the landscape of risks, to demonstrate that risk has been mitigated to the maximum extent possible. Due to the large, complex, and global nature of today's Information and Communications Technology (ICT) value chains, Team MicroTech has established a dedicated SCRM team as part of our corporate quality control organization with the primary objective of formalizing the function of risk management relative to Supply Chain (SC) affected operations.

MicroTech developed an analytical framework as an aspect of our corporate [redacted] [redacted] compliant processes, to assess and analyze risk scenarios and then work with manufacturing and supplier partners to help identify, assess, and manage risks. This SCRM-P is administered by mitigating risks through providing a consistent, disciplined environment for developing products, assessing potential discrepancies in the process (i.e. assessing risks), determining which risks to address (i.e. setting mitigation priorities), implementing actions to address high-priority risks, and bringing those risks within tolerance.

[redacted] MicroTech will identify and require that all subcontractors providing critical components provide all necessary information to complete the SCRM Plan in association with MicroTech.

[redacted]

[redacted]

[redacted] baseline information security controls as defined in NIST SP 800-53 Revision 4, as applicable

[redacted]

The plan ensures that standardized SCRM policies, procedures, and practices are implemented and adhered to at all contract locations for all involved staff. The plan, in terms of quality control, integration with project and corporate management operations, risk management, cost management and adherence to Federal mandates, will be executed [redacted] Together, application of these respective methodologies will not only monitor, inspect, and correct deficiencies, but also ensure continuous improvement across all SCRM program processes.

The SCRM-P's fundamental definitions and tenets ensure the SCRM-P provides the organizational framework for implementation of comprehensive risk, quality inspection, and reliable auditing of deliverables. Implementing Team MicroTech's SCRM-P for the government means policies and processes required to support continuous improvement efforts across all risk factors will be created and followed. Team MicroTech's SCRM Task Lead works with our respective EIS Program Manager and our project Technical Leads upon contract award to further tailor the SCRM-P to the government's specific needs. Our SCRM Lead ensures periodic reviews of the SCRM-P are performed to ensure the plan's continued effectiveness and suitability to the program. [redacted] Team MicroTech staff are expected to be well versed in all knowledge areas of the SCRM-P, related project management processes of the respective program, ISO, and other principles as required.

Core Components of SCRM

The scope of activities that are subject to SCRM assurance include [redacted]

- **Assessment**: Supply chain elements, processes, and actors must be accurately and uniquely identified. Knowing who and what comprises an enterprise's supply chain is critical to gain visibility into what is happening within it, as well as monitoring and identifying high-risk events and activities. Without visibility and traceability into the supply chain, it is impossible to understand and therefore manage risk to reduce the likelihood of adverse events.
- **SCRM Requirement Inheritance**: Acquirers, integrators, and suppliers need to share data and information related to their responsibilities regarding SCRM. [redacted] Information should be protected according to mutually agreed-upon

practices. All contractors and subcontractors are required to adhere to DFARS 252.239-7018.

- **Training**: Supply chain risk management awareness and training must be performed. A strong supply chain risk mitigation strategy cannot be put in place without significant attention given to training personnel on supply chain policy, procedures, and applicable management, operational and technical controls, and practices. NIST SP 800-50, "Building an Information Technology Security Awareness and Training Program," provides guidelines for establishing and maintaining a comprehensive awareness and training program.
- **System Security Engineering**: [redacted]
- **Configuration Management**: Effective control of all configuration is essential for ensuring that only approved, valid, genuine hardware and software is distributed. [redacted]
- **Perform continuous integrator review**: Continuous integrator review is an essential practice used to determine that defensive measures have been deployed. [redacted]
- **Delivery Security**: Delivery, including inventory management, is an essential function within the supply chain, which has a great potential for being compromised. [redacted]

[redacted]

- **Sustainment**: The sustainment of activities and processes must be ensured. [redacted]
- **Disposal**: Every system component has a finite life expectancy and at the end of its life, each system component must be disposed properly to ensure sensitive information is destroyed. NIST SP 800-88 “Guidelines for Media Sanitization” is followed – the security categorization of each component dictates whether a medium will be cleared, purged, or totally destroyed. [redacted]
- **Mutually informed decision making**: MicroTech and GSA participate in regularly scheduled meetings to share information regarding supply chain threats and then discuss effects, mitigations, and resolutions. Because the process includes information from all parties, decisions reached will have fewer unintended consequences and positive program impact overall.
- **Updates:** MicroTech will update and modify our SCRM Plan to include any future changes to the NIST SCRM Guidelines at no cost to the Government.

5.1 Ensuring Requirements for Information Technology Tools (ITT) are Imposed on Direct Suppliers

Team MicroTech ensures requirements for genuine ITT are imposed upon all suppliers. To do this, we will follow NIST SP 800-61 controls to ensure that third-party suppliers employ adequate security measures to protect products, information, applications, and/or services outsourced from the Team MicroTech. The controls recommended by NIST specifically ensure:

[redacted]

NIST SP 800-61: The following are specific examples of the multidisciplinary foundational practices that can be implemented incrementally to improve an organization’s ability to develop and implement more advanced ICT SCRM practices:

- Implement a risk management hierarchy and risk management process (in accordance with NIST SP 800-39, *Managing Information Security Risk* [NIST SP 800-39]) including an organization-wide risk assessment process (in accordance with NIST SP 800-30 Revision 1, *Guide for Conducting Risk Assessments* [NIST SP 800-30 Rev. 1]);
- Establish an organization governance structure that integrates ICT SCRM requirements and incorporates these requirements into the organizational policies;

- Establish consistent, well-documented, repeatable processes for determining [FIPS 199]impact levels;
- Use risk assessment processes after the [FIPS 199] impact level has been defined, including criticality analysis, threat analysis, and vulnerability analysis;
- Implement a quality and reliability program that includes quality assurance and quality control process and practices;
- Establish a set of roles and responsibilities for ICT SCRM that ensures that the broad set of appropriate stakeholders are involved in decision making, including who has the required authority to take action, who has accountability for an action or result, and who should be consulted and/or informed [redacted]
- Ensure that adequate resources are allocated to information security and ICT SCRM to ensure proper implementation of guidance and controls;
- Implement consistent, well-documented, repeatable processes for system engineering, ICT security practices, and acquisition;
- Implement an appropriate and tailored set of baseline information security controls in NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* [NIST SP 800-53 Rev. 4];
- Establish internal checks and balances to assure compliance with security and quality requirements;
- Special Publication 800-161 Supply Chain Risk Management Practices for Federal Information Systems and Organizations
- Establish a supplier management program including, for example, guidelines for purchasing directly from qualified original equipment manufacturers (OEMs) or their authorized distributors and resellers;
- Implement a tested and repeatable contingency plan that integrates ICT supply chain risk considerations to ensure the integrity and reliability of the supply chain including during adverse events (e.g., natural disasters such as hurricanes or economic disruptions such as labor strikes); and

- Implement a robust incident management program to successfully identify, respond to, and mitigate security incidents. This program should be capable of identifying causes of security incidents, including those originating from the ICT supply chain.

5.2 System Security Engineering Processes

System Security Engineering processes include defensive design for systems, elements, and processes must be used as a part of system security engineering. The use of design concepts is a common approach to delivering robustness in security, quality, safety, diversity, and many other disciplines that can aid in achieving supply chain risk management. Design techniques apply to supply chain elements, element processes, information, systems, and organizational processes throughout the system. Element processes include creation, testing, manufacturing, delivery, and sustainment of the element throughout its life. Organizational and business processes include issuing requirements for acquiring, supplying, and using supply chain elements.

