

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 1

Technical

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

1	NETWORK ARCHITECTURE	1-1
1.1	Understanding.....	1-6
1.1.1	Service-Specific Requirements	1-15
1.1.2	General Requirements	1-16
1.1.3	Traffic Routing Requirements.....	1-23
2	TECHNICAL RESPONSE	2-32
2.1	Mandatory EIS Services	2-32
2.1.1	Data Service.....	2-32
2.1.2	Voice Service	2-57
2.1.3	Managed Network Service	2-79
2.1.4	Access Arrangements	2-90
2.2	Optional EIS Services.....	2-103
2.3	Information Security	2-104
2.3.1	System Security Requirements	2-104
2.4	Traffic Identification and Routing Policy	2-105
3	RISK MANAGEMENT FRAMEWORK PLAN.....	3-1
3.1	System Security Compliance Requirements	3-1
3.2	Security Compliance Requirements.....	3-5
3.3	Security Assessment and Authorization (Security A&A)	3-6
3.4	System Security Plan (SSP).....	3-7
3.5	System Security Plan Deliverables	3-7
3.6	Additional Security Requirements	3-8
3.7	Personnel Background Investigation Requirements.....	3-9
4	MTIPS RISK MANAGEMENT FRAMEWORK PLAN.....	4-1
	APPENDIX A. ADDITIONAL MANDATORY ITEMS	A-1
	Voluntary Product Accessibility Template	A-1
	Section 508 Applicability to Technical Requirements	A-1
	Section 508 Provisions Applicable to Reporting and Training	A-1
	Section 508 Additional Information	A-2

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

Approach to Section 508 Compliance	A-2
APPENDIX B. DRAFT RISK MANAGEMENT FRAMEWORK PLAN	B-1
INTRODUCTION.....	B-1
1.0 RMF STEP 1 – CATEGORIZE THE INFORMATION SYSTEM	B-1
1.1 TASK 1-1: Document the Results of the Security Categorization	B-1
1.2 TASK 1-2: Description of the Information System	B-5
1.3 TASK 1-3: Information System Registration	B-6
2.0 RMF STEP 2—SELECT SECURITY CONTROLS	B-8
2.1 TASK 2-1: Identify and Document Common Security Controls	B-8
2.2 TASK 2-2: Select & Document Security Controls in the Security Plan	B-11
2.3 TASK 2-3: Develop Continuous Monitoring Strategy.....	B-14
2.4 TASK 2-4: Review and Approve the Security Plan.....	B-16
3.0 RMF STEP 3—IMPLEMENT SECURITY CONTROLS	B-17
3.1 TASK 3-1: Implement Security Controls Specified in the Security Plan	B-17
3.2 TASK 3-2: Document the Security Controls Implementation and Include a Functional Description of the Security Controls in the Security Plan	B-19
4.0 RMF STEP 4—ASSESS SECURITY CONTROLS.....	B-21
4.1 TASK 4-1: Develop the Security Controls Assessment Plan	B-21
4.2 TASK 4-2: Assess Security Controls in Accordance with Assessment Procedures in the Security Assessment Plan.....	B-23
4.3 TASK 4-3: Prepare the Security Assessment Report	B-25
4.4 TASK 4-4: Conduct Remediation Actions on Security Controls.....	B-26
5.0 RMF STEP 5—AUTHORIZE THE INFORMATION SYSTEM	B-28
5.1 TASK 5-1: Prepare the Plan of Action and Milestones (POA&M)	B-28
5.2 TASK 5-2: Assemble and Submit the Security Authorization Package...	B-35
6.0 RMF STEP 6—MONITOR SECURITY CONTROLS	B-36
6.1 TASK 6-1: Determine the Impact of Proposed System Changes	B-36

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

6.2	TASK 6-2: Schedule Ongoing Security Control Assessments	B-37
6.3	TASK 6-3: Conduct Ongoing Remediation Actions	B-38
6.4	TASK 6-4: Update Key Security Documents	B-38
6.5	TASK 6-5: Security Status Reporting	B-40
6.6	TASK 6-6: Continuous Risk Determination and Acceptance	B-41
6.7	TASK 6-7: Information System Removal and Disposal	B-42

LIST OF FIGURES

Figure 1: Team MicroTech.....	1-4
Figure 2: Proposed External Routing Architecture.....	1-25
Figure 2a: Site-to-Site IPsec VPN with Two VPN Gateways.....	2-36
Figure 2b: Extranet IPsec with Different VPN Endpoints.....	2-37
Figure 3: Illustration of PTSN Gateway Features.....	2-68
Figure 4: Gigabit Ethernet NNI.....	2-95
Figure 5: Physical Interfaces.....	2-95
Figure A-1: 508 Compliance	3
Figure B-1: Step 1 of the Risk Management Framework Plan.....	8
Figure B-2: The ISCM Process.....	15

1 NETWORK ARCHITECTURE

Team MicroTech brings together a team of data service providers that maintain an ability to provide next generation data network architectures and services to the GSA and its Federal and DoD customers. Our partners from around the world address today's technology needs with their infrastructure which allows us to support applications and connecting locations anywhere while driving increased productivity and ease of use throughout world.

As a small business, MicroTech itself, does not maintain the network architectures but with companies like [REDACTED], and others we have the ability to create and integrate the necessary components in order to deliver cost-effective and robust infrastructure services. In response to the GSA request for network architecture details we have included a summary of our major partner's network services and how we are able to meet the government standards of service and the global reach for EIS/GSA. [REDACTED]

MicroTech understands that as the prime contractor, the Government's privity of contract is solely with us and not our subcontractors. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

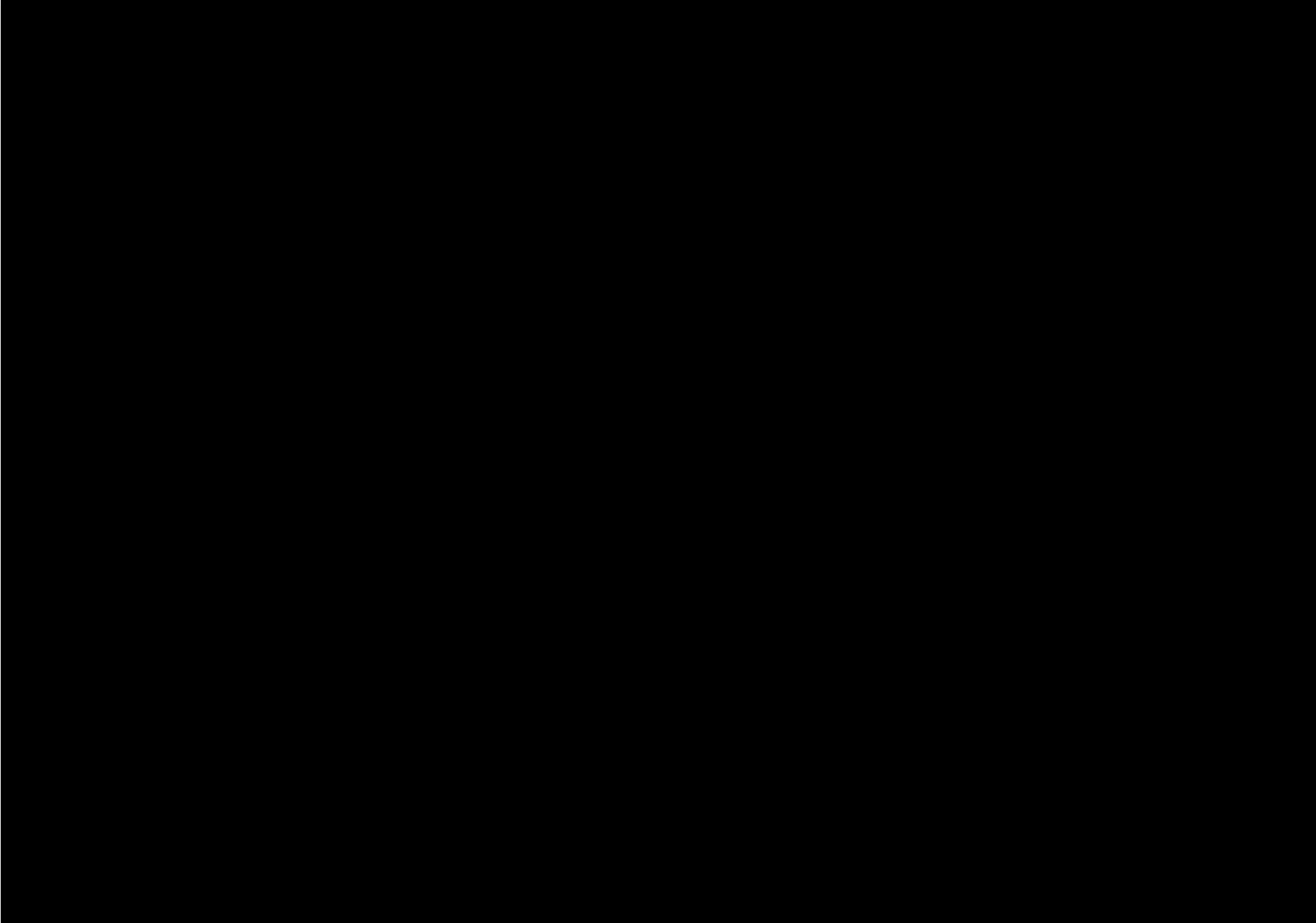
Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

[Redacted text block]

■ [Redacted text block]

■ [Redacted text block]

■ [Redacted text block]



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



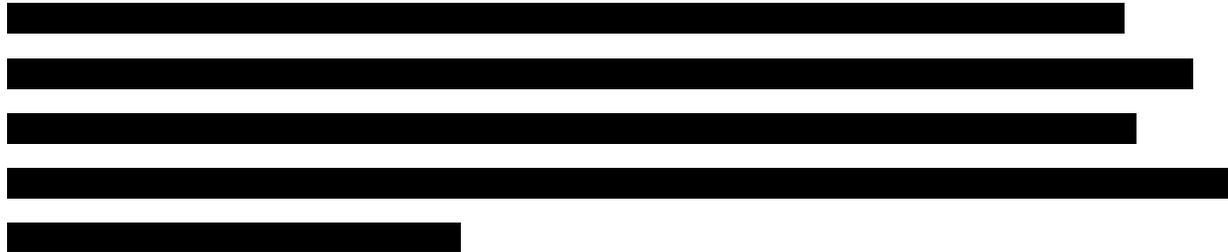
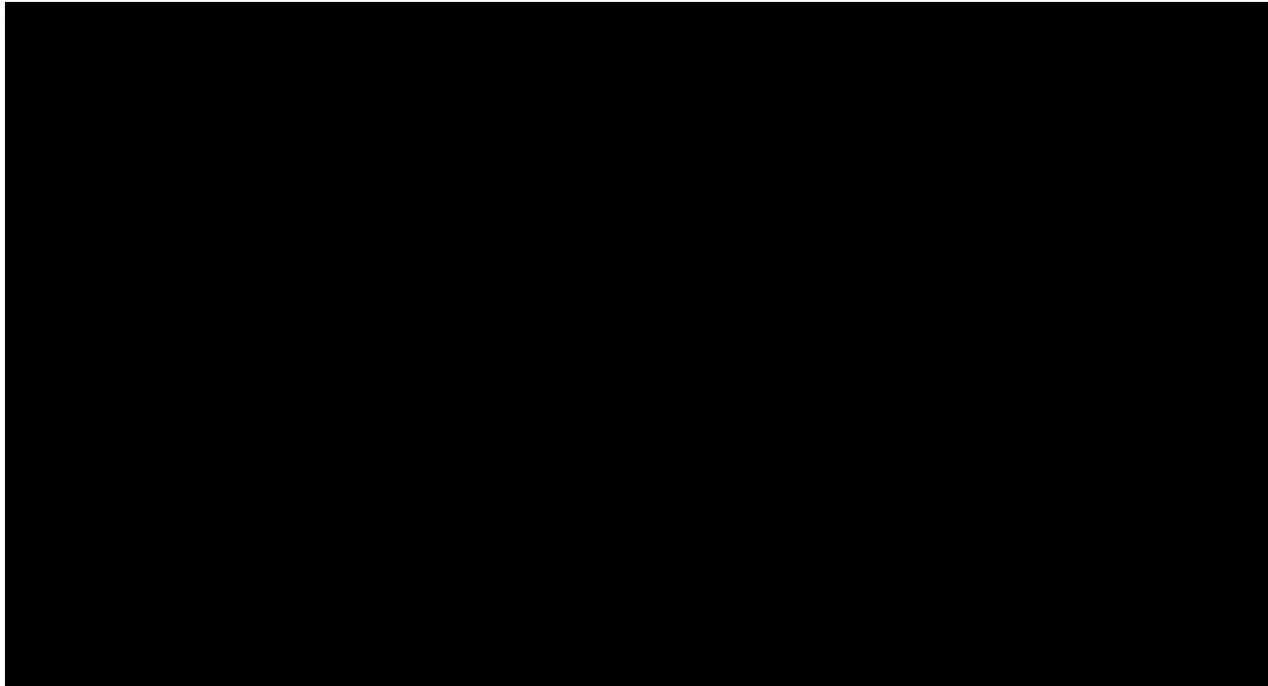
Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

Our approach focuses on the accessibility and understanding of the telecom infrastructure and next generation telecommunications and information technology (IT) infrastructure services. Team MicroTech has the capability to reach all major CBSAs. We have initially focused on supporting the 25 mandatory CBSAs but our reach includes an enormous capability to service OCONUS locations. [REDACTED]

[REDACTED]

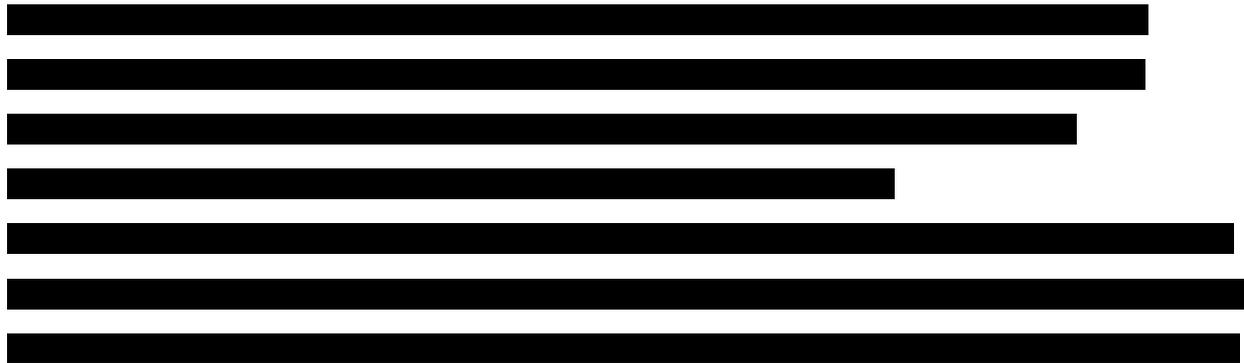
A major concern besides accessibility, is our ability to provide disaster recovery services. We bring a multi-service provider approach to support these often unforeseen circumstances. Our primary goal is to route traffic around an affected area and to assist in recovering communications as quickly as possible. The breadth of teammates gives us a redundancy in many of the CBSAs through different service providers. Our team brings worldwide knowledge and access to the undersea cable plants as well.

[REDACTED]



1.1 Understanding

MicroTech has brought together a team made up of CLECs, consultants, and Service Providers to meet the worldwide EIS service requirements. We work with teammates to provide integration and security approaches focused on the EIS requirements. The following describes some of the architectures that our partners employ to provide their services.



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

[Redacted text block containing multiple lines of blacked-out content]

[Large redacted text block]

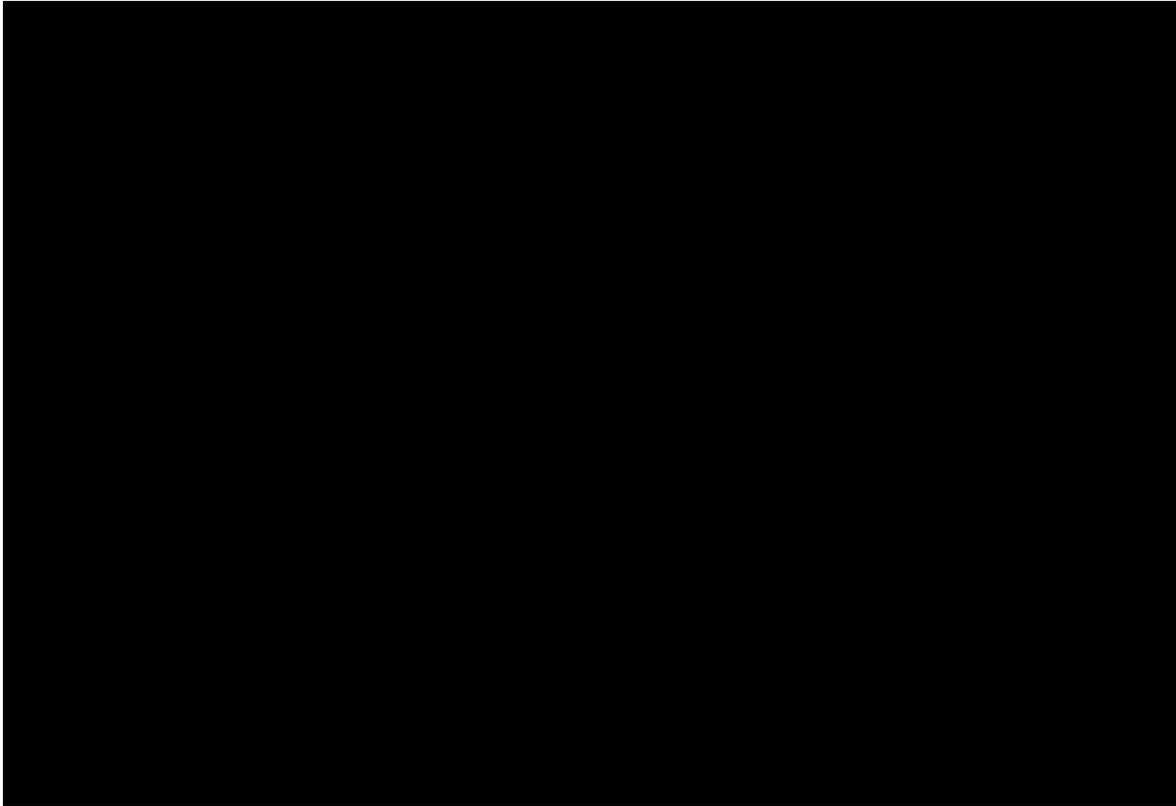
[Redacted text block containing three lines of blacked-out content]

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

[Redacted content]

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

[Redacted content]

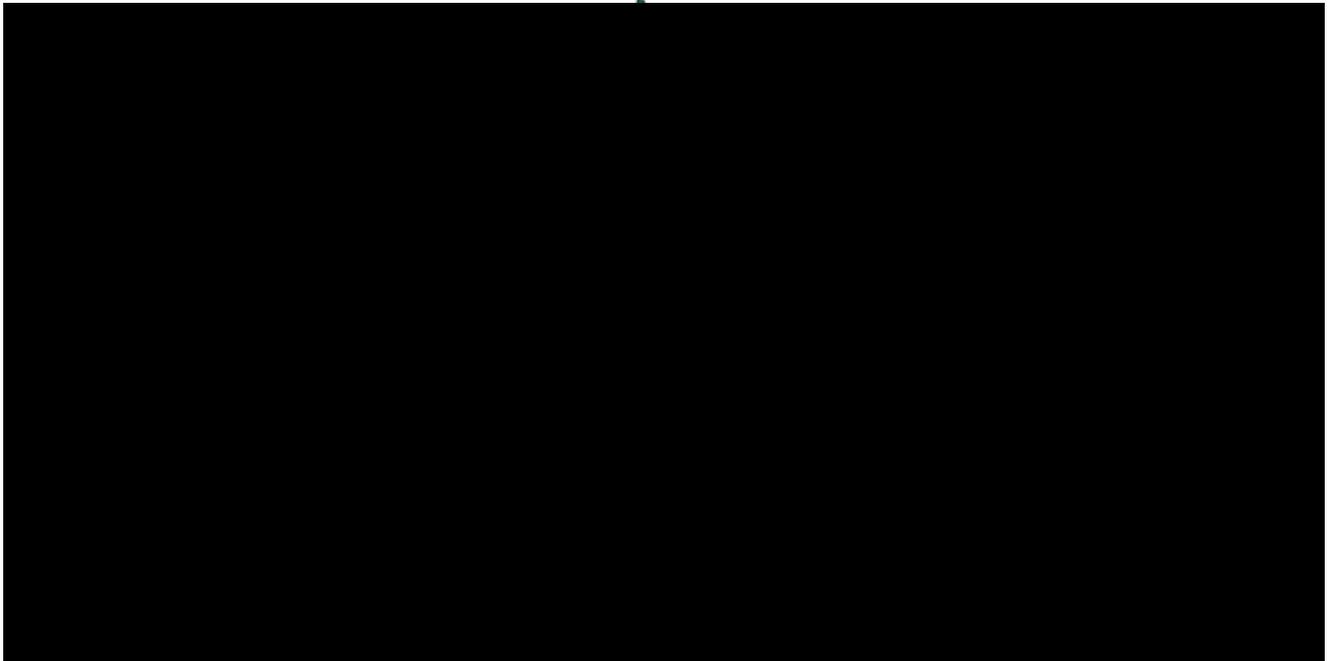


[Redacted text block consisting of approximately 18 horizontal black bars of varying lengths, representing obscured content.]

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



Our team has been rounded out to be able to support all service areas during the life of the EIS contract. [REDACTED]



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

[Redacted]

1.1.1 Service-Specific Requirements

Security is essential to the health and welfare of Federal Government agencies' network and internet structures. Our team is experienced and skilled in the assurance of data delivery and access as well as maintaining the security of that data both at rest and in transmission. Our team of carriers manages a huge section of the world's traffic on continual basis. We provide quality service under all conditions to include multilevel security and separate enclaves. Our current systems and operations have been adapted to meet the appropriate requirements for management of an MTIPS program. Our System Security Plan (SSP) is constructed in accordance with NIST Special Publication 800-18, Revision 1 and maps directly to the three tiered hierarchal system in

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

NIST 800-53. It also utilizes our team's deep knowledge and experience operating each individual network and associated peering procedures as major traffic carriers. Although modified for our specific services, our response levels of effort for the security assessment and authorization is based on the System's NIST FIPS Publication 199 categorization. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

1.1.1.1 Global Service

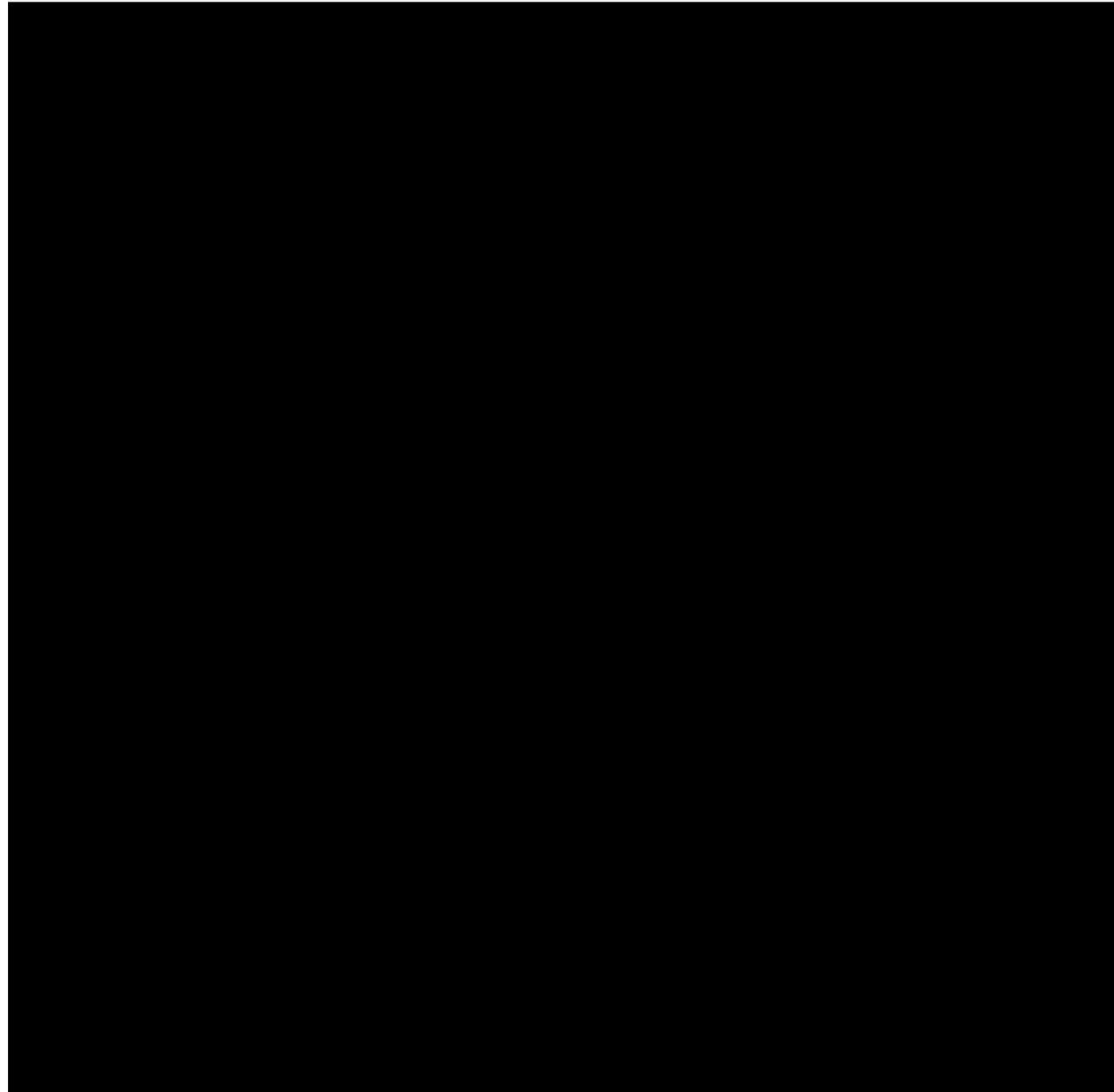
Team MicroTech provide EIS services on a global basis by leveraging the combined capabilities of our global, industry leading team. We selected our team members based on their service offerings and geographic cover to ensure robust support to EIS customers. In much of the global coverage area, we have multiple providers for a given service to facilitate speed of service delivery at a consistently competitive price. This redundancy allows us to address requests for diversity and redundancy with richer solutions that would likely be available from a single vendor.

1.1.2 General Requirements

1.1.2.1 Security Compliance Requirements

Team MicroTech understands the impact of FIPS 200 in reference to the information systems, such as BSS, that are used to support the EIS contract and services. We will ensure services delivered are in compliance with national policy directives that apply to the national telecommunications structure and automated information systems. Team MicroTech information and security staff are familiar with the NIST SP 800-53 requirements and standards and all government information will be maintained in approved systems. According to FIPS 199, the majority of the initial systems being deployed by Team MicroTech in support of EIS will be considered under the Moderate impact Level and the baseline security controls will be implemented in support of the environment. Team MicroTech is not providing Cloud services as part of our initial services. Our partners and government expertise provide knowledge around the

FedRamp requirements, and all future Cloud based services will be compliant based on the agency requirements.



1.1.2.1.1 Multi-Tenant Security

Separation of tenant applications and data at all levels is an important aspect of the security of our solution, especially critical in a multi-tenant environment. The ability to provide isolation and separation to preserve the integrity of a single tenant environment data access is important. Our Platform supports the following tenant separation:

- [Redacted]
- [Redacted]

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

■ [REDACTED]
[REDACTED]

■ [REDACTED]
[REDACTED]

1.1.2.2 Security Assessment and Authorization (Security A&A)

Our team maintains all systems supporting the EIS services and underlying BSS according to NIST standards and A&A security processes. As part of the support of GSA/EIS, we will conduct external security assessments in order to demonstrate our capabilities and security of our supporting systems. As defined in our security and risk management plans, we will maintain and document all IT security processes and guidance which will be followed by all MicroTech employees and subcontractors.

1.1.2.3 System Security Plan (SSP)

Our team maintains each system of record as ISO/IEC 27001 and 15408 compliant. All carriers MTIPS teams are updating current processes to ensure that current controls reflect NIST 800-53 controls as well as the intent of each control. Team MicroTech's plan provides for assuring that our partners current services (MSS, etc.) are adapted to meet the continuous monitoring activities as outlined in NIST SP 800-137. Our carrier team members' extensive and exhaustive security standard operation procedures are adopted to meet all compliance requirements required in section C 1.8.7.1 and C 1.8.7.6 of the RFP.

1.1.2.4 System Security Plan Deliverables

Specific controls for MTIPS require that all key or supervisory personnel assigned to support MTIPS are U.S. citizens, and eligible for Top Secret SCI clearances. All of our carriers have established compliance and security controls to comply with the outlined requirements for Sensitive But Unclassified (SBU) and Classified items. MicroTech has extensive experience operating within government agency-specific security requirements and will be a close partner with all our MTIPS carriers to assure compliance with all security requirements. The MTIPS Customer Project Manager and or SISO coordinates any periodic security reviews to verify compliance. When requested by the OCO, we will prepare and deliver an updated Service Security Plan to

meet specific agency requirements. Our employees receive training and briefings on proper techniques for accessing both classified and SBU data.

1.1.2.5 Additional Security Requirements

ID Number	Description
1	The deliverables are labeled "CONTROLLED UNCLASSIFIED INFORMATION" (CUI) or contractor selected designation per document sensitivity. External transmission/dissemination of CUI data to or from an agency computer must be encrypted. Certified encryption modules must be used in accordance with FIPS PUB 140-2, "Security requirements for Cryptographic Modules."
2	<p>The government has the right to perform manual or automated audits, scans, reviews, or other inspections of the contractor's IT environment being used to provide or facilitate services for the government. In accordance with the FAR (see Section I, 52.239-1) the contractor shall be responsible for the following privacy and security safeguards: The contractor shall not publish or disclose in any manner, without the CO's written consent, the details of any safeguards either designed or developed by the contractor under this TO or otherwise provided by the government. <i>Exception - Disclosure to a Consumer Agency for purposes of security assessment and authorization verification.</i></p> <p>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:</p> <ul style="list-style-type: none"> ▪ 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. <p>Automated scans can be performed by government personnel, or agents acting on behalf of the government, using government operated equipment, and government specified tools. If the contractor chooses to run its own automated scans or audits, results from these scans may, at the government's discretion, be accepted in lieu of government performed vulnerability scans. In these cases, scanning tools and their configuration shall be approved by the government. In addition, the results of contractor-conducted scans shall be provided, in full, to the government.</p>

Our team's efforts, in compliance with FAR Part 52.239-1, will use current routine security operations and the MTIPS SISO for each carrier to ensure that each carrier's plan is specifically compliant as well as provide monthly reports on internal scans, audits, and training conducted as a key component of our PMR to the CO. Actions will be conducted monthly as well as on an ad hoc basis. Government agencies will have the opportunity to conduct additional evaluations and testing as coordinated through the PMP. The SISO will provide updates on accessibility for government evaluations as a component of the PMR (monthly report)

All documentation regarding NDAs, specific documentation related to disclosure of information to third parties under NDAs, and all audits, and scans conducted will be maintained and managed by the projects/programs SISO. All materials will be managed

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

in accordance with NIST/FIPS recommendations as well as industry standards. All SISOs will be CISM-certified as well as cleared for classified information at the TS-SCI level using ISO/IEC 27001:2005 section 4.3.2 and TOGAF v9.1.