[redacted]

[redacted]

5.3 Strategy for Implementing SCRM Security Requirements

To ensure SCRM security requirements are implemented, Team MicroTech follows all recommendations in NIST SP 800-53 Revision 4, SA 12-Supply Chain Protection. We tailor our implementation to the specific effort. These include:

- 12-1 Acquisition Strategy/Tools/Methods
- 12-2 Supplier Reviews
- 12-3 Trusted Shipping and Warehousing
- 12-4 Diversity of Suppliers
- 12-5 Limitation of Harm
- 12-6 Minimizing Procurement Time
- 12-7 Assessments Prior to Selection/Acceptance/Update
- 12-8 Use of All-Source Intelligence
- 12-9 Operations Security
- 12-10 Validate as Genuine and not Altered
- 12-11 Penetration Testing/Analysis of Elements/Processes and Actors
- 12-12 Interorganizational Agreements
- 12-13 Critical Information System Components
- 12-14 Identity and Traceability
- 12-15 Process to Address Weaknesses and Deficiencies

5.4 Criticality Analysis Process

Per NIST recommendations, the SCRM-P’s criticality analysis ensures establishment of a prioritized list of critical functions, systems, and components. Critical functions are defined as those, which if corrupted or disabled, are likely to result in mission degradation or failure. The critical mission functions are “dependent on their supporting systems that in turn depend on critical components in those systems system (hardware, software, and firmware).” [redacted] Per NIST recommendations, a defensive posture will be prepared by executing a set of iterative steps:

1. Identify organization’s mission and business drivers, such as applicable regulations, policies, requirements, and operational constraints.
2. Prioritize these drivers to help articulate the organization’s critical SC functions, systems, and components.
3. Identify and group critical mission functions based on the drivers.
4. Map the mission-critical functions to the system architecture and identify the systems/ components/services (hardware, software, and firmware) and processes that are critical to the mission/business effectiveness of the system or an interfacing network.
5. Allocate SCRM criticality levels (high, moderate, low) to the components/services that have been defined.
6. Correlate identified critical components and services to ICT supply chain maps, historical data, and SDLC to identify critical ICT supply chain paths.

[redacted]

[redacted] Per NIST specification, initial reviews identify functions and systems/components that have a direct impact on mission functions and may be performed concurrently at each tier. Following reviews should include the criticality analysis, threat analysis, vulnerability analysis, and mitigation strategies defined at each of the other tiers. Each SC risk iteration will refine the criticality analysis results and result in the addition of defensive functions.

5.5 Ensuring Products and Components are not Repaired and Shipped as New Products and Components

MicroTech follows the controls listed in Supply Chain Protection, NIST SP 800-53 Revision 4, SA 12.

5.6 Ensuring Supply Channels are Monitored for Counterfeit Products

Team MicroTech implements NIST SP 800-61 (PE 20) controls for monitoring counterfeit products.

NIST SP 800-61 PE 20 Supplemental ICT SCRM Guidance specifies the organization should use asset location technologies to track system and components transported between protected areas, or in storage awaiting implementation, testing, maintenance, or disposal. Methods include RFID or digital signatures. These technologies help protect against:

- Diverting system or component for counterfeit replacement;
- Loss of confidentiality, integrity, or availability of system or component function and data (including data contained within the component and data about the component); and
- Interrupting supply chain and logistics processes for critical components.

5.7 How MicroTech's Physical and Logical Delivery Mechanisms Will Protect Against Unauthorized Access, Exposure of System Components, Information Misuse, Unauthorized Modification, or Redirection

Team MicroTech follows NIST SP 800-61 controls and guidance, Physical and Environmental Protection, Policies and Procedures.

5.8 How MicroTech's Operational Processes and Disposal Processes Will Limit Opportunities For Knowledge Exposure, Data Release, Or System Compromise

[redacted]

[redacted]

5.9 Identifying Relationship Between MicroTech and the Manufacturer

[redacted]

5.10 Expressed Warranty

Team MicroTech extends all software warranties, including standard COTS warranties, to the Government.

5.11 Ensuring Independent Verification and Validation of Assurances

Independent verification and validation of assurances is a component of the Team MicroTech's Supply Chain Risk Management (SCRM) plan. Our plan ensures independent verification and validation of assurances through a number of means. [redacted]

6.0 CLIMATE RISK MANAGEMENT PLAN

6.1 Climate Change Adaptation

The GSA intends that EIS contractors will use sustainable management to minimize the impact caused by the execution of the Enterprise Infrastructure Solutions (EIS) program. MicroTech and its partners (Team MicroTech) recognize the necessity of reducing environmental impact of the work and activities performed in the execution of EIS. We will use sustainable management practices including tracking and seeking continual reductions in energy usage, greenhouse gas (GHG) emissions, water consumption, solid waste and hazardous waste, and other relevant environmental impacts and associated costs. Using sustainable management practices lowers the environmental impacts of delivered products and services. We will work with the GSA to comply with the Presidents Executive Order 13693 – Planning for Federal Sustainability in the Next Decade (E.O. 13693), and other applicable laws, regulations, and directives. This will include relevant recommendations from the working groups established by E.O. 13693. We will work with the GSA to determine how to adapt and apply Federal mandates to private sector activities as necessary.

6.1.1 *Sustainability Reporting*

It is often the case that public disclosure of facts, and the process of assembling the facts, leads to operational improvements. Companies that disclosed their environmental impacts and sustainable management practices have had reductions in their supply chain and other business risks. Preparing sustainability disclosures aids in understanding the environmental impact of procured products and services. It can also help find strategies to reduce the impacts. These strategies can then be applied in designing projects and task orders (TO) with reduced environmental impact. Disclosure to EIS customers will alert them to the environmental impact procured products and services. Studying the mitigating strategies developed will help them design projects and TO requirements that use these strategies.

In accordance with GSA requirements Team MicroTech will provide locations (Internet URL or URLs) of sources for publicly available information regarding company-wide environmental impacts and sustainable management practices on our EIS Web portal. These sources will include existing, widely recognized third-party sustainability reporting portals and services such as the Global Reporting Initiative (GRI) Sustainability Disclosure Database (database of corporate social responsibility (CSR) reports), Ceres, and the Carbon Disclosure Project (CDP) Climate Change and Water Disclosure Questionnaires. Consistent use of these resources will keep our sustainability disclosures up-to-date and accurate.

We will develop standards for sustainability-related reports, including estimates of the life cycle costs and environmental impacts of proposed solutions, and will then apply them to the TO level. MicroTech will research available sustainability tools and methodologies in developing the standards. These will include those available from the GSA, the Sustainability Accounting Standards Board (SASB), the Corporate Sustainability Reporting (CSR) website, GRI's G4 Sustainability Reporting Guidelines, and other sources such as Ceres and their Aqua Gauge and Supplier Self-Assessment Questionnaire (SAQ). The SAQ is given to prospective suppliers to identify, assess, manage, and disclose possible supply chain sustainability risks.

6.1.2 *Climate Change Adaptation*

As part of its portfolio, the GSA is tasked with ensuring delivery of goods and services. It is also designated as a lead agency for the E.O. 13693 Federal Sustainable Acquisition and Materials Management Practices Standing Workgroup. This includes looking forward to what the possible effects of climate change could be and what risks they might pose to the GSA mission. They may include events that cause network disruption, and possibly temporary interruption of transportation routes to reach and repair a facility. We will consider climate change adaptation aspects in the design and operations of services to be provided under this contract. This would include design and operation of new facilities and, in the operation of existing facilities, plans to mitigate possible problems.

Section 3(h)(viii) of E.O. 13693 addresses climate resilience: improve building efficiency, performance, and management by including the incorporation of climate-resilient design and management elements into the operation, repair, and renovation of existing agency buildings and the design of new agency buildings.

Actions that could be taken to add climate resilience in designing new buildings and retrofitting existing buildings include:

- Incorporate resilient design and management into the building management plan.
- Identify and evaluate vulnerabilities to natural hazard risks (e.g., earthquakes, drought, storms, floods, sea level rise, and wildfires).
- Consider flood-proofing strategies.
- Enhance wind resistance.
- Provide access to electricity in the event of an extended power outage.
- Improve energy performance of building envelopes (ensure that buildings maintain habitable temperatures in the event of power outages).
- As appropriate, use information modeling to assess design options and improve decisions based on life cycle analysis.
- When cost-effective, adopt passive and natural design strategies over active and mechanical systems.