1.1.2.6 Personnel Background Investigation Requirements

As a longtime provider of IT and Telecom support services to the Government on a number of complex efforts, MicroTech possesses a thorough understanding of the critical nature of the security requirements called for in the GSA EIS solicitation. All Team MicroTech contractor employees who are granted access to the environment must first be able to prove they are citizens of the United States. The employee is fingerprinted and completes a background investigation.

Team MicroTech is responsible for administering, tracking, and maintaining the screening/rescreening process for all personnel working under this contract. We ensure all Team MicroTech personnel with access to Government information that is within the security A&A scope must successfully complete a background investigation in accordance with Homeland Security Presidential Directive-12 (HSPD-12) Office of Management and Budget (OMB) guidance M-05-24, M-11-11.

Procedures and Management of Clearances. The PM works with the FSO and our recruiting staff to identify the security requirements from the contract for each position. Using a detailed job description, the recruiting manager searches resume databases that contain cleared personnel to discover appropriate candidates. Resumes are then gathered and presented to the applicable managers for review.

Immediately following the interview, we review the employment application. Application assessment allows a reference check and JPAS review to be conducted verifying their active clearance is in good standing, and to authenticate their references, degrees, or certifications.

If an individual has an active clearance, the FSO checks the JPAS record to verify the type of clearance and date granted. If the age of the clearance is within the periodic reinvestigation (PR) interval set for that clearance, the FSO directs the employee to begin the PR process. If the individual requires a different clearance than the one already held (e.g., the person holds a Secret clearance and Top Secret is required), the FSO initiates the process to obtain the additional clearance.

If the individual does not have a current clearance, the FSO uses JPAS to initiate the clearance process. The candidate uses the Electronic Questionnaires for Investigations Processing (e-QIP) system to provide the necessary information to the government. Once the security questionnaire is completed and submitted, the FSO monitors JPAS for status updates, such as interim and final adjudication notices. Status changes are passed on to the PM immediately for action.

When information (SCI) access is required, the request is forwarded to the agency central adjudication facility (CAF). Defense Industrial Security Clearance Office (DISCO) may issue collateral clearance eligibility. Once the clearance is confirmed or approved by the government through JPAS, the employee receives security training in accordance with the contract requirements.

Employees are processed for a personnel security clearance (PCL) only when a determination has been made that “need to know” access is required for work on a classified contract. The level of access granted is equal to or less than the assigned level of clearance. Only the minimum necessary number of security clearances is granted. If emergency access to material is required at a higher level than that for which the employee is cleared, the employee contacts the FSO.

When a candidate accepts and employment begins, the on-boarding security process commences. Pertaining to security, the newly on-boarded employee must read, agree to, and sign various confidentiality agreements, including a Non-Disclosure Agreement (NDA), a security briefing, and the employee handbook. We require all staff with access to Government systems to complete annual security awareness training in addition to normally mandated company security training.

Background Security Forms Completion/Review. Applicants who successfully reach this phase are in the final stage of processing, during which they must complete background security forms. We seek to hire individuals who already possess the required security clearances. If not, each candidate is reminded he or she must be able to pass any required background security investigation to be employed in the intended position.

Team MicroTech directs applicants to respond to all questions to the best of their ability. Any questions requiring clarification because “yes” was entered must be provided in

detail. Once all security forms are completed, they are forwarded to our security officer for processing.

Reference/Education/Affiliation Check. We consider references to be one of the most important discriminators in selecting a qualified applicant. Our procedures require at least two excellent references be received from either supervisors or clients. We do not make employment offers to applicants who receive negative or equivocal references. The consistent enforcement of this policy is key to ensuring a high-quality, technically capable contract staff.

Our third-party background investigator verifies each applicant's employment history to confirm dates of employment, salary, duties, and reason for leaving. The investigator calls educational institutions to confirm degrees granted and certifications awarded. As a cross-check, the recruiter may also contact professional references and ask them a series of structured questions regarding the candidate's technical ability, dependability, willingness to shoulder responsibility, and interpersonal skills.

U.S. Citizenship. Some positions require U.S. citizenship. All recruiting and advertising efforts for a citizenship-restricted position clearly state the restriction. Prior to beginning work, prospective employees for a restricted position must present proof of U.S. citizenship. We follow the Government standard for proof of citizenship—such as, birth certificate or U.S. passport.

E-Verify. As a federal government contractor, we comply with contractual requirements and verify each employee's eligibility to work, comparing information from an employee's Form I-9, Employment Eligibility Verification, against DoD and Department of Homeland Security databases.

Background/Security Check. Candidates for applicable contracts are asked to complete some, all, or a combination of the following Security forms, as applicable:

- Questionnaire for Public Trust Positions (SF-85P)
- Fingerprint Chart (SF-87)
- Questionnaire for Sensitive Positions (or National Security) (SF-86)
- Financial Statement
- Customs Authorization for Release of Information (TFD 67-32.5)

Team MicroTech forwards these forms to the Government security officer for an initial review and regular processing. We then request an informal, non-attributable opinion of the security officer, based upon their initial review of submitted forms, whether the applicant's profile appears typical or atypical from a background/security check standpoint. We solicit a non-attributable opinion of submitted security forms to determine if the candidate for a position can obtain the required security clearance. We do not pursue a candidate that receives an atypical rating.

Team MicroTech provides customer technical support as a component of each EIS service.

1.1.3 Traffic Routing Requirements

MicroTech provides technical and programmatic support ensuring our customers have reliable services. When capabilities are unavailable due to disaster, crisis or other event we will execute our NS/EP plan which has several continuity of government functions and programs imbedded within our own restoration, reconstitution, and recovery operations.

Our team members all have extensive Disaster Recovery (DR) and COOP support for all systems and capabilities which leverage TSP, WPS, and GETS for our government customers. We aligned our network restoration plans with the five levels of priority as designated and assigned by TSP for our services provided to the government. Our systems integration team plans, designs and implements redundant, fail-over systems such that critical USG capabilities do not fail. Restoration efforts to maintain redundancy and our knowledge and understanding of the nations as well as global communications infrastructure enable us to provide continuity to customers' critical systems capabilities. Our technical program management experience ensures a coordinated effort, assuring critical capabilities such as MTIPS are maintained at the highest possible state throughout an event. As designated in our response to section G.11 we have a detailed understanding of the NCIRP, NS/EP programs and requirements to include providing response mechanisms of activities related to the National Coordinating Center, OEP and OSTP. Our team has decades of experience in the managing of NE/EP activities and FEMA ESF-2 efforts.

Our team of national and global telecommunications carriers were all selected based on their state of the art facilities which maintain the highest degree of reliability under ANSI standards. Physical security and site surveillance are all maintained on a 24x7 basis and exceed standards. MicroTech brought together this team of carriers to provide a packaged solution which will facilitate government agencies to meet the mandates of OMB M-05-22 and OMB M-09-32. Our team is comprised of experienced telecommunications providers that have built and delivered direct provisioning and cloud based solutions all over the world. All have experience with co-location of GFE/GFP as well as effective partitioning and accessibility of proprietary systems within a single data center. Our consortium provisions networks operation in the IPV4 and IPV6 spaces concurrently with a proven track record in the secure and efficient transitioning of backbone traffic to IPV6. All customer data, unless specifically requested, is encrypted at rest as well as in motion. Our team has unique combination of network locations, architectures, and peering capabilities that allow us to provide exceptional service for customer complex requirements such as MTIPS. Our team of providers builds specific networks which disambiguate traffic origins and route through multiple enclaves with minimal impact (or un-noticeable) to the end user.

Systems we propose for customers will leverage the best service, security, and value model.

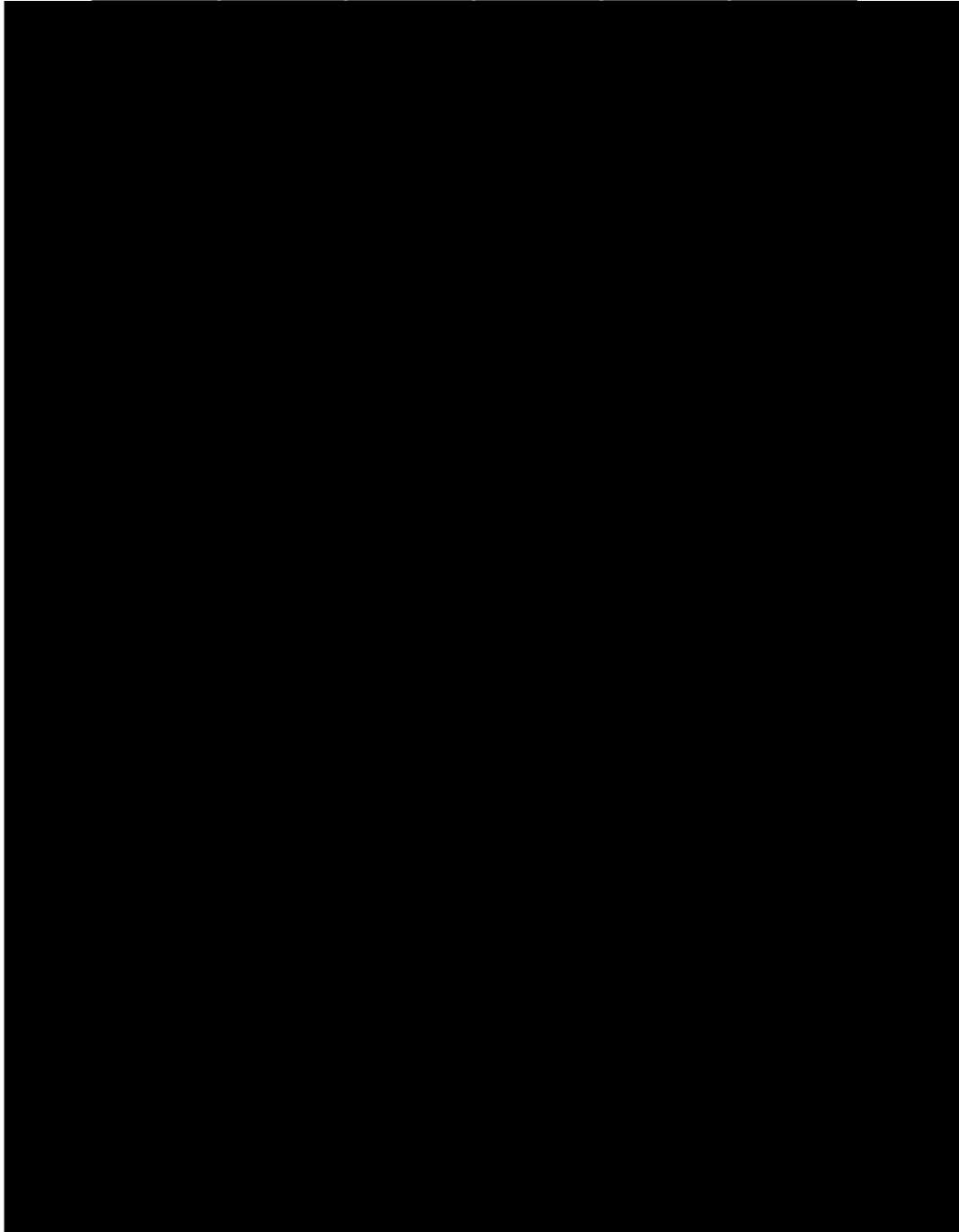
A SOC and/or NOC will manage the baseline for agency traffic normalization and traffic monitoring (signatures). Key locations include Atlanta, GA; Anaheim, CA; New York, NY; and Ashburn, VA. These sites are all highly experienced in co-location and provide COOP redundancy that exceeds the double standard for a tier 3 level facility in addition to being located in some of the nation's highest bandwidth connectivity centers. These sites will also be the physical locations for logical connections of customer and provider enterprises, managing of TICs and other infrastructure components of our major enclaves. Team MicroTech uses high performance computing platforms as well as scalable offerings to baseline traffic, disambiguate entities, and identify specific traffic for routing through the DHS enclaves.



[Redacted text block consisting of multiple horizontal black bars of varying lengths, representing redacted content.]

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

[REDACTED]



[Redacted text block consisting of seven horizontal black bars of varying lengths.]

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

[REDACTED]

Key to the effectiveness of this solution is our network team. [REDACTED]

[REDACTED]

[REDACTED]. Our telecommunications partners have a history in building diversity into

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

their networks. We anticipate the need for this diversity to extend into customers “last mile” with highly diverse connections into multiple TICs and SENs assigned.

[REDACTED]

[REDACTED] Design and management of mechanisms will have specific technical considerations that will address the agencies privacy management plan, policies regarding privacy and information management, as well as policies provided by DHS. All changes and agency requirements will be managed as part of technical change plan in the awarded contract and/or updated as part of the SLA.

MicroTech will be the principle in guiding the establishment of security compliant with ANSI/TIA-942 and ICD 705 for those carriers that do not have the appropriate level of classified facilities at award. All ISP/Carrier team members currently follow ANSI/TIA-942 standards as routine business practices. [REDACTED]

[REDACTED]

[Redacted content]

Our carriers are established and high quality service providers. Each carrier utilizes a network management monitoring model for assurance of customer connectivity and quality. Key for the MTIPS customers will be a measure of latency into, within and from the MTIPS DMZ to assure operations to/from DHS EINSTEIN enclaves and impacts caused within the EINSTEIN enclave are excluded from KPI reporting and meeting SLA requirements.

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

[REDACTED]

2 TECHNICAL RESPONSE

2.1 Mandatory EIS Services

Team MicroTech possesses the required capabilities to support the following EIS mandatory services: VPNS, IPVS, ETS, MNS, and Access Arrangement.

2.1.1 Data Service

2.1.1.1 Virtual Private Network (VPN) Service

A. Understanding

██████████ we provide VPN Services across high-speed unified multi-service IP-enabled backbone infrastructure. We configure the network to optimize an agency's applications allowing for traffic prioritization and cost effectiveness to support various VPNS traffic types. We comply with the standards as defined in the RFP.

B. Quality of Services

Our base-level, comprehensive Quality of Services is applied in our solution across all areas of the PWS: Service and Functional Description, Standards, Connectivity, Technical Capabilities, Features, Interfaces, and Performance Metrics.

- **Quality of Service (QoS):** Team MicroTech VPNS Standard QoS acts like Metro Ethernet services where all traffic uses one class of service. Premium QoS maps traffic to four classes of service.
- **Multiple Class of Service (CoS) Options:** Depending on the network configuration, Team MicroTech VPNS can support up to four classes of service, including Real Time, Interactive Data, Priority Data, and Best Effort all with multiple profile allocation options.