Team MicroTech will incorporate climate change adaptation strategies into risk-management programs to reduce property, infrastructure, and supply chain vulnerabilities. [redacted] These activities will be performed in accordance with E.O. 13693 and other applicable laws, regulations, and directives.

E.O. 13693 accepts the fact that the world is not perfect and trade-offs must be made in some circumstances. Therefore the Government has set priorities in its goal to “improve environmental performance and Federal sustainability.” MicroTech will follow these priorities, [redacted] We will prepare and update as needed Corporate Climate Risk Management Plans for our activities. The plans will be made available for agency use to directly support the Agency Adaptation Plans of agencies procuring services through this contract.

6.1.3 *Corporate Sustainability Reports*

To ensure that our corporate sustainability goals are being reached, Team MicroTech will engage accredited third-party firms to report on our sustainability status. These reports will be provided to the GSA. [redacted] are among the largest third-party providers of sustainability reports. Companies such as [redacted] base their business around sustainability. There are also companies like [redacted] who research corporate sustainability and provide fee-based data for diagnostics, supply chain analysis, or competitive benchmarking.

We will use the collected data on our activities to prepare a yearly *Climate Change Adaptation, Sustainability, and Green Initiatives Report* and deliver it to the GSA CO in accord with the schedule in Section F in the RFP. The report will highlight changes made during the year to remain fully compliant with the Federal directives and goals of E.O. 13693.

If conditions thought to be out of compliance with the relevant Executive Orders, laws, regulations, and directives occur at any time during the year, we will immediately notify the contracting agency and the GSA CO.

6.2 Sustainability and Green Initiatives

The GSA is committed to reducing the Federal Government's environmental footprint by using environmentally friendly, sustainable practices. To further this end, MicroTech will provide sustainable products and services whenever possible. We will consider the sustainable acquisition and data center requirements of E.O. 13693 in the design and operation of services to be provided under this contract. We will also comply with the climate change adaptation conditions set forth in the Executive Orders, and other applicable laws, regulations, and directives. If conditions arise that are thought to be out of compliance with them, we will immediately notify the relevant agency and the GSA COR.

The Government has programs to define criteria for commercially available products to meet energy consumption and sustainability requirements; it also has online tools to help identify products covered and aid in acquiring them. The three programs are the ENERGY STAR® program, the Federal Energy Management Program (FEMP), and the

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

Electronic Product Environmental Assessment Tool (EPEAT®). We will research products before purchase to see if they are covered by one or more of the programs. We will first check the Green Procurement Compilation at https://sftool.gov/greenprocurement for a complete list of products covered by these programs. There is a link on that webpage to other GPC-related resources https://sftool.gov/learn/about/540/other-gpc-links.

ENERGY STAR

ENERGY STAR is a voluntary EPA program where manufacturers test products to prove they meet the requirements for a respective category. The specifications are periodically reviewed and updated to meet advancing technology, quality, and production standards. In addition to the ENERGY STAR product list, the program also offers advice on how to save energy, and how to benchmark energy usage and measure change. The ENERGY STAR Portfolio Manager® is an online tool that can be used to measure and track energy and water consumption, as well as greenhouse gas emissions. It can be used for one building or a portfolio of buildings, all in a secure online environment. It can also be used to assess the efficiency of data centers.

FEMP

FEMP is part of the DOE’s Office of Energy Efficiency and Renewable Energy (EERE), which leads the agency’s efforts in renewable energy, energy saving homes and manufacturing, and sustainable transportation, all referenced in E.O. 13693. FEMP maintains acquisition guidance on a number of products covered by the other two programs and Water Sense. EPA's WaterSense program focuses on labeling water-efficient products in homes and offices.

To meet the requirements of sections 3(i)(i) and 3(l)(i) of E.O. 13693, [redacted] FEMP maintains a list of electronic product categories with ENERGY STAR specifications that do not yet include the standby power level required, or otherwise allow products be certified to ENERGY STAR but not meet mandated standby power levels.

If there is not an ENERGY STAR specification for a specific electronic product, or it has not been revised in accordance with the standby power levels, electronic products with standby power levels of one Watt or less will be purchased. If such a product is not available, the product with the lowest standby power level available.

Unlike prior executive orders, E.O. 13693 requires that all applicable procurements, rather than 95%, of purchases for electronic products be environmentally sustainable including those electronic products typically used in office spaces and data centers.

E.O. 13693 requires that the EPA issue recommendations for procurement of sustainable electronics. To meet the requirements of sections 3(i)(iii) and 3(l)(i) of E.O. 13693, we will purchase electronic products that meet or exceed specifications, standards, or labels that have been recommended by the EPA. These recommendations are available at: http://www.epa.gov/greenerproducts/eparecommendations/ For products that recommendations have not been issued for yet, purchasers may continue to use the EPEAT product registry.

Unlike prior executive orders, E.O. 13693 does not include a specific reference to Electronic Product Environmental Assessment Tool (EPEAT). However, EPEAT is currently the only tool available to achieve the electronic stewardship mandates of section 3(l) of E.O. 13693.

[redacted]

In addition to the Federal programs there are numerous organizations that point the way to sustainable products and services. Some examples for building materials and services include Sustainable Sources providing online green building information including planning guides for energy, lighting, and water usage; and resources to achieve sustainable goals. The National Institute of Building Sciences has a program dedicated to creating successful high-performance buildings, the Whole Building Design Guide. It includes training, recommendations, and resources for planning, building, and operating facilities efficiently and sustainably. GSA, DOE, and EPA are among the participating Federal agencies.

The goal of the U.S. Green Building Council (USGBC) and its community is to change the way buildings and communities are designed, built, and operated. It developed the LEED (Leadership in Energy and Environmental Design) green building certification system. Another USGBC product is the Green Building Information Gateway (GBIG), designed to connect people, products, and services to green buildings around the world.

6.2.1 *Electronic Product Environmental Assessment Tool*

The EPEAT program is the definitive global rating system for greener electronics. It was developed through a stakeholder consensus process funded by a grant from the EPA. EPEAT is managed by the Green Electronics Council (GEC). GEC maintains EPEAT's website and product registry, and documents the environmental benefits resulting from the purchase of EPEAT-registered products. It is an easy-to-use resource for purchasers, manufacturers, resellers and others to identify environmentally preferable devices; combining strict, comprehensive criteria for design, production, energy use and recycling with ongoing independent verification of manufacturer claims.

Where possible MicroTech will deliver and furnish for Government use, or furnish for contractor use at a Federally-controlled facility, equipment that was EPEAT-registered at the bronze level or higher throughout the life of the contract.

We will use the collected data on our activities to prepare a yearly Climate Change Adaptation, Sustainability, and Green Initiatives Report and deliver it to the GSA CO in accord with the schedule in Section F in the RFP. The report will highlight changes made during the year to remain fully compliant with the Federal directives and goals of E.O. 13693.

If conditions thought to be out of compliance with the relevant Executive Orders, laws, regulations, and directives occur at any time during the year, we will immediately notify the contracting agency and the GSA CO.

6.2.2 *Energy Efficient Products*

Team MicroTech will ensure that energy-consuming products are energy efficient (e.g., ENERGY STAR-certified products or FEMP-designated products or low standby power products) throughout the life of the contract, in compliance with FAR Clause 52.223-15 Energy Efficiency in Energy-Consuming Products.