C. Service Coverage

We propose to serve the top 25 markets:

Rank	CBSA Name	CBSA Code
1	Washington-Arlington-Alexandria, DC-VA-MD-WV	47900
2	Baltimore-Columbia-Towson, MD	12580
3	Durham-Chapel Hill, NC	20500
4	Dallas-Fort Worth-Arlington, TX	19100
5	Chicago-Naperville-Elgin, IL-IN-WI	16980
6	San Jose-Sunnyvale-Santa Clara, CA	41940
7	Salt Lake City, UT	41620

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

Rank	CBSA Name	CBSA Code
8	Kansas City, MO-KS	28140
9	Atlanta-Sandy Springs-Roswell, GA	12060
10	Virginia Beach-Norfolk-Newport News, VA-NC	47260
11	St. Louis, MO-IL	41180
12	Nashville-Davidson--Murfreesboro--Franklin, TN	34980
13	Chattanooga, TN-GA	16860
14	Denver-Aurora-Lakewood, CO	19740
15	San Diego-Carlsbad, CA	41740
16	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD	37980
17	New York-Newark-Jersey City, NY-NJ-PA	35620
18	Houston-The Woodlands-Sugar Land, TX	26420
19	Richmond, VA	40060
20	Memphis, TN-MS-AR	32820
21	Huntsville, AL	26620
22	Orlando-Kissimmee-Sanford, FL	36740
23	Gulfport-Biloxi-Pascagoula, MS	25060
24	Hagerstown-Martinsburg, MD-WV	25180
25	San Antonio-New Braunfels, TX	41700

D. Security

A highest level of security is required for VPNS for compliance purposes. For On-Off government work, conducted across the country and the world, our solution requires world-class security measures. VPNS is a security measure which provides the reliable transport of agency documents and applications across our infrastructure. As we demonstrate below, we comply with the standards as defined in the RFP. We support these standards alongside our partners and employ these measures for government agencies as we have done so across our many years in business.

[Redacted content]

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

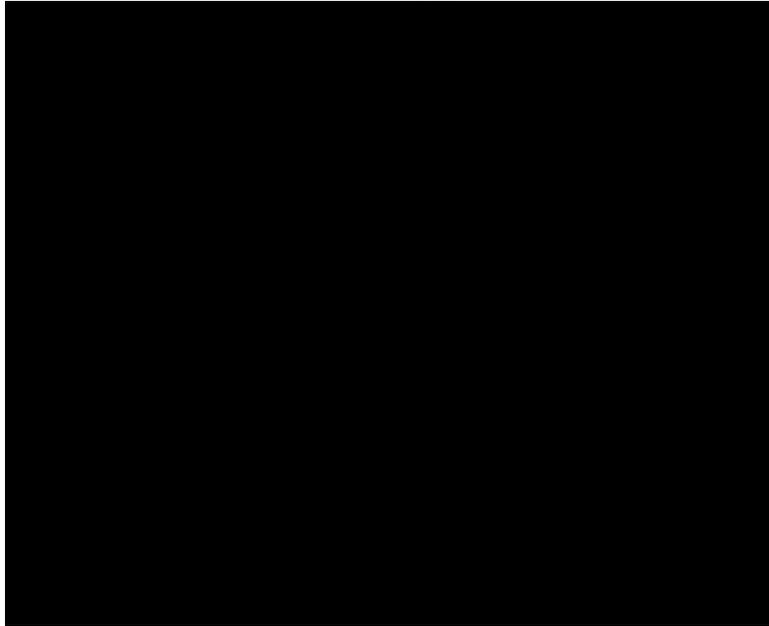
2.1.1.1.1 Service Description

Team MicroTech's Virtual Private Network Service (VPNS) provides secure and reliable transport of agency applications across our transport providers' high-speed, unified, multi-service IP-enabled backbone infrastructure. Like other Team MicroTech networking services we currently offer such as Private Line and Ethernet services, the fundamental goal of this service is to create a private network that connects multiple buildings in multiple locations. Our VPNS supports fully meshed, hub and spoke, and partial mesh configurations as standard network topologies. The service:

- Supports common routing protocols based on customer requirements
- Is built to allow for complementary services including managed services, CPE, and security
- Supports multicast traffic to enable next-generation applications such as IPTV, distance learning, and multipoint videoconferencing

- [REDACTED]
- [REDACTED]
 - [REDACTED]
 - [REDACTED]

Typical VPNS configuration:



2.1.1.1.2 Functional Definition

Team MicroTech's Virtual Private Network Service (VPNS) provides secure and reliable transport of agency applications across MicroTech partner 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 owned or controlled by MicroTech partners and located at the edge of their backbone. Tunnels terminate at the Team's edge router.

The backbone consists of carrier grade dual redundant switches, routers, and firewalls connected to multiple transmission media including fiber optics, microwave radio and copper/TDM facilities. Numerous transport providers have multi-fiber facilities terminating at MicroTech partner data centers. Further, MicroTech partners have fully redundant power sources, dual redundant air conditioning capability, 24/7 high tech security capabilities including integrated video surveillance, biometrics, interior and exterior Infra-red cameras, physical security access into facilities and data centers using multi-factor authentication methods security and a multitude of other capabilities and services required and expected for carrier grade facilities such as theirs that provide mission critical services.

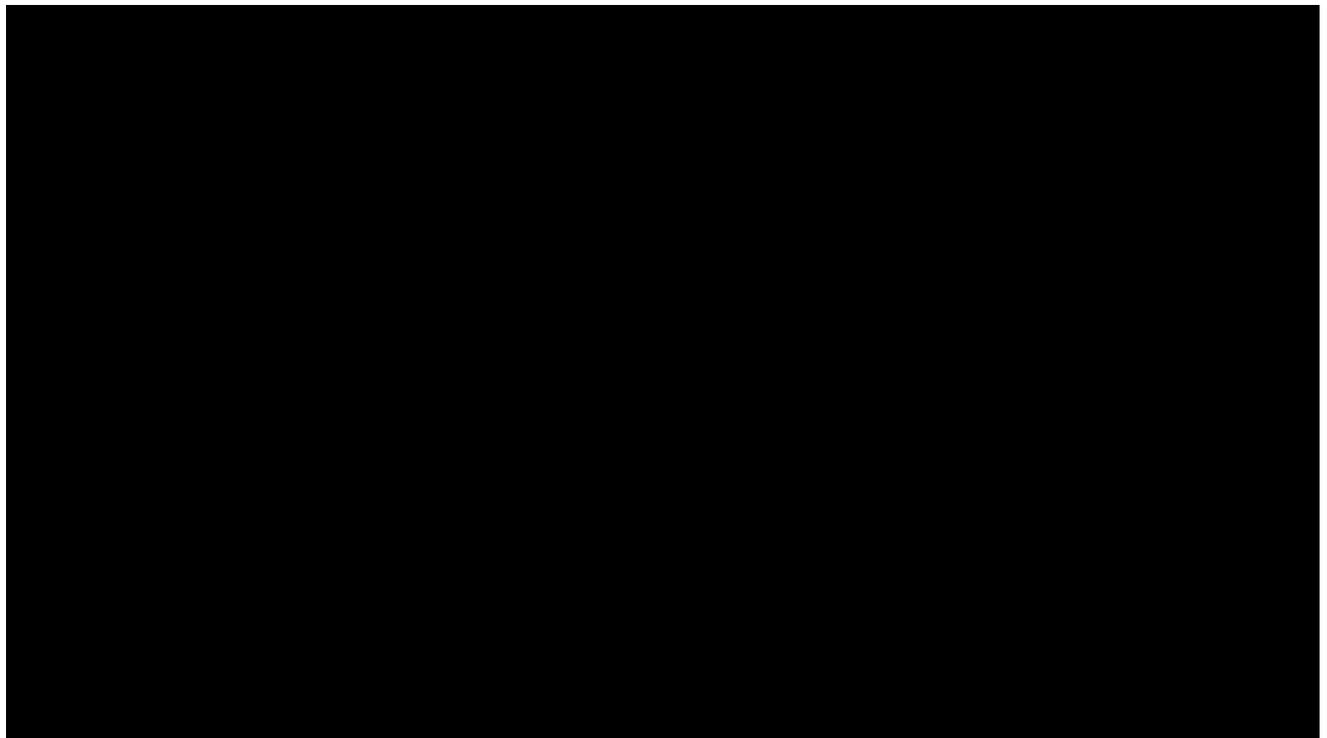
In the provided backbone Team MicroTech provides three basic solutions for VPNS:

- 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.

Team MicroTech configures the network to optimize an agency's applications allowing for traffic prioritization and cost effectiveness to support the following VPNS traffic types:

- Time-critical traffic such as voice and video.
- Business-critical traffic such as transactions.
- Non-critical traffic such as email.

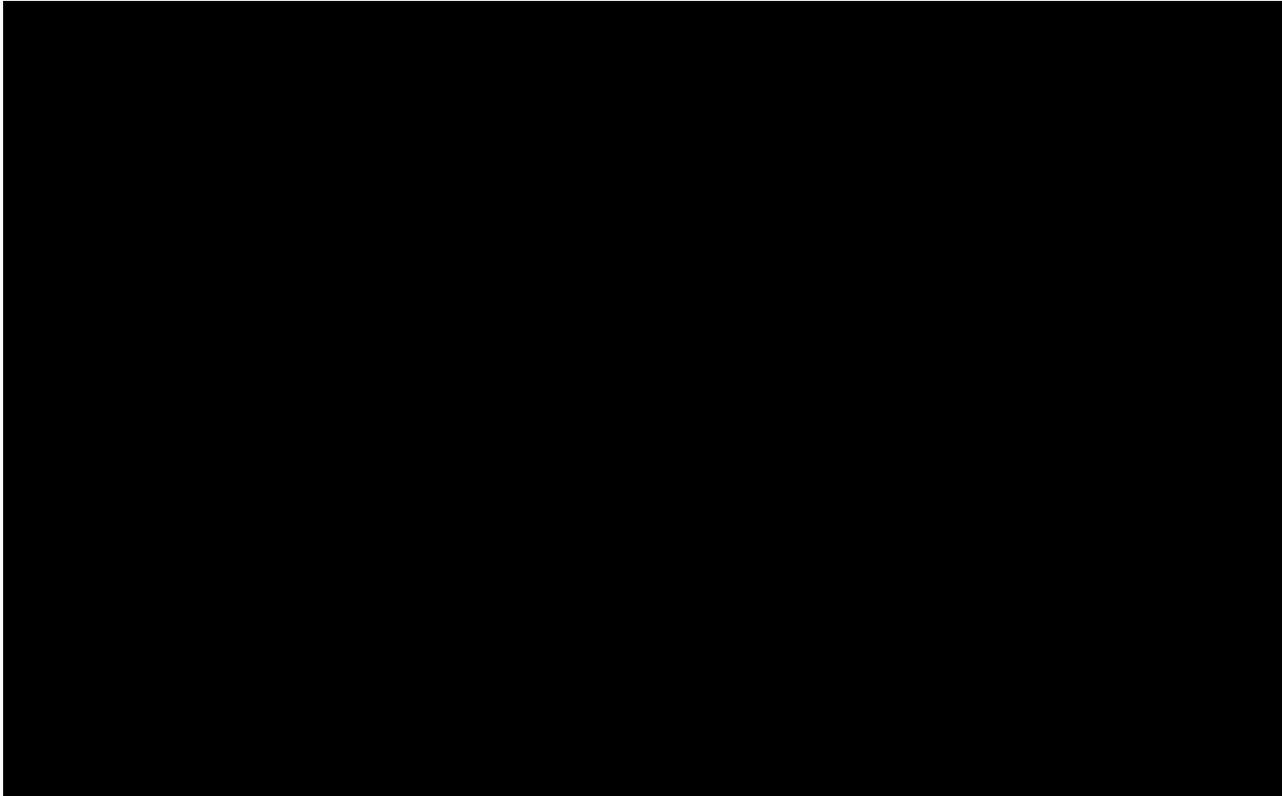
Architecture: Site-to-Site VPNs (IntraNet)



In this example, the organization can have transparent communication between two networks located behind different firewalls at different offices using route-based IPsec VPN. This allows for secure, encrypted, private communication from site to site. [REDACTED]

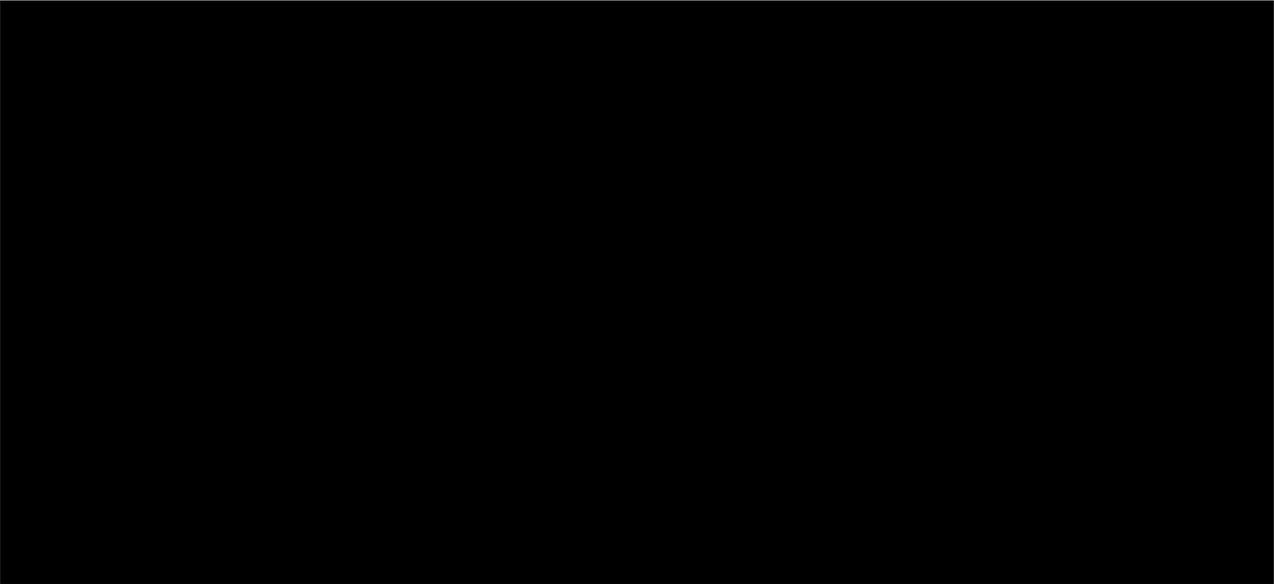
[REDACTED]

[REDACTED]



[Redacted text block consisting of approximately 18 horizontal black bars of varying lengths, representing obscured content.]

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



Team MicroTech offers a number of Routing Protocols depending on the customer's needs, including:

- BGP Routing: Standard Supported Routing—default routing protocol.
- Static Routing: Standard Supported Routing—should only be used with simple networks, as customers need to provide Team MicroTech initially with their network subnets and update them each time the customer adds a subnet to their network.
- OSPF Routing: Non-Standard Routing requiring Network Operations approval; considered only for customers with large, complex networks already using OSPF.

2.1.1.1.3 Standards

Team MicroTech complies with all of the following standards.

- OMB M-11-11 “Continued Implementation of Homeland Security Presidential Directive (HSPD-12) Policy for a Common Identification Standard for Federal Employees and Contractors”
- NIST Special Publication (SP) 800-46 Revision 1 “Guide to Enterprise Telework and Remote Access Security”

- IETF RFCs:
 - For secure VPNs:
 - General IPsec
 - ESP and AH
 - Key exchange
 - Cryptographic algorithms to include but not limited to 3DES, RC4 and AES
 - IPsec policy handling
 - IPsec MIBs
 - Remote access
 - Certification Authorities
 - For trusted VPNs:
 - General MPLS
- IP Security Working Group – RFC 4303
- IP Security Policy Working Group – RFC 3586
- MPLS Working Group – RFC 3468
- Layer 3 Virtual Private Network (L3VPN) Working Group – RFC 4176
- Pseudo Wire Emulation Edge to Edge (pwe3) Working Group – RFC 3985
- Use of PE-PE GRE or RFC 4364 VPNs:
 - draft-ietf-l3vpn-gre-ip-2547-00.txt
 - IETF-TLS Working Group – RFC 5246 for TLS 1.2
 - TLS 1.2 Protocol Specification
 - IETF RFCs for IPv4 and IPv6
 - CNSSP-15, National Information Assurance Policy on the Use of Public Standards for Secure Sharing of Information Among National Security Systems
 - All new versions, amendments, and modifications to the above documents and standards

2.1.1.1.4 Connectivity

Team MicroTech's network connects 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. We will comply with all listed connectivity instances. Team MicroTech's VPNS supports today's most widely

deployed access technologies across a variety of network mediums providing near-ubiquitous access. Ethernet and private line access are supported through Fiber and other cable distribution. Access via TDM and other mediums is supported and based on access third-party providers have to customer locations.