6.2.3 *Data Centers and Cloud Services*

Section 3(a)(ii) of E.O. 13693 deals with improving data center energy efficiency, establishing a PUE target of 1.2 to 1.4 for new data centers and less than 1.5 for existing data centers. PUE is a ratio of total energy use to that of information technology (IT) equipment. The equation used is:

PUE = Total (Data Center) Facility Annual Energy Use

IT Equipment Annual Energy Use

Where:

- Total (Data Center) Facility Annual Energy Use includes all IT Equipment Energy, plus power delivery and cooling system components, lighting, and all other energy using devices that support the IT equipment.
- IT Equipment Annual Energy Use includes the energy associated with all of the IT equipment (e.g., computers, storage, and network equipment).

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

Team MicroTech will identify data centers that will provide data center or cloud services and have PUE between 1.2 and 1.4. Cloud services providing data centers with a PUE between 1.2 and 1.4 will be favored when they can show an economy of scale. We will provide an annual reporting of the PUE of data centers used under this contract.

The EPA’s interactive energy management tool, ENERGY STAR Portfolio Manager, can be used to measure and track energy consumption and greenhouse gas emissions. It can benchmark the performance of one building or a whole portfolio of buildings, all in a secure online environment.

By inputting a year’s worth of monthly IT and total building energy use into Portfolio Manager, data center operators can:

- Compare their data center’s energy efficiency to others. Portfolio Manager generates a score from 1–100 relative to hundreds of other data centers nationwide.
- Earn the ENERGY STAR certified building designation if a data center generates a score of 75 or above.
- Estimate the data center’s carbon footprint. Portfolio Manager calculates the building's greenhouse gas emissions – including carbon dioxide, methane, and nitrous oxide – consistent with the Greenhouse Gas Protocol.
- Track and report progress at the data center. Portfolio Manager allows you to examine data center energy use over time, evaluate savings from retrofit measures, and generate a Statement of Energy Performance (SEP) report.

7.0 FINANCIAL STATUS REPORT (SAMPLE)

Team MicroTech has more than 12 years of experience delivering IT and Telecom solutions to the federal government, reporting all data accurately and thoroughly. We provide a monthly Financial Status Report to the GSA PMO showing the total dollar activity for the month broken down by service types and services. A sample of our monthly Financial Status Report can be seen on the following page.

[redacted]

[redacted]

8.0 BSS RISK MANAGEMENT FRAMEWORK PLAN

As the Prime Contractor for Team MicroTech, MicroTechnologies, LLC has a distinctive understanding of the network and information system security required for the EIS contract. We have worked with our team partners to ensure that they are aware that their networks will carry traffic ranging from non-sensitive programmatic and administrative voice and data; Controlled Unclassified Information (CUI) traffic; and higher-level voice and data traffic, up to and including encrypted Top Secret/SCI traffic. Our network services are protected by anti-virus and anti-malware software, firewalls, identification and authentication controls, security tokens, smart card tokens, and biometrics to name just a few of the available options. We employ role-based access control lists, intrusion detection in the network, product- and application-specific protections, along with environmental controls. Core network services are proactively monitored for system failures that could potentially impact critical communication nodes. Our system security complies with the Federal Information Security Management Act (FISMA); NIST SP 800-36, Guide to Selecting Information Technology Security Products; NIST SP 800-53A R4, Assessing Security and Privacy Controls in Federal Information Systems and Organizations; and DoD and Intelligence Community requirements, as applicable.

8.1 System Security Compliance Requirements

MicroTech and our team partners have carefully evaluated the security requirements related to providing EIS services under this contract and comply with all standards, regulations, DoD, and Intelligence Agency guidance and directives. Our experience supporting other Federal, DoD, and Intelligence Agency customers provides us with an extensive knowledge base, allowing us to deliver EIS services using both industry and federal best practices. We meet ITU security standards for international voice and data communications, particularly those relevant to cybersecurity and incident management, and those for emergency and encrypted satellite communications. Further, we comply with service- and Agency-specific requirements identified in Section C.2 for Cloud Infrastructure as a Service (IaaS), or Managed Trusted Internet Protocol Services (MTIPS).

The list of standards, regulations, guidance, and directives is exhaustive; however, for purposes of this proposal, we restate those identified in the solicitation for this section:

- Federal Information Security Management Act (FISMA) of 2002; (44 U.S.C. Section 301. Information security) 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 (formerly 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", dated August 27, 2004; available at: http://www.idmanagement.gov/.
- Office of Management and Budget (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-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." Dated February 2004.
- FIPS PUB 200, "Minimum Security Requirements for Federal Information and Information Systems." Dated March 2006.
- FIPS PUB 140-2, "Security Requirements for Cryptographic Modules." Dated May 2001.
- NIST SP 800-18 Revision 1, "Guide for Developing Security Plans for Federal Information Systems." Dated February 2006.

- NIST SP 800-30 Revision 1, “Guide for Conducting Risk Assessments.” Dated September 2012.
- NIST SP 800-34 Revision 1, “Contingency Planning Guide for Information Technology Systems.” Dated May 2010.
- NIST SP 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.” Dated February 2010.
- NIST SP 800-40 Revision 3, “Guide to Enterprise Patch Management Technologies.” Dated July 2013.
- NIST SP 800-41 Revision 1, “Guidelines on Firewalls and Firewall Policy.” Dated September 2009.
- NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems.” Dated August 2002.
- NIST Special Publication 800-53 Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations.” Dated April 2013.
- NIST Special Publication 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations, Building Effective Assessment Plans.” Dated December 2014.
- NIST SP 800-58 “Security Considerations for Voice Over IP Systems.” Dated January 2005.
- NIST SP 800-60 Revision 1, “Guide for Mapping Types of Information and Information Systems to Security Categories.” Dated August 2008.
- NIST SP 800-61 Revision 2, “Computer Security Incident Handling Guide.” Dated August 2012.
- NIST SP 800-88 Revision 1, “Guidelines for Media Sanitization.” Dated December 2014.
- NIST SP 800-94 “Guide to Intrusion Detection and Prevention Systems.” Dated February 2007.
- NIST SP 800-128 “Guide for Security-Focused Configuration Management of Information Systems.” Dated August 2011.
- NIST SP 800-137 “Information Security Continuous Monitoring for Federal Information Systems and Organizations.” Dated September 2011.

- NIST SP 800-144 “Guidelines on Security and Privacy in Public Cloud Computing.” Dated December 2011.
- NIST SP 800-160 “Systems Security Engineering.” Dated November 2016.
- NIST SP 800-161 “Supply Chain Risk Management Practices for Federal Information Systems and Organizations.” Dated April 2015.
- NIST SP 800-171, “Protecting Controlled Unclassified Information in the Nonfederal Information Systems and Organizations.” Dated June 2015.
- Committee on National Security Systems (CNSS) Policy No. 12, National Information Assurance Policy for Space Systems Used to Support National Security Missions. Dated 28 November 2012.
- Committee on National Security Systems (CNSS) Policy No. 15, National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems. Dated 1 October 2012.
- Committee on National Security Systems Instruction (CNSSI) No. 1253, Security Categorization and Control Selection for National Security Systems. Dated March 2012.
- Committee on National Security Systems Instruction (CNSSI) No. 5000, “Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony.” Dated October 17, 2016.
- Department of Defense Instruction (DODI) 8500.01 “Cybersecurity.” Dated 14 March 2014.
- DODI 8510.01 “Risk Management Framework (RMF) for DOD Information Technology (IT).” Dated 12 March 2014.
- Department of Defense (DOD) Cloud Computing Security Requirements Guide (SRG). Draft Dated 7 December 2014.
- ICD 503, “Intelligence Community Information Technology Systems Security: Risk Management, Certification and Accreditation.” Dated 15 September 2008.
- ICD 703, “Protection of Classified National Intelligence, Including Sensitive Compartmented Information.” Dated 21 June 2013.