2.1.1.1.5 Technical Capabilities

Team MicroTech's VPNS complies with all mandatory requirements listed below:

- Applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow for inspection.
- Multiple tunneling standards. Examples include L2TP, GRE, IP-in-IP, MPLS, IPSec, and TLS.
- Various encryption levels. Examples include 3DES, RC4 and AES in accordance with the appropriate FIPS publications and modules.
- Authentication services. Examples include RADIUS, Internal LDAP, token integration, PKI, and X.509 certificates.
- Support IPv4 as both the encapsulating and encapsulated protocol.
- Support 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

- Support one or more of the following application level QoS objectives:
 - Intserv model for selected individual flows.
 - Diffserv model for aggregated flows.
- Team MicroTech provides isolation of traffic and a routing service that isolates the exchange of traffic and routing information to only those sites that are authenticated and authorized members of a VPN. We provide layered security architecture to ensure attackers do not find a single point of entry but instead are faced with multiple layers of security.
- Team MicroTech supports multiple VPNs by allowing both permanent and temporary access to one or more VPNs for authenticated users across a broad range of access technologies.
- Team MicroTech provides secure routing services to ensure full routing capability on the VPN platform with a secure policy across the VPN.
- Team MicroTech supports the inclusion of encryption, decryption, and key management profiles as part of the security management system.
- Team MicroTech deploys its own internal security mechanisms, in order to secure specific applications or traffic at a higher level than a site-to-site basis.
- Team MicroTech allows GSA’s customers to choose from alternatives for authentication of temporary access users. Authentication server choices include:
 - Contractor-provided
 - Third party
 - Agency-provided
- Service Level Agreement: Applies to core network performance (PE-to-PE); specified for packet delivery, latency, jitter, service availability, and time to repair. Latency performance and SLAs vary per class of service and distance.

2.1.1.1.6 Features

Team MicroTech will comply with the required VPNS features delineated in Section C.2.1.1.2 of the Solicitation, to include:

ID Number	Name of Feature	Description
1	High availability options	Availability options:

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

		<ul style="list-style-type: none"> ▪ Load sharing ▪ Fail-over protection ▪ Diverse access points to service provider's POP(s).
2 (optional)	Interworking Services	Compatible services for an agency's VPN to transparently access agency locations that use the Team MicroTech's Ethernet Transport Service.

2.1.1.1.7 Interfaces

The following UNIs at the SDP for VPNS are available from Team MicroTech.

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)
1	Ethernet Interface	1 Mbps up to 10/40/100 Gbps (Std IEEE802.3ae and 802.3ab)	IPv4/v6 over Ethernet
2	Private Line Service	<ul style="list-style-type: none"> ▪ DS0 ▪ T1 ▪ T3 ▪ OC-3c ▪ OC-12c ▪ OC-48c ▪ OC-192c ▪ OC-768c (optional) 	IPv4/v6 over PLS
3	IP over SONET Service	<ul style="list-style-type: none"> ▪ OC-3c ▪ OC-12c ▪ OC-48c ▪ OC-192c ▪ OC-768c (optional) 	IP/PPP over SONET
4	DSL Service	xDSL access at 1.5 to 6 Mbps uplink, and 384 Kbps to 50 Mbps downlink	Point-to-Point Protocol, IPv4/v6
5 (optional)	Cable high speed access (DOCSIS only QOS)	320 Kbps up to 150 Mbps	Point-to-Point Protocol, IPv4/v6
6	Wireless Access	<ul style="list-style-type: none"> ▪ Wi-Fi ▪ LTE ▪ Satellite 	Point-to-Point Protocol, IPv4/v6

2.1.1.1.8 Performance Metrics

Team MicroTech complies with the performance levels and acceptable quality level (AQL) of KPIs for VPNS.

KPI	Service Level	Performance Standard (Threshold)	AQL	Meet/Exceed
Latency (CONUS)	Routine	70 ms	≤ 70 ms	Meets
Latency (OCONUS)	Routine	150 ms	≤ 150 ms	Meets
Av(VPN)	Routine	99.9%	≥ 99.9%	Meets
	Critical	99.99%	≥ 99.99%	Meets
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	Meets
	With Dispatch	8 hours	≤ 8 hours	Meets

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

2.1.1.2 Ethernet Transport Service

A. Understanding

Team MicroTech's Ethernet Transport Service product is designed to provide standardized Ethernet-based services for Enterprise customers across the United States. Ethernet Transport Services are offered via a network infrastructure that seamlessly connects customers on our Metro Wide Area, and National networks, and utilizes Type II (3rd party) circuits for off-net connectivity. Our Ethernet Transport Services addresses the market and technology trend of companies moving to simple, yet highly flexible and robust, network transport options.

[REDACTED]

Ethernet Services utilizes standardized product offerings and includes an Ethernet Services portal which provides an overview of circuit inventory information, as well as easy access to performance management data. Customers are able to see performance data in near real-time, by circuit (for Ethernet Line services) or by location (for Ethernet Private LAN). Additionally, the portal provides on-demand reports.

B. Quality of Services

Team MicroTech manages Ethernet Quality of Service (QoS), also known as Class of Service, (CoS), using the two industry standard approaches of Integrated Services (IntServ) and Differentiated Services (DiffServ). [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Our

service offerings include multiple approaches and levels of QoS. Team MicroTech is experienced at implementing and managing QoS across multiple vendors and providers' boundaries while ensuring the desired level of service.

C. Service Coverage

Team MicroTech propose to serve the top 25 markets, as follows:

Rank	CBSA Name	CBSA Code
1	Washington-Arlington-Alexandria, DC-VA-MD-WV	47900
2	Baltimore-Columbia-Towson, MD	12580
3	Durham-Chapel Hill, NC	20500
4	Dallas-Fort Worth-Arlington, TX	19100
5	Chicago-Naperville-Elgin, IL-IN-WI	16980
6	San Jose-Sunnyvale-Santa Clara, CA	41940
7	Salt Lake City, UT	41620
8	Kansas City, MO-KS	28140
9	Atlanta-Sandy Springs-Roswell, GA	12060
10	Virginia Beach-Norfolk-Newport News, VA-NC	47260
11	St. Louis, MO-IL	41180
12	Nashville-Davidson--Murfreesboro--Franklin, TN	34980
13	Chattanooga, TN-GA	16860
14	Denver-Aurora-Lakewood, CO	19740
15	San Diego-Carlsbad, CA	41740
16	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD	37980
17	New York-Newark-Jersey City, NY-NJ-PA	35620
18	Houston-The Woodlands-Sugar Land, TX	26420
19	Richmond, VA	40060
20	Memphis, TN-MS-AR	32820
21	Huntsville, AL	26620
22	Orlando-Kissimmee-Sanford, FL	36740
23	Gulfport-Biloxi-Pascagoula, MS	25060
24	Hagerstown-Martinsburg, MD-WV	25180
25	San Antonio-New Braunfels, TX	41700

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

D. Security

Team MicroTech's Ethernet service offering includes a number of Ethernet security features. While a number of these features are carrier-side based features that show how we assure security within our environment, some are available to the customer to configure as part of their service. The following is a list of Ethernet security features:

- Authentication, authorization, and accounting (AAA) with TACACS+ and RADIUS
- Layer 2-4 ACLs (Available to the customer)
- Broadcast/unicast/multicast storm control (Configurable in coordination with the customer)
- Control Plane Policing
- DHCP option 82 insertion
- Static Access port
- MAC security on EVC (Configurable in coordination with the customer)
- Dynamic ARP inspection
- BPDU Guard, BPDU Filtering, Loopguard
- Port Security
- MAC address changes notification

2.1.1.2.1 Service and Functional Description

Ethernet is the most widely installed local area network (LAN) technology. Ethernet is a link layer protocol in the TCP/IP stack, describing how networked devices can format data for transmission to other network devices on the same network segment, and how to put that data out on the network connection. It touches both Layer 1 (the physical layer) and Layer 2 (the data link layer) on the OSI network protocol model. Ethernet defines two units of transmission, packet, and frame. The frame includes not just the "payload" of data being transmitted but also addressing information identifying the physical "Media Access Control" (MAC), addresses of both sender and receiver, VLAN tagging and quality of service information, and error-correction information to detect problems in transmission. Each frame is wrapped in a packet, which affixes several bytes of information used in establishing the connection and marking where the frame starts.

[REDACTED]

Ethernet Transport Service (ETS) allows agencies to connect their LANs (10 Mbps, 100 Mbps, 1 Gbps, and 10/40/100 Gbps) transparently over the Metro Area Networks (MAN) and the Wide Area Networks (WAN) regardless of the geographical location of their sites. Ethernet Transport Service enables Intranet and Extranet services, as well as intra- and inter-agency communications.

Ethernet is provided as a dedicated service or a shared service. Dedicated Ethernet is defined as private services that are carried over dedicated facilities at fixed and predetermined speeds. Shared Ethernet is defined as statistically multiplexed Ethernet connections. Team MicroTech's network allows agencies to connect LANs transparently over the Wide Area Networks (WAN) regardless of the geographical location of their sites. We provide a dedicated Ethernet service or a shared Ethernet service.

Team MicroTech's network gives agencies the ability to connect LANs transparently over Wide Area Networks, providing point-to-point, point-to-multipoint and multipoint-to-multipoint connections. Our network takes advantage of Ethernet's flexibility, cost effectiveness, and differentiation of service (e.g., traffic priority) capabilities while providing end-to-end transport of data traffic with minimal protocol conversion. [REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

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

[Redacted text block]

2.1.1.2.1.1 Ethernet Private Line

[Redacted text block]

2.1.1.2.1.2 Ethernet Private LAN (E-LAN)

[REDACTED]

2.1.1.2.2 Standards

Team MicroTech supports the following ETS standards, [REDACTED]

[REDACTED]

- Metro Ethernet Forum (MEF CE 2.0):
 - Support Jumbo Ethernet frames
 - CE 2.0 is set of MEF CE 2.0 Certified network elements that connect to transport Carrier Ethernet services for all users, locally and worldwide. Ethernet transport services are carried over physical Ethernet networks and other legacy transport technologies.
 - Key Specifications:

- MEF 6.1 - CE Service Definitions
- MEF 10.2 - CE Service Attributes
- MEF 33 - Ethernet Access Services
- MEF 23.1 - Class of Service
- MEF 26.1 - ENNI
- CE 2.0 expands CE 1.0 to:
 - 8 services, 2 of each respectively in E-Line, E-LAN, E-Tree, and E-Access (defined in MEF Standards MEF 6.1, 22.1, 33)
 - Standardized Multi-CoS with application-oriented CoS Performance Objectives, new metrics (MEF 6.1, 10.2, 20, 23.1)
 - Interconnect through the integrated delivery of MEF Service Attributes (MEF 10.2, 26.1, 33) which allows for ubiquitous deployment spanning multiple providers
 - Manageability, (MEF 7.1, 16, 17, 30, 31) plus additional specifications
- International Telecommunications Union (ITU):
 - Network architecture:
 - G.8010/Y.1306 Architecture of Ethernet layer networks
 - Services:
 - G.8011/Y.1307 Ethernet over Transport – Ethernet services framework
 - G.8011.1/Y.1307.1 Ethernet private line service
 - G.8011.2/Y.1307.2 Ethernet virtual private line service
 - G.8011.3/Y.1307.3 Ethernet virtual private LAN service (draft)
 - G.8011.4/Y.1307.4 Ethernet virtual private rooted multipoint service (draft)
 - G.8012/Y.1308 Ethernet UNI and Ethernet NNI
 - OAM:
 - Y.1730 Requirements for OAM functions in Ethernet-based networks and Ethernet services
 - Y.1731 OAM functions and mechanisms for Ethernet-based networks
 - Protection:
 - G.8031/Y.1342 Ethernet linear protection switching
 - G.8032/Y.1344 Ethernet ring protection switching

- Equipment:
 - G.8021/Y.1341 Characteristics of Ethernet transport network equipment functional blocks
- Equipment management:
 - G.8051/Y.1345 Management aspects of the Ethernet-over-Transport (EoT) capable network element
- Terminology:
 - G.8001/Y.1354 Terms and definitions for Ethernet frames over Transport (EoT)
- Institute of Electrical and Electronics Engineers, Inc. (IEEE):
 - IEEE 802.3, 1Gbps LAN PHY, 10Gbps LAN PHY, 10Gbps WAN PHY
 - IEEE 802.3ae, 10Gbit Ethernet 802.17, Resilient Packet Rings (RPR) – in progress
 - IEEE 802.1ah, Ethernet First Mile
 - IEEE 802.1p
 - IEEE 802.1q
- Acceptance Testing of ETS:
 - RFC 2544
 - RFC 6815
- All new versions, amendments, and modifications to the above documents and standards

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.1.1.2.3 Connectivity

Team MicroTech connects and operates with intra-agency LAN-providing connectivity for LANs located in the same city or different cities and sharing resources to connect to the metro or long haul network:

- Team MicroTech supports delivery of the ETS at the agency's Service Delivery Point (SDP) via a UNI.
- If required, Team MicroTech supports circuit emulation services for TDM services.
- Team MicroTech supports point-to-point, multipoint-to-multipoint, and Rooted multipoint EVCs.
- Team MicroTech supports EVC multiplexing.
- Team MicroTech supports rate-limited throughput access links, i.e., 1 Gbps port rate limited in 100 Mbps increments.
- Team MicroTech supports rate-limiting at the agency's SDP and at the individual VLAN ingress and egress.
- Privacy and security is supported per IEEE 802.3 as defined in the TO.
- Team MicroTech supports the following service attributes:
 - Physical interfaces as listed in Section C.2.1.2.3
- The following traffic profiles is supported:
 - Committed Information Rate (CIR) – minimum amount of bandwidth guaranteed for an ETS
 - Committed Burst Size (CBS) – the size up to which subscriber traffic is allowed to burst and still be in-profile and not discarded or shaped
 - Peak Information Rate (PIR) – specifies the rate above the CIR that traffic is allowed into the network for a given burst interval defined by the MBS
 - Maximum Burst Size (MBS)
- Performance parameters are supported as listed in Section C.2.1.2.4.
- Service Frame Delivery options supported include:
 - Unicast Frame Delivery
 - Multicast Frame Delivery, as per RFC 4604
 - Broadcast Frame Delivery as per IEEE 802.3
- VLAN tag supported include:
 - VLAN tag preservation
 - VLAN tag translation
 - VLAN tag stacking
 - VLAN aggregation across a common physical connection (optional)

- Service multiplexing is supported to include multiple EVCs connected via a single UNI.
- Bundling is supported to enable two or more VLAN IDs to be mapped into a single EVC at a UNI.
- Security Filters are supported as specified in the TO.
- Team MicroTech provides proactive Performance Monitoring (PM) supporting the following:

Team MicroTech's surveillance system has ping sensors that measure Layer 3 IP connectivity. It measures packet loss, delay, and jitter and connection state and gathers all types of related SNMP statistics for networked devices.

- Signal failure = sensors alarm when failure is detected.
- Signal degradation = Ping sensors show delay and jitter on degraded connectivity.
- Connectivity or Loss of connectivity = sensors alarm when connectivity is lost.
- Frame loss = Ping sensors indicate packet loss if there is frame loss.
- Errored Erred frames = Ping sensors demonstrate packet loss, abnormally high delay if there are errors in frames.
- Looping = Ping sensors are a form of loop testing. A ping probe is sent and expected to be received once received statistics are analyzed and graphed.
- Denial of service (DoS) = Intrusion Prevention System and Intrusion Detection System
- Misinserted frames = Measured with the RMON MIB as implemented in our surveillance system.
- Maintenance parameters = Our collected surveillance system historical data can be analyzed and a decision can be made as to what action is required.
- Team MicroTech supports the following maintenance functions:
 - Alarm suppression
 - Loopbacks (intrusive and non-intrusive (transparent to on-going connections))
 - Protection switching, restoration, etc.
- Team MicroTech supports the following network topologies:
 - Point-to-point
 - Rooted Multipoint

- Multipoint-to-multipoint (i.e., mesh)
- Team MicroTech supports geographical diversity to provide added reliability. An agency may buy a geographical diverse route from the same or a different contractor to serve as a protection path.
- Team MicroTech supports bridging in compliance with IEEE 802.1Q (2014).
- Team MicroTech supports the following Virtual Connection sizes:
 - For point-to-point Ethernet connections – up to 40 Gbps
 - For multi-point-to-multi-point connections – up to 40 Gbps
- Quality of Service (QoS) – Team MicroTech supports traffic prioritization that enables higher priority traffic to be transmitted first.
- Team MicroTech supports traffic reconfiguration that supports the ability of the agency to modify a specific service connection subsequent to the establishment of the connection. Changes to an established connection may include upgrade/downgrade of speeds that do not result in physical equipment changes.

2.1.1.2.5 Features

ID Number	Name of Feature	Description
1	Bandwidth-on-Demand (BoD)	Team MicroTech supports bandwidth increments and decrements on demand, as agreed between us and the agency. We indicate what increments are available to modify the contracted bandwidth in near real time. Options for incremental/reduction steps include at least 1, 5, 10, 40, and 100 or higher Mbps. Provisioning time for this feature does not exceed 24 hours per instance unless otherwise agreed by the agency and MicroTech case-by-case.

2.1.1.2.6 Interfaces

Team MicroTech complies with all mandatory and some optional UNIs at the SDP.

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling Protocol Type/Granularity	Response
1	Optical	IEEE 802.3z	1310 nm	1 Gbps	Gigabit Ethernet	████████
2	Optical	IEEE 802.3z	850 nm	1 Gbps	Gigabit Ethernet	████████
3	Optical	IEEE 802.3	1310 nm	100 Mbps	Fast Ethernet	████████
4	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm	10/40/100 Gbps	10/40/100GBASE-SR (65 meters)	████████████████████ ████████████████████ ████████
5	Optical	IEEE 802.3ae IEEE 802.3ba	850nm	10/40/100 Gbps	10/40/100GBASE-SW	████████████████████ ████████████████████ ████████

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

UNI Type	Interface Type	Standard	Frequency of Operation or Fiber Type	Payload Data Rate or Bandwidth	Signaling Protocol Type/Granularity	Response
6	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm	10/40/100 Gbps	10/40/100GBASE-ER	[REDACTED]
7	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm	10/40/100 Gbps	10/40/100GBASE-LR	[REDACTED]
8	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm	10/40/100 Gbps	10/40/100GBASE-LW	[REDACTED]
9	Optical	IEEE 802.3ae IEEE 802.3ba	1300 nm Multimode	10/40/100 Gbps	CWDM 10/40/100GBASE-LX4 (300 meters)	[REDACTED]
10	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm Single Mode	10/40/100 Gbps	CWDM 10/40/100GBASE-LX4 (10,000 meters)	[REDACTED]
11	Optical	IEEE 802.3ae IEEE 802.3ba	1310 nm Single Mode	10/40/100 Gbps	10/40/100GBASE-LW (10,000 meters)	[REDACTED]
12	Optical	IEEE 802.3ae IEEE 802.3ba	1550 nm Single Mode	10/40/100 Gbps	10/40/100GBASE-EW (40,000 meters)	[REDACTED]
13	Electrical	IEEE 802.3	N/A	10 Mbps	10Base	[REDACTED]
14	Electrical	IEEE 802.3	N/A	100 Mbps	100 Base	[REDACTED]
15	Optical	IEEE 802.3		1 Gbps	1000Base	[REDACTED]
16	Optical	ITU-T G.707	1300 nm	STM-4	SDH STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4	[REDACTED]
17	Optical	ITU- G.707	1300 nm	STM-4c	VC-4-4c	[REDACTED]
18	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-LX	[REDACTED]
19	Optical	IEEE 802.3z IEEE 802.3ab	Multimode	1 Gbps	1000BASE-SX	[REDACTED]
20	Electrical (Copper)	IEEE 802.3z	N/A	1 Gbps	1000BASE-CX	[REDACTED]
21	Electrical (Twisted pair)	IEEE 802.3z	N/A	1 Gbps	1000BASE-T	[REDACTED]
22	Optical	GR-253, ITU-T G.707	1310 nm	10/40 Gbps	SONET or SDH	[REDACTED]

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

2.1.1.2.7 Performance Metrics

Team MicroTech will comply with the following performance levels and AQL of KPIs for ETS as defined in Section C.2.1.2.4 of the Solicitation. We understand and acknowledge that the requirements are mandatory unless marked optional.

KPI	Service Level	Performance Standard (Threshold)	AQL	Meet/ Exceed
Av (ETS)	Routine(Single Connection)	99.9%	≥ 99.9%	Meets
	Critical (Double Connection)	99.99%	≥ 99.99%	Exceeds
Latency (ETS)	CONUS	100 ms	≤ 100 ms	Meets
	OCONUS	200 ms	≤ 200 ms	Meets
Jitter (Packet)	Routine	10 ms	≤ 10 ms	Meets
Grade of Service (Packet Delivery)	Routine	99.95%	≥ 99.95% at all times	Meets
	Critical	99.99%	≥ 99.99% at all times	Meets
Time To Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	Meets
	With Dispatch	8 hours	≤ 8 hours	Meets
Grade of Service	Routine	1 minute	1 minute	Meets
	Critical	100 ms	≤ 100 ms	Meets

2.1.2 Voice Service

Team MicroTech's solution complies with and exceeds the technical requirements for both options of Voice Service (VS).

- [REDACTED]
- [REDACTED]
- [REDACTED]

Team MicroTech focuses primarily on the IPVS provided by our teaming partners by means of implementations using SIP Trunking, IP Trunking via a gateway, hosted PBX, and Hosted ACD. Team MicroTech will provide IPVS service over an end-to-end managed network that will meet or exceed the KPIs required by the RFP Solicitation.

2.1.2.1 Internet Protocol Voice Service

A. Understanding

Team MicroTech's advanced communications portfolio of cloud-based solutions offers businesses the latest hosted voice, managed firewall, web collaboration, IP-VPN, IP Telephony, Video, High Speed Data, Internet services and other critical managed cloud based technologies for mid to large enterprise businesses all over its fully managed and redundant private MPLS network. Several Team MicroTech partners' comprehensive suite of cloud-based communications and collaboration solutions include both Unified Communications as a Service (UCaaS) and ancillary services, covering customer needs ranging from high definition enterprise- grade phone service with built-in mobile apps, web and video conferencing, to hosted contact center software and virtual desktop infrastructure solutions.

B. Quality of Services

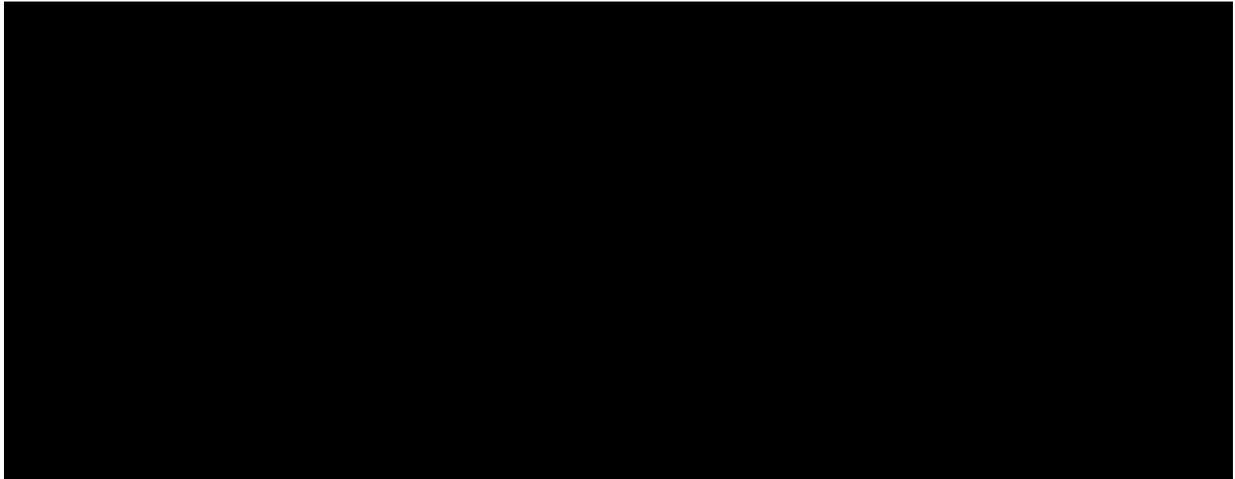
IPVS and SaaS Optimized

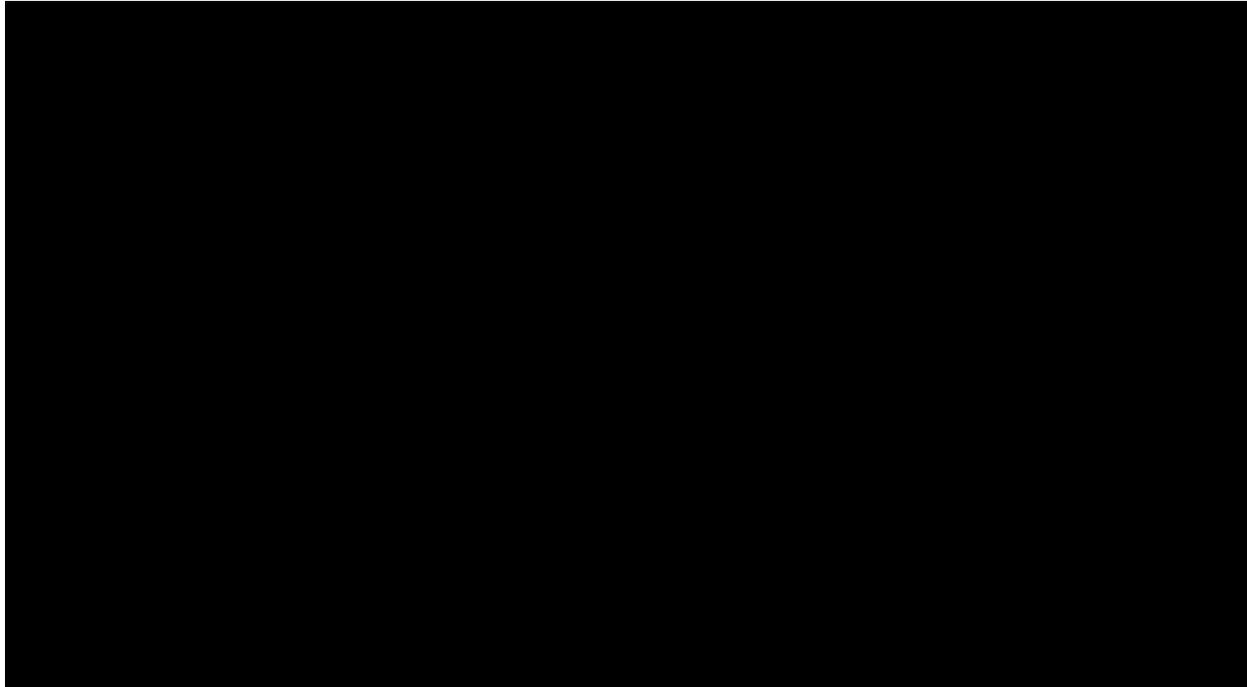
- Data-plane nodes in Cloud can provide application assurance for SaaS applications (e.g. Lync, Box)
- Peering with 3rd party Cloud Providers

MSP Enabled – Managed SD-WAN

- Multi-tenant cloud service designed for cloud deployment

- Software-based virtualization enables network abstraction that results in simplification of network operations.
- Network-based (hosted) and premises-based telephone Internet Protocol Voice Service (IPVS) is provided by Team MicroTech over a managed IP network. Team MicroTech also provides Managed LAN Service and Session Initiation Protocol (SIP) Trunking Service.
- Provides WAN Monitoring and IP-Network performance measurements over a Team MicroTech-managed IP network. In this case, the Managed NID and software will monitor managed IP network connections for end-to-end managed service and will ensure that Ethernet network KPIs are monitored and met.
- Team MicroTech will leverage a solution utilizing secure private WAN/LAN connections. Utilizing architecture like those shown, Team MicroTech can monitor and maintain performance of its network and voice service complying with the metrics in Section C.2.2.1.4.





We excel with industry-leading service response times. Customers call and have a real person answer the phone to assist, within seconds, with an average speed of answer (ASA) rate of 15 seconds and mean time to resolve (MTTR) of less than one day.

C. Service Coverage

For the purposes of this Solicitation response, Team MicroTech is bidding on the 25 CBSAs listed below. We have the capacity to expand on the CBSAs listed below if requested by the government. We propose to serve the top 25 markets as follows:

Rank	CBSA Name	CBSA Code
1	Washington-Arlington-Alexandria, DC-VA-MD-WV	47900
2	Baltimore-Columbia-Towson, MD	12580
3	Durham-Chapel Hill, NC	20500
4	Dallas-Fort Worth-Arlington, TX	19100
5	Chicago-Naperville-Elgin, IL-IN-WI	16980
6	San Jose-Sunnyvale-Santa Clara, CA	41940
7	Salt Lake City, UT	41620
8	Kansas City, MO-KS	28140
9	Atlanta-Sandy Springs-Roswell, GA	12060
10	Virginia Beach-Norfolk-Newport News, VA-NC	47260
11	St. Louis, MO-IL	41180
12	Nashville-Davidson--Murfreesboro--Franklin, TN	34980
13	Chattanooga, TN-GA	16860
14	Denver-Aurora-Lakewood, CO	19740
15	San Diego-Carlsbad, CA	41740

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

Rank	CBSA Name	CBSA Code
16	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD	37980
17	New York-Newark-Jersey City, NY-NJ-PA	35620
18	Houston-The Woodlands-Sugar Land, TX	26420
19	Richmond, VA	40060
20	Memphis, TN-MS-AR	32820
21	Huntsville, AL	26620
22	Orlando-Kissimmee-Sanford, FL	36740
23	Gulfport-Biloxi-Pascagoula, MS	25060
24	Hagerstown-Martinsburg, MD-WV	25180
25	San Antonio-New Braunfels, TX	41700

D. Security

Physical Security

Our team's systems are located in Tier 4 class data center locations. Each data center employs the same physical security standards in four different categories:

- Integrity - Physical access is controlled by 5 security parameters including mantraps and up to 500 surveillance cameras supported by infrared, ultrasonic, and photoelectric motion sensors. In addition, a 24x7 armed ex-military law enforcement staff is present.
- Confidentiality - Only authorized users can access any physical layer of our infrastructure.
- Authentication - Multiple levels of authentication in the system including 2 layers of biometric authentication.
- Audit Trail - Full historical reporting of any physical access

Network Security

Team MicroTech includes important network elements that interconnect systems and information across multiple locations. Therefore, maintaining network security at all levels is essential. We achieve a high level of network security through technical and procedural means with focus on the following:

■ [REDACTED]

■ [REDACTED]

In addition, our Network Operations Center (NOC) staff monitors all activities on the network 24x7. The NOC team manages all aspects of the network, not only to detect and prevent threats, but also maintain recovery control and audit logs of all users'

activities. This allows the security team to assist any necessary investigation or future audits.