- ICD 704, “Personnel Security Standards and Procedures Governing Eligibility for Access to Sensitive Compartmented Information and Other Controlled Access Program Information.” Dated 1 October 2008.
- ICD 705, “Sensitive Compartmented Information Facilities.” Dated 26 May 2010.
- ICD 731, “Supply Chain Risk Management.” Dated 7 December 2013.
- Other agency-specific policies, directives and standards as identified at the TO level.

8.2 Security Compliance Requirements

Team MicroTech’s network systems infrastructure meet the requirements of FIPS 200, Minimum Security Requirements of Federal Information and Information Systems. Signed into law in December 2002, FIPS 200 recognized the importance of information security to the economic and national security interests of the United States. Title III of the E-Government Act, the Federal Information Security Management Act (FISMA), articulated the need for each Federal Agency to develop, document, and implement an enterprise-wide information security for the data and information systems that support Agency operations and assets, including those provided or managed by another agency, contractor, or an external source.

FIPS 200 correlates to NIST SP 800-53A R4, which specifies “state-of-the-practice” security controls for Federal information systems. Security controls are to be reviewed by NIST at least once a year, after which the controls may be revised or extended to implement the experience gained with the existing controls; meet changing security requirements in the Agency; and/or implement new security technologies to enhance the Agency’s security posture. Proposed deletions, additions, and/or modifications to the Agency’s security controls, and any recommended changes to the security control baselines will undergo a thorough review to obtain feedback to build consensus for any changes; up to one year to comply fully with the changes. However, they are encouraged to initiate compliance activities immediately.

Security requirements and standards continually evolve in response to emerging threats and incursions to Government network services. In addition, new services such as Cloud IaaS require security in depth to meet NIST, DoD, Homeland Security, and Intelligence community standards and directives. The Federal Risk and Authorization Management Program (FedRAMP) furnishes a cost-effective, risk-based approach for the adoption and use of cloud services. Team MicroTech and our carrier partners understand the minimum security requirement is for a “Moderate Impact Level”, as specified under FedRAMP and are prepared to provide the requisite security controls required for compliance. FedRAMP is implemented at the task order level by the individual Agencies, and not as a contract requirement by the GSA.

According to the Executive Summary in the pamphlet, Guide to Understanding FedRAMP, the program offers Executive departments and agencies the following support for Cloud services:

- Standardized security requirements for the authorization and ongoing cybersecurity of cloud services for selected information system impact levels.
- A conformity assessment program capable of producing consistent independent, third-party assessments of security controls implemented by Cloud Service Providers (CSPs).
- Authorization packages of cloud services reviewed by a Joint Authorization Board (JAB) consisting of security experts from the DHS, DOD, and GSA.
- Standardized contract language to help Executive departments and agencies integrate FedRAMP requirements and best practices into acquisition.
- A repository of authorization packages for cloud services that can be leveraged government-wide.

Team MicroTech complies with all FedRamp requirements at the time the Cloud service is included in our service capabilities.

8.3 Security Assessment and Authorization (Security A&A)

Team MicroTech’s carrier partners’ network information systems will undergo the Government’s Security Assessment and Authorization (Security A&A) before storing, transporting, or processing Federal Government data. The Security A&A will be performed in accordance with NIST SP 800-37, R1. The Risk Management Framework thereunder, provides a disciplined and structured process that integrates information security and risk management activities into the system development life cycle. Software applications, such as database applications and Web applications hosted by an information system, are included in the Security A&A process since application security is critical to the overall security of the system. We understand and acknowledge that our network information systems must have a valid Security A&A before any Agency can award a TO under the EIS contract. We further understand that failure to maintain a valid A&A will be grounds for terminating a TO.

8.4 System Security Plan (SSP)

Our network systems comply with all Security A&A requirements, as mandated by Federal laws, policies, and directives. The A&A addresses necessary system/network documentation, physical access controls to network assets, including logical access. Our processes and procedures comply with NIST SP 800-18, R 1; and the system's FIPS Pub. 199 categorization. The System Security Plan (SSP) are prepared in accordance with NIST SP 800-18, R1 and any other applicable standards and regulations.

The SSP provides a detailed accounting of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The SSP will also detail responsibilities and expected behavior of personnel who access the system. Viewed as the documentation for the process of planning adequate, cost-effective security protection for the system, the SSP should reflect input from various managers with responsibilities concerning the system, including information owners, the system owner, and the Agency's Senior Information Security Officer.

The SSP details our approach to providing compliant security to all network and information systems we interconnect with on the EIS contract. The SSP includes all appendices and attachments related to each specific TO we are awarded on EIS.

8.5 System Security Plan Deliverables

Each task order specifies the required security deliverables for that TO. Documents are delivered to the Ordering Contracting Officer (OCO); the Information System Security Officer (ISSO); or the Information System Security Manager (ISSM) when required following TO award, and then provided quarterly and/or annually as updates. Significant system updates, as articulated in NIST SP 800-37, require a related revision to the SSP deliverables, as required by the Contracting Officer or designated representative.

8.6 Additional Security Requirements

Team MicroTech's PMO prepares and delivers all required deliverables with the appropriate security markings, ranging from Controlled Unclassified Information (CUI) to

Top Secret/SCI, in accordance with classification regulations. External transmission of CUI data to or from an agency computer are encrypted. Certified encryption modules are used in accordance with FIPS PUB 140-2, Security requirements for Cryptographic Modules. We understand and acknowledge that the Government has the right to perform manual or automated audits and other inspections of our IT and network systems carrying voice or data traffic for the Government; scheduled or unscheduled. In accordance with FAR Section I, 52.239-1, we maintain the following privacy and security safeguards:

- Team MicroTech does 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 TO or otherwise provided by the government. Exception - Disclosure to a Consumer Agency for purposes of security assessment and authorization verification.
- To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, availability, and confidentiality of any non-public government data collected and stored by the contractor, the contractor shall afford the government logical and physical access to the contractor's facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request. Automated audits shall include, but are not limited to, the following methods: authenticated and unauthenticated operating system/network vulnerability scans; authenticated and unauthenticated Web application vulnerability scans; authenticated and unauthenticated database application vulnerability scans; and internal and external penetration tests.
- Automated scans can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools. In these cases, scanning tools and their configuration shall be approved by the government. In addition, the results of contractor-conducted scans are provided, in full, to the government.

8.7 Personnel Background Investigation Requirements

Ensuring the security and integrity of our IT and network assets is critical to our success as a prime contractor. Team MicroTech conducts thorough background investigations on all personnel supporting systems carrying Government voice and data traffic. We work with the Agency's senior security officials, including the head of the Agency, the designated Risk Executive, the CIO, the Information Owner, and the Senior Information Security Officer to ensure our staff members meet security standards, regulations, and directives for interacting with Government systems and information. Background investigations are compliant with Homeland Security Presidential Directive-12 (HSPD-12) Office of Management and Budget (OMB) guidance M-05-24, M-11-11, *Continued Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors*, and as specified in agency-identified security directives and procedural guides. Team MicroTech also complies with the directives of the National Industrial Security Program Operating Manual (NISPOM), compiled May 2, 2014, or its latest revision. The NISPOM guides the issuance of security clearances, which we carefully monitor throughout the life of the contract; paying particular attention to Chapter 7, Subcontracting, which specifies our responsibilities as Prime Contractor for the EIS Program. We also pay strict attention to Chapter 9, Special Requirements, which discusses international requirements and personnel security clearances.

In accordance with Section G.9.3 Team MicroTech will identify the:

- Security POCs that will be processing background investigations and security clearances at the appropriate levels per Sections C.1.8.7.7 and G.5.6.
- POCs that have passed national agency checks or background investigations, and the security clearance levels held by these as defined in Section G.5.6.