Platform Access Security

As a cloud-based solution, we were built from the ground up as a multi-tenant solution with distributed systems on an application architecture which ensures that each tenant's security is fully preserved. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Application Security

Security considerations are a driving force for software high availability, software load distribution, and multiple tenancy support. Team MicroTech's software is designed to provide security at the application level with specific implementation around high availability and multi-tenancy to ensure uninterrupted business operation for each of our customers.

2.1.2.1.1 Service Description

Team MicroTech provides Cloud based PBX services (IPVS) based on the latest VoIP technology [REDACTED]

[REDACTED]

[REDACTED] Team MicroTech provides Managed LAN Service in order to assure VoIP service quality and quick response time in case of any issues. As the customer requires, Team MicroTech will provide a premises-based IPVS solution in compliance with RFP Section C.2.2.1.1.

2.1.2.1.1.1 Software High Availability

A complete application failure can be the result of either a DoS (Denial of Service) attack, for example, a flood of requests sent by a malicious application, or an external event (i.e. a power failure). It can manifest itself either as no response from a process, or as termination. Redundant applications (typically server applications), provide backup capability in the event that an application fails. If one server (the primary server) goes out of service for some reason, such as failure due to security attack, the backup server can act as the primary server, with little or no loss of service.

2.1.2.1.1.2 Software Load Distribution

In a cloud environment, deploying proxy and parallel servers add efficiency to large configurations, and can limit the damage caused by an outage or security attack. The use of these technologies can significantly reduce the loss functionality and data. We take advantage of proxy and parallel servers to ensure that in any event, such as security attack, we limit the service interruption for a particular client or application.

2.1.2.1.1.3 Multi-Tenant Security

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

2.1.2.1.1.4 Patches and Upgrades

Patches and upgrades for security, infrastructure, operating systems, databases, network devices, and applications are rolled out via patch management scheduling through a change control/management process. All components are addressed in a

controlled and timely fashion. Patches are tested in a non-production environment prior to being released for the production environment.

2.1.2.1.1.5 Security Monitoring

Security Monitoring and reporting is 24X7, 365 from multiple Team MicroTech Network Operations Centers. Security events are triggered on various tools and controls throughout the network. Once an incident is declared, appropriate response is taken by the subject matter experts for Root Cause Analysis, mitigation and remediation. Processes are in place to notify customers if and when they are affected by a security incident (see Network Security section above for additional information).

2.1.2.1.2 Standards

Team MicroTech's Cloud PBX, which has the capability of being scaled down and deployed on a customer's premise, complies with the following standards:

- ITU-T G.711 - Team MicroTech complies with this codec standard as default codec and can include other optional CODECs as required below.
- (Optional) ITU-T G.723.x, G.726, G.728, or G.729.x -Team MicroTech VoIP solution can support G.726, G.729. G.723.x is supported in hardware and G.728 has limited support (no transcoding).
- ITU-T H.323, H.350 – Team MicroTech provides full support for H.323.
- H.350 Directory service option can be activated if requested.
- Real-Time Transport Protocol (RTP) IETF RFC 3550 – Team MicroTech supports this protocol.
- Session Initiation Protocol (SIP) IETF RFC 3261 – Team MicroTech supports this protocol.

2.1.2.1.3 Connectivity

Team MicroTech brings capabilities that include both hosted (Cloud) and on-premise IPVS Solutions. The Cloud-based PBX can connect to and operate with a wireline or wireless network and can reach any voice telephone number, domestic or international, via Team MicroTech voice gateways to the PSTN. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

2.1.2.1.4 Technical Capabilities

Team MicroTech’s IPVS includes unlimited on-net to on-net and on-net to CONUS off-net calling. We provide capabilities that enable Cloud PBX users to establish and receive telephone calls between both in on-net locations and the PSTN.

Off-net calling to CONUS is included as the unlimited calling of our service. Calls to OCONUS, and non-domestic locations are subject to prices provided in Section B of the proposal. Equipment provided by Team MicroTech will support Power over Ethernet (PoE) to supply necessary power to IP phone sets or other PoE devices.

Team MicroTech provides remote access capability to make or receive phone calls as if the user were making or receiving calls with VoIP using our softphone. This solution is

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

compatible with PC, MAC, iOS, and Android, providing users with the ability to use a PC or Smartphone. The solution can also reroute calls intended for the VoIP phone to a regular land line or cell phone with no interruption to the caller.

Team MicroTech Cloud PBX service complies with the following capabilities:

- Real time transport of voice, facsimile, and TTY communications – Team MicroTech fully supports real time transport protocol and facsimile.
- Simple calls involving TTY/TDD users and our platform are supported as follows:
Two parties may set up a two-way call and both use TDDs to communicate with each other. This works in CFS assuming a high-bandwidth G.711 connection is established – the requirements for transmitting the Baudot tones are similar to those for fax tones, and the subscribers can be configured as fax or data subscribers on CFS forcing it to use G.711.

TDD users can also place calls to a Telecommunications Relay Service (TRS), where an operator working with a TDD can translate between the TDD communication with the TDD user, and normal speech with the regular phone user. This would be supported with the TRS connected over a normal phone line attached to the CFS, and the TDD user calling their number to complete a call (essentially a special case of the previous bullet). Team MicroTech's VoIP solution supports voicemails being left and received with Baudot tones.

- Real time delivery of Automatic Number Identification (ANI) - Team MicroTech provides ANI information as long as it is delivered by the originating party
- Operate with public network dial plans (e.g., North American Numbering Plan and ITU-E.164) - Team MicroTech hosted PBX operates with North American Numbering Plan as well as International Telecommunication Standards.
- Team MicroTech provides private dialing plans and supports direct dialing.
- (Optional) Operate with non-commercial, agency-specific 700 numbers - 700 numbers (dialed as 1-700-NXX-XXXX) are not widely used in the US with one exception - as a test number to identify your long distance carrier. With the exception of carrier identification, most often 700 numbers are toll calls. We support routing 700 numbers.

- Team MicroTech can provide Directory assistance and operator services via an existing agreement with ILEC.
- Unique directory numbers can be provided, as required, for all agencies, including portability of existing government numbers.
- Team MicroTech supports automatic callback (AC). This service allows the subscriber to automatically redial the last outgoing call, by dialing an access code.
- If the call to the last called number fails because the called party's line is busy, call setup is performed automatically when the target line becomes idle. The subscriber can cancel all outstanding AC on busy callback requests using another access code.
- Cloud PBX fully supports 3-way calling.

Team MicroTech provides gateways for compatibility between the contractor's IP-based network and the PSTN, or with agency UNIs. The specific gateway depends on the ordering agency's UNI requirements. Gateways and functionality:

Subscriber Gateway – Team MicroTech provides subscriber gateway to allow analog station or ISDN BRI interconnection to our VoIP network. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] A variety of configurations are available to support:

- Support for 2 to 24 analog ports
- High density scalable solution with three capacity options: 288, 216 and 144 FXS ports
- Rich subscriber feature set: 3-way conference with local mixing, call pickup, hunt groups, call forwarding, call hold and call transfer
- Echo cancellation, jitter buffer, voice activity detection (VAD) and comfort noise generation (CNG)
- Complies with MGCP, MEGACO, and SIP control protocols
- Leverage investment in existing analog telephone, modem, and fax systems – easing VoIP migration

- Lifeline for fallback to PSTN for E911 (Emergency number PSTN breakthrough) or upon network/power failure (FXO and/or FXS configurations)
- Standalone Survivability (SAS) keeps your business running in the event of a network failure
- Support for advanced coders such as NB-AMR and NB-OPUS
- Support for SRTP on all channels without capacity hit
- Integrated protection against surge damage on FXS ports (ITU-T K.21 - basic level compliance)
- Supports short and long haul up to 7.5 Km
- Support for emergency / elevator phones that require higher loop current and increased ring voltage
- Rich and Powerful SIP normalization and routing mechanisms for seamless interoperability
- SIP header manipulation
- Extensive fax support including T.38 version 3
- Supports survivability for hosted communications services and centralized IP-PBX deployments

[Redacted content]

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

Team MicroTech provides the capability of station mobility. Customers easily move IP phones within enterprise WAN facilities and initiate and receive calls as long as their network allows IP phone registration to our provided Cloud based PBX. Mobility increases the complexity of providing appropriate 911 services.

Team MicroTech is accustomed to working with other vendors and customers' firewall managers in order to allow in and out VoIP traffic. Our personnel work closely with the customer designated technical support to perform required firewall modifications to provide access to VoIP services and required security policies in order to avoid security issues. We ensure practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access.

This includes SIP-specific gateway security for SIP firewalls, where applicable. Team MicroTech ensures security practices and policies are regularly updated and audited. We acknowledge the general areas of security to be addressed are:

- Denial of service – Team MicroTech provides safeguards to prevent hackers, worms, or viruses from denying legitimate users from accessing IPVS.
- Intrusion – Team MicroTech provides safeguards to mitigate attempts to illegitimately use IPVS.
- Invasion of Privacy – Team MicroTech ensures IPVS is private and that unauthorized third parties cannot eavesdrop or intercept IPVS communication numbers, IP addresses or URLs.

Team MicroTech works with customer technical resources to evaluate and implement required security policies for customer managed firewalls. For managed LAN services, we configure and manage all required configuration and policies to prevent and address any security issue as requested.

Team MicroTech complies and provides these services to existing customers for E911. We have redundant connections to local PSAP to route any E911 calls from our customers. Each day, we update the PSAP database with new customer information as required.

Team MicroTech complies and provides Local Service Portability (LNP) following all applicable FCC requirements.

2.1.2.1.5 Features

Team MicroTech complies with the mandatory features and some optional features.

ID Number	Name of Feature	Description
1	Voice Mail Box	<p>Team MicroTech offers voice mail capability that includes voice messaging transmission, reception, and storage 24x7, except for periodic scheduled maintenance. The service meets or exceeds the following minimum requirements:</p> <ul style="list-style-type: none"> ▪ At least sixty minutes of storage time (or 30 messages). ▪ Ability to remotely access voice mail services. ▪ Secure access to voice mail via a password or PIN. ▪ Automatic notification when a message is received. ▪ Minimum message length of two minutes. ▪ Capability to record custom voice mail greetings. <p>Team MicroTech provides Voice Mail, Auto attendant, and 911/E911. Customer can have an administrator with access to modify, move, add, and delete accounts as required.</p> <p>The system has an included option to automatically send an email with a WAVE (.wav) file attachment of each voicemail message received by users of this feature to the email address that the user designates.</p> <p>Our VM provides users the capability to add other notification devices / email addresses or to update email information and email preferences when receiving and forwarding messages through a secure user web portal.</p>
2	Auto Attendant	<p>Our Auto Attendant allows callers to be automatically transferred to an extension without the intervention of an operator. Team MicroTech's Cloud PBX solution provides capabilities allowing callers to dial a single number for high volume call areas and to select from up to 9 options to be directed to various attendant positions, external phone numbers, and mailboxes or to a dial by name or extension, at a minimum.</p>
3	Augmented 911/E911 Service	<p>Team MicroTech complies with populating 911 Private Switch/Automatic Location Identification (PS/ALI) database with the government's profile which shall include all of the users' telephone numbers, station locations, building locations, building addresses, building floors, and room numbers during service implementation. We provide secure remote access to the government via a client or a web browser to allow the government to maintain the government's profile on an ongoing basis (e.g., to account for moves, adds, deletions, or other changes). We ensure these government profile updates are reflected in the PS/ALI database.</p>

Team MicroTech provides the following standard features in the basic service. Features can be assigned individually by customer:

- Caller ID
- Do Not Disturb
- Call Park
- Call Forward – Busy
- Hunt Groups
- Class of Service Restriction
- Conference Calling
- Call Forward – All
- Hotline
- Call Pickup
- Call Forward – Don't Answer
- Multi-Line Appearance

- Call Hold
- Directory Assistance
- Call Waiting
- Call Number Suppression
- Last Number Dialed
- IP Telephony Manager (Subscriber)
- Mobile apps for iPhone, iPad, and Android
- Unlimited Long Distance calling (Continental US)
- Hands on implementation and project management
- Phone rental option: Desk and conference phones
- Inbound caller ID name & number
- Find-me, Follow- me features
- Voicemail to Email
- Simultaneous Ring
- Call Park & Pickup
- Audio Conferencing
- Speed dial Group & Personal
- Selective Call Rejection/Acceptance
- Distinctive Ringing
- Call Transfer
- Speed Dial
- Specific Call Rejection
- IP Telephony Manager (Administrator)
- Call Management and phone system administration
- Unlimited Local Calling
- Nationwide 4-Digit Dial capability
- 24x7x365 support team
- Integration with CRM tools such as Salesforce, Zendesk, Clio, Netsuite and more
- Call log reports
- HD voice
- Seamless handoff between desk and mobile phone
- Voicemail Transcription Services
- Faxmail (inbound & outbound faxing from desktop)

2.1.2.1.6 Interfaces

The UNIs at the SDP are mandatory unless marked optional. Team MicroTech’s Cloud PBX can be supported on a router or LAN Ethernet connection using SIP protocol. Team MicroTech will comply with the IPVS interfaces required by Section C.2.2.1.3 of the Solicitation.

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type	Meets/Exceeds
1	Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)	Up to 100 Mbps	SIP (IETF RFC 3261), H.323, MGCP, or SCCP	Meets

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

2.1.2.1.7 Performance Metrics

The performance levels and AQL of KPIs for IPVS are mandatory unless marked optional. Team MicroTech complies with required performance levels and AQL of KPIs for IPVS.

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	Meets/Exceeds
Latency	Routine	200 ms	≤ 200 ms	Meets
Grade of Service (Packet Loss)	Routine	0.4%	≤ 0.4%	Meets
Availability	Routine	99.6%	≥ 99.6%	Meets
	Critical	99.9%	≥ 99.9%	
Jitter	Routine	10 ms	≤ 10 ms	Meets
Voice Quality	Routine	Mean Opinion Score (MOS) of 4.0	MOS ≥ 4.0	Meets
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	Meets
	With Dispatch	8 hours	≤ 8 hours	

2.1.2.2 Managed LAN Service (C.2.2.1.5)

Team MicroTech manages LAN switches at the customer premise via our Managed LAN Services (MLAN Service). MLAN Service provides management of Agency designated local area network (LAN) switches. We provide options for three levels of management: 1) Monitor and Notify Service, 2) Physical Management or 3) Full Management. Our Network Operations Center (NOC) provides 24x7x365 monitoring, management and restoral. In addition to management, we ensure that only OCO approved services are provided.