9.0 NS/EP FUNCTIONAL REQUIREMENTS IMPLEMENTATION PLAN

The National Security/Emergency Preparedness (NS/EP) program of the United States institutes a national response to Federally declared emergency circumstances/crises, whether local, national, or international, that cause, or could cause, injury or harm to the populace; damage to or loss of property; or that degrades or threatens our nation's ability to respond in situations of natural or man-made disasters and emergencies. The core of the nation's NS/EP capability is the infrastructure that makes up our national telecommunications system. Emergency Preparedness policies mandate that telecommunications carriers and alternative providers maintain a telecommunications capability always in a state of readiness to meet the needs of authorized Government users as permitted by law (Federal, state, local, and tribal) during National Emergencies. Therefore, the networks of Offerors to EIS are required to be maintained in a state of readiness for any emergencies. The detailed specifications of NS/EP requirements are described in Sections G.11.1 through G.11.3. Each carrier's NS/EP Plan must be updated annually.

Telecommunications requirements for NS/EP are based on a set of policies and procedures originally established by the National Communications System (NCS), now the Office of Emergency Communications (OEC) under Executive Order 12472, and currently operational under EO 13618, Assignment of National Security and Emergency Preparedness Communications Functions, dated 06 July 2012. NS/EP was developed to ensure critical Government and industry needs are met when an actual or potential emergency threatens the security or socio-economic structure of the U.S. To meet these NS/EP telecommunications requirements the OEC maintains the Government Emergency Telecommunications Service (GETS), EIS is required to support GETS. Furthermore, because EIS service extends into thousands of Government offices throughout the country, the EIS networks represent a key resource for coping with emergency and disaster situations.

This NS/EP Plan was prepared by MicroTech, serving as the Prime Contractor leading a team of telecommunication carriers including [redacted] [redacted] in accordance with the requirements of this solicitation, and applicable Federal policies and Executive Orders, including 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.

In the following sections, MicroTech addresses the functional requirements for NS/EP services. We will draw on our partners' knowledge of the current telecommunications environment to fulfill the 14 requirements specified by the GSA. As the Prime Contractor we are aware of our responsibilities to meet and exceed the Government's needs. We manage our EIS partners to ensure their telecommunication services are always in a state of readiness to respond to an emergency or crisis. If an event impacts the immediate availability of our team's network resources, we will inform the GSA CO. We apply all necessary resources to return the out-of-service portion of our network to full service as soon as possible. MicroTech's Program Manager, [redacted] brings more than 13 years of experience in program management services in a telecommunications operations environment on programs held with DoD. We acknowledge that while the GSA CO sets priorities, network operations are MicroTech's sole responsibility.

9.1 Basic Functional Requirements

Enhanced Priority Treatment: In the event of a national disaster or emergency, the Federal Government will invoke the NS/EP priority use of voice and data communications. [redacted] MicroTech's NS/EP Call Completion Service (NCCS) capability will provide the following features to NS/EP critical users:

- When a busy condition occurs, [redacted]
- NCCS [redacted] NCCS architecture [redacted] This ensures all NS/EP critical users are not impacted by a catastrophic NCCS node failure.

- All critical users' on-net calling in the MicroTech network is protected from restrictive network management controls. [redacted] If calling into a disaster area is restricted by terminating switch controls, EIS on-net critical calls are not affected by those controls.
- If the only off-net service is provided by non-digital service, [redacted] is used to place NS/EP calls for EIS NCCS users.

MicroTech will work with the Government to identify key EIS Government locations which must be accessible during crisis situations and review the use of diverse, dedicated Service Data Point (SDP) access trunks; dual-homed, dedicated SDP access trunks; dedicated overflow trunks; and overflow to the PSTN. These capabilities ensure multiple network paths are available for call termination to a particular SDP, thus enhancing the call routing through the EIS network for critical users.

Service capabilities specified in this document are not intended to replace capabilities provided under GETS or any other Government contracts, but assure EIS contract services, as a result of the networks' characteristics and the use of prudent emergency contingency planning, provide EIS critical users availability and reliability during national emergencies that is comparable to the service provided during normal conditions.

The following definitions are used in this section:

- C*ontractor's EIS network*: All infrastructure, SDP to SDP, used by MicroTech to provide EIS services, whether or not that infrastructure is owned by us, but excluding the access portions of an end-to-end circuit when circuit-switched access is used.
- *Critical users:* Key Government officials whose positions requires special access and network treatment to assure telecommunications services during emergencies. It is estimated that the number of EIS critical users will not exceed 10,000, and for the purposes of traffic analyses we assume they are distributed uniformly among the population that utilizes SVS.

Secure Networks: Team MicroTech has developed, adopted, and implemented a broad range of security mechanisms and procedures to protect the integrity of our network systems and ensure the availability of transmission services to our customers.

[redacted]

Team MicroTech will maintain an active dialogue with EIS users, industry, and commercial customer organizations on network security issues. For example, MicroTech senior staff members participate in the Network Security Information Exchange (NSIE). Within MicroTech, the security organizations are tightly coupled and meet frequently to discuss the latest threats and security techniques.

This section elaborates on many of the network security mechanisms and procedures adopted by Team MicroTech. In particular, [redacted] We are confident these measures are sufficient to protect the network against known threats and must continue to evolve to meet new challenges.

MicroTech Security Manager: MicroTech designates a Network Security Manager to support the PMO as the primary contact for all security-related matters. As a member of MicroTech's senior security staff, she offers a broad base of security and related experience including managing and executing contract-based security services for Government customers in areas such as electronic, physical, investigative, and DoD-required security. Our Security senior staff members will interact with the EIS PMO in all areas of physical and electronic security associated with contract services, and meet with EIS PMO personnel to address security policies and procedures for network services. Our Security Officer has access to all corporate resources to resolve security issues and provide updated security information as an element of our Program Management Reports.

Summary of Security Features and Procedures: Team MicroTech's networks are guarded by several layers of protection. [redacted]

[redacted] Network safeguards will ensure all problems are isolated to a small portion of the network, and redundant systems will provide for the rapid restoration of all affected services.

Denial of Service Attacks: Protection from denial of service attacks is a critical requirement of any public network. In the National Communications Systems (NCS) report entitled "Electronic Intrusion Threat to National Security and Emergency Preparedness Telecommunications," a number of malicious attacks are associated with denial of service including:

- Jamming
- Manipulated overloads
- Induced system crashes
- Spoofing
- Computer virus
- Unauthorized message injection.

The following sections describe the mechanisms that protect the MicroTech transmission network from these attacks.

Protection from Jamming. Most services required for the EIS Program will be provided over fiber optic facilities, which are not susceptible to jamming attacks. [redacted]

Protection from Spoofing. Modern telecommunications networks rely on computer systems, and unprotected computer systems are subject to spoofing techniques, such as address forgery. Team MicroTech's computer systems and networks incorporate mechanisms that minimize this type of attack.

Our security policies minimize or strictly prohibit untrusted relationships. [redacted]

Protection from Manipulated Overloads. Manipulated overload attacks are typically used to congest the bearer channels of a network. For private line services, such as those being requested for the EIS PMO, [redacted]

Protection from Computer Viruses. [redacted]

Protection from Induced System Crashes. Induced system crashes are prevented by techniques [redacted] Individual users and application programs operating on mid-range and mainframe computing systems have only the privileges and priorities necessary to perform specific tasks. [redacted] In the event a system crash occurs, [redacted]

Protection from Unauthorized Messages. The bandwidth provided by private line services is not subject to unauthorized message injection except at the user facility. [redacted]

Authorized Access: Identification and authentication mechanisms will promote and support controls used to protect the network against a variety of threats including unauthorized access at the system interface and system resource levels. Our security requirements apply to direct system users, remote users, and machines.

Identification. System users, including individual users and remote machines, are uniquely identified for individual accountability. [redacted]

Authentication. When remote access is required, our network security systems incorporate and use [redacted]

Password Requirements. Security features are not restricted to static password mechanisms to authenticate user identities. Other methods such as smart cards, one-time only passwords, cryptographic-based authentication, and biometrics provide stronger authentication and are required for remote access and some local access to sensitive systems.

Network security systems do not facilitate explicit sharing of passwords nor do they provide any indication that a password is already associated with another user ID.

[redacted]

[redacted]

Data and system integrity features protect against unauthorized or undesired access and modifications of EIS network management data and records, [redacted]

[redacted]

Transport of Government-encrypted Classified Information: Team MicroTech's network is certified to transmit classified voice and data traffic including Top Secret as requirements are identified. The security discussion presented in Section G.11.1.2.2, and in greater detail in our Technical Proposal, details our incorporation of a robust suite of products and technologies that will protect classified information. [redacted]

Non-Traceability: The security architectures of Team MicroTech's networks meet the Secure Communications Interoperability Protocol (SCIP) requirements for secure voice communications. SCIP operates over a variety of communications systems, including commercial land line telephone service, communication satellites, VOIP, military radios, and a number of cellular telephone standards.

[redacted]

[redacted]

[redacted]

Team MicroTech’s security for NS/EP data communications is established under the FISMA, and governed by NIST SP 800-53A R4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations*. Our network security architecture integrates a layered security model, similar to that shown in **Figure 30**.

[redacted]

Figure 30: Model of a Secure Network Architecture. *Offering layers of protection for information residing on the Agency’s systems, Team MicroTech will emphasize the use of firewalls and redundancy in critical network components.*

NIST SP 800-53A R4 provides Agencies with security controls to manage their information systems and operating environments; and enables the resiliency to overcome cyber threats from a variety of sources. NIST SP 800-53 R4 emphasizes the use of tools and applications suitable to continuous monitoring of the Agency’s systems. It further accentuates providing comprehensive information to Agency decision makers who must make risk-based decisions in real-time situations. NIST SP 800-53A R4 correlates to FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*; and NIST SP 800-39, *Managing Information Security Risk*.

As our team is made up of many different carriers and they all utilize their software and hardware differently, we will be able to provide the necessary detail upon task order award to address the NS/EP requirements.

Network and Service Restorability: Restoration of NS/EP services is always done on a priority basis. Whether an outage is the result of a fiber cut, an incursion, or a disaster, Team MicroTech has the resources to reroute existing service, and the experienced field technicians to repair a fiber outage on location. We will provide incident analysis and assessment in order to determine the scope and impact of all incidents. When an Agency suspects an incident they can call our 24x7x365 NOC and report it. [redacted] We use commercial products that meet or exceed Security Level 1 and Security Level 2 FIPS 140-2 standards, *Security Requirements for Cryptographic Modules*. [redacted] Our practices meet or exceed all recommendations provided within IETF RFC 2350, *Expectations for Computer Security Incident Response*. Remediation will occur in line with our established practices and our agreement with the affected Agency.

Other types of emergencies such as hurricanes, floods, tornadoes, or forest fires receive the level of priority service based on the scale of the emergency. Team MicroTech has disaster teams specially trained to meet extreme situations, and they are equipped with the necessary tools, portable living quarters, and tractor-trailers equipped with wireless or satellite telephone connectivity so they can provide service to residents once they reach the scene. They will coordinate directly with FEMA, and state and local emergency personnel and law enforcement; assess damage to company assets and switches; and begin repairs immediately. In the event our network experiences significant degradation or failure, we will provide priority restoration of the affected service in accordance with the TSP system five levels of priorities.

International Connectivity: Often, emergencies extend beyond US borders. NS/EP communications are used by “on-the-ground” professionals from the State Department, the Armed Forces, and other Government Agencies to convey conditions about disasters and other situations. These transmissions must be done with the utmost clarity and security, particularly when US citizens may be in harm’s way.

[redacted] They have agreements in place in many areas of the world, and understand the importance of secure NS/EP communications. Both carriers have experience in supporting the US and other international governments with secure voice and data services. [redacted]

We routinely provide solutions that integrate services into existing network environments with minimal disruption and near perfect interoperability. We will connect to and interoperate with Agency networking environments, including DMZs and secure LANs, as required. Our service will support connectivity to extranets and the Internet.

Interoperability: Team MicroTech carriers offer voice and data services that will interconnect and interoperate with other telecommunications networks, including US and foreign government and private facilities. We meet Government-specified terminations such as single-line telephones, STE, multi-line key telephone systems, conference-room audio equipment, PBX, Centrex, T1 MUX, modem, FAX, and video teleconferencing systems. [redacted] Our carriers maintain their own interoperability arrangements and we will act as the coordinator for services when interconnections and interoperability with external systems is required.

Mobility: Protection of telecommunications and automated information systems is imperative to prevent exploitation through unauthorized electronic access, interdiction, or other intelligence threats. [redacted]

The use of smart phones, satellite communications, tablets, laptops, and other mobile devices dictates that security must be more than an application on a device; it must be powerful enough to prohibit intrusion wherever the Government user is. At the same time, it must enable communications necessary to make effective decisions and can be re-provisioned and redeployed if the situation requires. Team MicroTech's networks support mobile voice, data, and video services for Government Agencies, using the Advanced Encryption Standard (AES). The AES algorithm's *Cipher Key* is a sequence of 128, 192, or 256 bits. No other input, output, or Cipher Key lengths are permitted by the standard. AES allows mobile voice, video, and data communications to be encrypted up to Top Secret, depending on NSA authorization.

Under the DoD's Cryptographic Modernization Program, newer, safer mobile products are coming on line that use more advanced encryption. An example of this technology is the AN/PRC-148 hand-held radio which uses multiple encryption modes. Another recent encryption device is the High Assurance Internet Protocol Encryptor, or HAIPE, a Type 1 encryption device that meets the NSA's HAIPE Interoperability Specification (IS).

Coverage: Team MicroTech's partners, [redacted] have the infrastructure and carrier relationships to provide NS/EP services to our national security executives both in the US and OCONUS to meet emergency situations. We will ensure that intra-agency emergency services are interoperable on our networks, including voice, data, and video connectivity. If an incident requires our field technicians to provide on-the-scene support, we will dispatch them in under 24 hours. Our primary contact with the Government will be our Director of Emergency Operations, who will travel to the scene to coordinate our response. We will work with DHS through the NCC Watch, FCC, ESF-2 FEMA, law enforcement, and National Guard and other military forces who may respond. We will provide satellite communications in the event land-line and cellular services have been disrupted. If the emergency is both international and political in scope, we will provide secure transmission for national security communications among the Office of the President, the DoD, and US national security agencies.

Survivability/Endurability: Our nation's domestic and international telecommunications resources, including commercial, private, and government-owned facilities and services, are essential components in our national security policy and strategy. This infrastructure must be survivable to sustain our national security leadership: the President. Supporting him/her in those responsibilities are heads of our Military, Intelligence, and State Departments; and Commerce, Energy, and Homeland Security. Critical objectives will be maintenance of command and control of the military forces, and providing for continuity of government and its essential services to the population. Current national policy requires that the nation's telecommunications support the continuity of the Government and recovery of the citizenry during and after any national emergency. DHS's Office of Emergency Communications (OEC) ensures that the policies required by these directives are carried out.

Under NS/EP, disasters are categorized in three degrees:

- Natural, manmade, or civil disasters, largely local in scope, include incidents such as storms, floods, tornadoes, wildfires, hurricanes, earthquakes, and volcanic eruptions. Other types of limited disasters include chemical spills, unexpected explosions, and riots with major vandalism or other civil disturbances. They can also include nuclear power plant failures and accompanying nuclear waste discharges. State and local respondents, including the National Guard, are usually the first on the scene to assess damage. They reach out to national-level entities to support recovery. Federal support may be limited, other than financial, depending on the scale of the emergency, but agencies such as FEMA will help coordinate the delivery of telecommunications equipment to rapidly restore service.

- “Limited” nuclear incidents, categorized as having fewer than ten sites, in which the damage is limited to specific geographical areas. In contrast to category one above, roads leading from the impacted areas will be crowded to the point of impassability. Governmental authorities in the affected regions will be disrupted and avenues of communication will be nonfunctional. The Federal Government will lead the recovery efforts to restore communications by rerouting the nation's communications and electrical infrastructure around the impacted zones, in tandem with maximizing medical aid and removal of contaminated materials so reconstruction can begin in the stricken areas. Once the contaminated materials are removed, telecommunications infrastructure can be restored as well.
- The worst case scenario is survivability of Government and citizens in a major nuclear war. The US maintains secure communications facilities across the country and partners with allies around the world to ensure that telecommunications are designed specifically for survivability. The OEC prioritizes the restoration of communications services. Its authority applies in the period starting a minute or two after the end of the mass bombing. The OEC’s view is that the disruption and destruction of power and communications facilities; the data needed to reconstruct communications hardware; and lines of authority will be so complete planners assume it could be impossible to plan and pre-install a communications infrastructure effective over the broad areas of responsibility of the President. It is possible, however, to plan for survivability of systems that meet specific objectives, such as the wartime needs of the President as Chief Executive. The immediate need will be to determine whether the Government survived, and if not, what comprises the next tier of national authority to initiate a national response. Medical and military responses will be primary. Infrastructure

restoration follows to ensure electrical power, telecommunications, and civil services are reconstituted.

Team MicroTech's communications carriers actively participate in the NS/EP program, and will respond to the Government's emergency preparedness requirements. [redacted]

Voice Band Service: Team MicroTech will provide secure, encrypted, priority voice service for Presidential communication, primarily through our Circuit Switched Voice Service (CSVS). We bring more than 15 years of expertise in delivering circuit switched voice services, including circuit orders to DISA, VA, and hundreds of commercial customers located throughout the US and internationally.

[redacted]

Our carrier relationships ensure we deliver the highest quality of service to all of our customers. We will endeavor to exceed service levels when possible, always meet existing service levels on a daily operational basis, and look to identify risks before impact.

However, there are some instances where geographic challenges can impede service delivery. In these rare instances, Team MicroTech will work with the GSA to find suitable solutions at minimal impact to the existing user environment. Our partners will provide encrypted satellite-based communications for the President when he travels internationally. Details of our voice services can be seen in Section 2.2.2 of Volume 1.

Broadband Service: Team MicroTech is fully prepared to provide broadband services including Web access, video, multimedia, and imaging. [redacted] Virtual Private Network Service (VPNS) provides secure and reliable transport of agency applications across their, and its transport providers', high-speed, unified, multi-service IP-enabled backbone infrastructure. The main characteristic of VPNS is that all infrastructure and devices involved in implementing the VPN are [redacted] Tunnels terminate at [redacted] network will connect Government locations with trusted business partners for site-to-site access or broadband for remote access, to provide direct connectivity between all sites as a partially or fully-meshed WAN. [redacted]

In [redacted] backbone we can provide three basic solutions for VPNS:

- Intranet – provides secure tunnels between remote sites, using broadband or dedicated access.
- Extranet – enables trusted business partners to gain access to corporate information via secure/encrypted tunnels using broadband or dedicated access.
- Remote Access – enables mobile/remote workers to gain access to secure corporate information via secure encrypted tunnels such as IPsec and TLS.

[redacted] VPNS complies with all mandatory requirements listed below:

- Applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and authorized to allow for inspection.
- Multiple tunneling standards, as required by an agency. Examples include L2TP, GRE, IP-in-IP, MPLS, IPSec, and TLS.
- Various encryption levels, as required by an agency. Examples include 3DES, RC4 and AES in accordance with the appropriate FIPS publications and modules.
- Authentication services as required by an agency. Examples include RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates.
- Support IPv4 and IPv6 as both the encapsulating and encapsulated protocol.
- Support QoS in the following standardized modes:
    - Best effort
    - Aggregate Customer Edge (CE) Interface level QoS (“hose” level)

  - Site-to-site level QoS (“pipe” level)
  - Intserv (RSVP) signaled
  - Diffserv marked
- Support QoS across a subset of the access networks as listed below:
  - 802.1p Prioritized Ethernet
  - MPLS-based access
  - Multilink Multiclass PPP
  - QoS-enabled wireless:
    - LTE
    - Wireless 802.11.x
    - Cable high-speed access (DOCSIS 1.1)
    - QoS-enabled Digital Subscriber Line (DSL)
    - QoS-enabled Satellite Broadband Access

Scalable Bandwidth: Scalable bandwidth is the result of communications technology such as 4G LTE, and is the modulation method for second-generation Broadband Wireless. It combines both upstream access and modulation, and is based on Orthogonal Frequency Division Multiple Access, or OFDMA, which in turn is based on multiple orthogonal sub-carriers.

OFDMA offers up to an 18dB gain in the upstream link budget and up to a 12dB gain in the downstream link budget relative to traditional multiple access technologies. These gains are complemented by the capability to operate in severe non-line-of-sight conditions. Armed with these advantages, OFDMA enables deployment of integrated indoor BWA subscriber units (SU).

The value to the Government of scalable bandwidth is its ability to expand to allow more calls and callers in emergency situations, which is ideal when NS/EP communications are used.

OEC can coordinate with carriers to ensure that enough bandwidth is available to meet whatever emergency has arisen. Under OEC regulatory authorities the Government can take temporary control of carrier assets to allow top security and critical Agency officials to be in constant communications with any of their resources on the scene.

9.2 Protection of Classified and Sensitive Information

Team MicroTech understands that for the planning, management, and operations for the NS/EP we have access to sensitive and classified materials, including hardcopy and electronic media. We will comply will all NISPOM and NSA-approved standards for the identification and safeguarding of classified information, including a classification of Top Secret/SCI, as identified by the government in support of the EIS requirements. [redacted]

9.3 Department of Homeland Security Office of Emergency Communications Priority Telecommunications Services

Team MicroTech executes a NS/EP assurance plan that fully complies and interoperates with DHS for GETS, WPS, and TSP activities as well as facilitates interaction with OEC and NCC operations, and when released, NGN-PS. The plan outlines coordination between the GETS and WPS offices with carrier engineering staff to assure customer availability of these services either through specific network modifications or partner agreements. Additionally the plan provides for assurance that NCC Watch operations and capabilities are included, in addition to OCO directed POCs for the agency, in all carriers SOPs regarding government customer services.

Government Emergency Telecommunications Service: Our team will coordinate with the GETS engineering staff to ensure each service provided by each carrier can provide GETS capability. Testing of each service that provides government customers with voice capability will include [redacted]

Wireless Priority Service: Our team will coordinate with the WPS engineering staff to ensure each service provided by each carrier can provide WPS capability. Testing of each service that provides government customers with voice capability will include monthly testing as a component of the PMR. [redacted]

[redacted]

Telecommunication Service Priority (TSP): When TSP is specified in the order, we provide the service in accordance with these telecommunication service priority levels:

- PROVISIONING PRIORITY (5,4,3,2,1, or E),
- RESTORATION PRIORITY (5,4,3,2, or 1),
- BOTH for provisioning and restoration as specified in the order from Service Delivery Point to Service Delivery Point (SDP).

Team MicroTech will restore service in accordance with TSP priority levels designated for transmission service and in accordance with NCS Directive (NCSD) 3-1, TSP System for NS/EP, and NCS Manual 3-1-1 "Service User Manual for the TSP System." We understand that NS/EP, including urgent or emergency delivery order service is negotiated separately on an individual case basis.

Expedited Service. Team MicroTech provides expedited service implementation when ordering agency requires priority provisioning for NS/EP circumstances or other circumstances in which the TSP system is invoked. We make best efforts to implement ordered service(s) by CWD, based on essential priorities as certified by DHS program. Services provided by our carriers to government customers that require provisioning will include a registration of that provisioning with the TSP management office. [redacted] The TSP program will be a key capability in our team's capability assurance plan.