MLAN Service Levels:

- Monitor and Notify service includes proactive Simple Network Management Protocol (SNMP) of customer LAN switches for status and error messages. Additionally, we will use Internet Control Message Protocol (ICMP) to periodically poll (“ping”) the devices to ensure availability. When our poll indicates a switch is unavailable or we receive a critical SNMP message, we create a trouble ticket and notify the customer within 15 minutes via phone or email. We initiate troubleshooting and continue until the issue is resolved.
 - Customer responsibilities:
 - Trouble isolation
 - Diagnostics, repair and maintenance dispatch of switches and devices
 - Management of all connected devices outside MLAN scope
 - Provide SNMP read access to all MLAN switches
- Physical Management also includes design services in addition to the services provided under Monitor and Notify.
 - Customer responsibilities
 - Changes to LAN network
 - Routine maintenance of LAN switches
- Full Management includes all of the services of Physical Management plus full management of the MLAN to include trouble isolation, diagnostics, repair and maintenance dispatch of devices.
 - Customer responsibilities
 - Provide privileged access to all LAN Switches

- Provide NMP write access community string for all monitored LAN Switches
 - Additional managed devices are available 7 days from order under all service levels
- It is Team MicroTech's practice that all service-affecting faults are designated with a critical severity. As stated above, we open a trouble ticket when a monitoring system or our staff detect the fault. We manage these faults according to our IT Service Management (ITSM) process and the incident is automatically escalated to the next level if not resolved with a specified time frame. The purpose of escalating an open case is to ensure that all appropriate resources are focused on solving the issue and executing an action plan to resolve the issue, as well as ensuring communication to our internal as well as the customers' points of contact. In all cases, a customer may initiate an escalation at any time, for any reason. 15 minutes after the ticket is opened, if the critical service-affecting issue remains unresolved, we escalate the incident to the next higher support tier. Escalations continue to our Tier 3 or OEM support until the issue has been identified, resolved, tested and service has been restored.
- Team MicroTech will provide all hardware and licensing necessary to extend the IPVS site demarcation point to the terminating device (e.g., the handset), for both hosted and premises based solution. In the case of an on-premises solution this would include any hardware or licensing necessary to support on-premises call processing (e.g., call manager, IP PBX, etc.).
 - Team MicroTech's hardware/software solution will interoperate with the ordering agency's provided VoIP ready cabling infrastructure including category 5, 5E, 6, 6A and single mode and multimode fiber at a minimum. We will identify any cabling limitations with regards to either form of VoIP solution in our proposals.
 - Team MicroTech will propose 2-4 hour installation time intervals for additional user devices at sites already using a Managed LAN Service.
 - Team MicroTech will not include any wireless devices or components on the LAN (i.e., wired solution only) unless requested and approved by the OCO.
 - Team MicroTech's Managed LAN Service will not support other services (i.e., data video, etc.) unless requested and approved by the OCO.

For IPVS service specifically, in addition to the services described above, Team MicroTech provides Managed LAN services whereby we will provide and manage all

LAN networking hardware components (e.g. Layer 2 switching devices, routers, switches, call servers, etc.) to extend the IPVS from the site demarcation point to the terminating user device (e.g., handset), including the management of the router that terminates the IPVS access arrangement. Equipment provided by Team MicroTech will support Power over Ethernet (PoE) in order to supply necessary power to IP phone sets or other PoE devices. IPVS service is a pre-requisite for Managed LAN Service. Under Managed LAN services for IPVS service, Team MicroTech will provide, manage, maintain and repair or replace all equipment necessary to provide the Managed LAN Service, except for those portions of the service for which the government is responsible (e.g., power, facilities, rack space, cabling/wiring). Team MicroTech will be responsible for the ongoing maintenance and upgrades of the contractor-owned equipment used to provide the IPVS Managed LAN Service. If the contractor replaces, makes any changes to the contractor's equipment or device software, or reprograms user devices in order to meet the required service performance level, the government will not incur any additional cost.

2.1.2.3 Session Initiation Protocol Trunk Service

A. Understanding

SIP Trunks are designed to provide a cost-effective and reliable voice service for IP PBX's. In a typical installation, a provider-owned and managed Enterprise SIP Gateway (ESG) device is installed at the customer premises, connected to the customer's IP PBX. The SIP service provides a direct IP connection between a SIP-enabled PBX system on an agency's premises and our SIP-compliant IPVS network. SIP trunking shall be fully integrated with IPVS to support calling to on-net and off-net locations. The network and its management are provided by the underlying network service.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

B. Quality of Services

Our team's SIP Trunking for Unified Communications and Collaboration (UC&C) applications will provide QoS. A high QoS helps expedite projects and improve customer service through rapid information sharing and ideas between colleagues, customers, partners, and suppliers. Applications include instant messaging, voice and video calling, desktop sharing, conferencing, and web collaboration. We have UC&C clients for desktops, laptops and smartphones to ensure GSA customers are easily contactable from practically whatever device they use and from wherever they need to work.

C. Service Coverage

N/A

D. Security

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

2.1.2.3.1 Standards

SIP Trunking offers efficiency and flexibility with optional bursting capability in voice traffic/capacity. The system also interfaces with newer PBXs more efficiently, and with typically less expensive interfaces than traditional PRI cards. Team MicroTech supports:

- Automatic call routing – Inbound/Outbound blocking may also be supported
- Bandwidth QoS management (some partners)
- Trunk bursting
- Telephone number blocks (DID) – some limitations, such as number of DID's on a single SIP Trunk, may apply depending on partner.

2.1.2.3.2 Technical Capabilities

With the latest advancements in voice over IP technology, SIP Trunking offers a tailored, cost-effective voice service with scalable features and end-user mobility options that increases productivity, improves efficiencies and increases reliability. The system integrates well with your existing communications network, with your PBX already certified for integration for our SIP trunking.

Our team and partners maintain interconnection with ILEC/RBOC institutions nationwide as well as interconnections with independent telephone companies, including many cooperative telephone companies (i.e. South Central Rural, Foothills Rural, Highland Telephone, etc.). Our team's extensive background providing service to residential and business broadband customers allows us to be able to provide 24/7 prioritized call routing to business customers in our world-class, U.S.-based support centers, where we proactively monitor and troubleshoot network issues that may arise. This proactivity assists our operations team to support performance metrics as defined in 2.1.2.3.4.

2.1.2.3.3 Features

Team MicroTech supports the following SIP Trunk Service Features as described:

- Automatic call routing (ACR) – Our service allows each direct inward dial (DID) number to failover to a different number (managed by the customer). We automatically redirect calls in the event of a service disruption.
- Bandwidth QoS management – In conjunction with data service and compatible equipment, bandwidth is managed such that any shared bulk traffic from the enterprise is throttled back, giving the VoIP media traffic priority, and in so doing attains a QoS for VoIP traffic over that SIP trunk. This preserves the quality of voice traffic. SLA reports allow the customer to monitor this throttling in order to adjust service plans or capacity.
- Trunk bursting – We support trunk bursting to accommodate traffic that occasionally exceeds defined trunking limits. Bursting is included as a standard feature with the level of bursting determined based on the defined trunking limit. This bursting is compatible with nearly any IP or analog PBX.
- Telephone blocks of Direct Inward Dialing numbers (DID) – Are Subject to availability of contiguous DID numbers in the requested quantities. We allow the customer to request blocks of DIDs according to their needs and where blocks of sufficient sizes are not available; we will provision the request into the smaller numbers blocks of contiguous numbers based on customer request to match “last four”. This request where quantities exceed the limits of the “last four” digits, can be expanded to the last five, six or seven digits,

As we upgrade our infrastructure, we intend to offer additional features based on feedback from our customers.

2.1.2.3.4 Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	Meet/Exceed
Latency	Routine	200 ms	≤ 200 ms	Meets
Grade of Service (Packet Loss)	Routine	0.4%	≤ 0.4%	Meets
Availability	Routine	99.6%	≥ 99.6%	Meets
	Critical	99.9%	≥ 99.9%	Meets
Jitter	Routine	10 ms	≤ 10 ms	Meets
Voice Quality	Routine	Mean Opinion Score (MOS) of 4.0	MOS ≥ 4.0	Meets
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	Meets
	With Dispatch	8 hours	≤ 8 hours	Meets

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

2.1.3 Managed Network Service

A. Understanding

Managed service is the practice of outsourcing day-to-day customer management responsibilities and functions to the service provider as a strategic method for improving operations and cutting expenses. The managed service provider is accountable for the functionality and performance of the managed service.

Managed services provide the delivery and management of network-based services, applications, solutions, labor, and equipment needed by the enterprises. The managed service includes a) service planning and solution engineering, b) solution implementation (including labor and equipment), c) service provisioning, d) end-to-end service management (including LAN routers and WAN), and e) service assurance (performance metrics and SLA management).

B. Quality of Services

Team MicroTech's Managed Network Service Offering meets or exceeds the standards for quality and standards for performance across the agency's networks, including planning engineering, design, and implementation, day-to-day operations, and maintenance. In our Managed Services offering, we provide dynamic and elaborate cross-functional EIS services which are interoperable and provide the highest quality of services across a range of network options available to end users.

Team MicroTech supports interoperability for our service offerings so a user of a service from one EIS contractor can communicate with users of services from other EIS contractors with equivalent performance. We will make interoperability available for any service that is currently commercially offered by Team MicroTech and is interoperable with the services of other EIS contractors. We will make available any future service interoperability at no additional cost to GSA when Team MicroTech offers the interoperability for our commercially provided service and we will support interoperability between voice services, circuit switched data service, and wireless services.

When Team MicroTech identifies a TO, we analyze the needs of the particular correspondent and identify a customized solution for the requirements of the TO. We believe our customized approach through agency-approved hardware and software is the best way to bring the best quality of managed network services. We know our full

spectrum of services is interoperable and our trained technicians provide a single point of accountability for all networks managed under this service, including operations, maintenance, and administration activities. Below, Team MicroTech identifies and analyzes our standards, connectivity, technical capabilities, managed network design and engineering services, implementation management and maintenance, features, interfaces, and performance metrics.

C. Service Coverage

For the purposes of this solicitation response, Team MicroTech is bidding on the 25 CBSAs listed below. We have the capacity to expand on the CBSAs listed below if requested by the government. We propose to serve the top 25 markets as follows:

Rank	CBSA Name	CBSA Code
1	Washington-Arlington-Alexandria, DC-VA-MD-WV	47900
2	Baltimore-Columbia-Towson, MD	12580
3	Durham-Chapel Hill, NC	20500
4	Dallas-Fort Worth-Arlington, TX	19100
5	Chicago-Naperville-Elgin, IL-IN-WI	16980
6	San Jose-Sunnyvale-Santa Clara, CA	41940
7	Salt Lake City, UT	41620
8	Kansas City, MO-KS	28140
9	Atlanta-Sandy Springs-Roswell, GA	12060
10	Virginia Beach-Norfolk-Newport News, VA-NC	47260
11	St. Louis, MO-IL	41180
12	Nashville-Davidson--Murfreesboro--Franklin, TN	34980
13	Chattanooga, TN-GA	16860
14	Denver-Aurora-Lakewood, CO	19740
15	San Diego-Carlsbad, CA	41740
16	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD	37980
17	New York-Newark-Jersey City, NY-NJ-PA	35620
18	Houston-The Woodlands-Sugar Land, TX	26420
19	Richmond, VA	40060
20	Memphis, TN-MS-AR	32820
21	Huntsville, AL	26620
22	Orlando-Kissimmee-Sanford, FL	36740
23	Gulfport-Biloxi-Pascagoula, MS	25060
24	Hagerstown-Martinsburg, MD-WV	25180
25	San Antonio-New Braunfels, TX	41700

D. Security

Team MicroTech values the need for secure managed networks. Our Risk Management Framework (RMF) employs security tactics across day-to-day and network-to-network

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

requirements. These include preemptive measures. For instance, if our 24x7x365 monitoring on our managed networks identifies a threat, we build our threat solution on that network and patch across other networks, as necessary. Our process identifies and mitigates security awareness, treats, and breaches, should they occur.

2.1.3.1 Service Description

Through Managed Network Services Team MicroTech takes full responsibility of the agency's networks, including planning engineering, design, and implementation, day-to-day operations, and maintenance. Our offerings include all functions typically performed while running a telecom network. Those functions are as follows:

- Day-to-day operation and management of the entire network infrastructure including transport services (Ethernets, MPLS, Fiber), Voice services (SIP trunks, Centrex Class 4,5), and Cloud Services (VM Ware private cloud and all flavors of cloud services).
- Management of end-customer problems escalated by the agency's customer care function.
- Corrective and preventive field maintenance through 7 x 24 x 365 monitoring and Network Operations Center services.
- Optimization of systems and services to ensure performance is maintained at or above agreed quality levels through preventive maintenances, upgrades, and engineering services.
- Management of changes to the network through Quality Assurance Services.
- Installation and upgrades of equipment.
- Multivendor Support [REDACTED]

Team MicroTech Network Managed Services embraces multi-vendor environments, which gives the agency the flexibility to develop and deploy services and infrastructure by using their vendor of choice.

Team MicroTech uses the appropriate labor and equipment as defined in the Task Order (TO).

2.1.3.2 Functional Definition

Team MicroTech MNS Network Management Solutions provides a single point of accountability for all network managed services to our customers. Real-time proactive

infrastructure monitoring and troubleshooting is accomplished with reliable monitoring tools such as PRTG sensors and probes, CACTI and logging tools such as Intrusion Detection/Prevention systems and Syslogs. Team MicroTech can provide these services with our Customer Support department and NOC (Network Operations Center) using all of the necessary tools to maintain, operate and administer all activities of the agency's infrastructure.

Team MicroTech is the agency's single point of accountability for all networks managed under this service, including operations, maintenance, and administration activities.

2.1.3.3 Standards

Team MicroTech MNS complies with all appropriate and specific standards for the underlying EIS access and transport services identified in the TO:

2.1.3.4 Connectivity

Team MicroTech MNS works with underlying EIS offerings such as VPNS, PLS and other services as needed, to ensure seamless connectivity to agency networking environments. We have experience designing and implementing VPNS and Private Line Services, Site-to-Site or Host-to-Site ensuring seamless connectivity to remote networks.

2.1.3.5 Technical Capabilities

Team MicroTech complies with MNS capabilities provided by the contractor.

2.1.3.5.1 Design and Engineering Services

Our MNS provides design and engineering services that include:

- Identification of hardware, firmware, and software for all Network related devices and SRL required by the agency to deliver the EIS services. Our services assist customers to procure any network device and software required.
- Networking, engineering, and consulting services by designing protocol integration, redundancy schemes, traffic engineering, traffic filtering, and prioritization requirements. Team MicroTech is up to date with all protocols and complies with them according to their RFCs and industry standards. We measure and create reports on capacities to guarantee performance levels and are proactive to adjust as necessary.

- Complete project management for design, engineering, implementation, installation, access coordination, provisioning, equipment configuration, hardware testing, and service activation. Team MicroTech coordinates installation activities with the agency to minimize the impact on the current networking environment.

2.1.3.5.2 Implementation, Management and Maintenance

Team MicroTech develops, implements, and manages comprehensive solutions using the EIS services to meet agency-specific requirements. [REDACTED]

[REDACTED]

- Access solutions through a combination of different services that fulfill customer needs and specifications. [REDACTED]

[REDACTED]

- Transport solutions [REDACTED]

- Customer premises solutions [REDACTED]

- Security solutions as required by the agency.

Team MicroTech supplies and manages the hardware, firmware, and related software required by the agency. Components include but are not limited to routers and switches, encryption devices, CSUs/DSUs, hubs, adapters, and modems. We provide customers with logistics and procurement services to supply and manage the hardware, firmware, and all related networking devices.

Team MicroTech provides tools to:

- Monitor performance of agency-specific networks including transport services, access circuits, and government edge routers
- Provide real-time visibility of transport and access services performance

Team MicroTech MNS provides real-time visibility of transport and access services performance with SNMP tools [REDACTED]

Performance monitoring tools and any monitoring tool that the customer specifies.

Reports on and access to these tools are also provided to customers.

Team MicroTech:

- Manages the network in real-time on a 24x7 basis. Team MicroTech's MNS NOC department monitors in real-time, 24x7, all customer devices and proactively reacts to any potential anomaly that may occur in the network. We use SNMP tools such as [REDACTED] and other means of alert along with expert technical personnel 24x7x365.
- Team MicroTech MNS supports remote management capabilities from its operations center to every device it monitors by utilizing secure remote tools defined in the TO.
- Monitors all devices utilizing performance sensors that allow us to set thresholds that send notifications and can be configured to probe in any interval according to customer specifications.
- Assesses and reports access and transport services performance and SLAs by utilizing monitoring and reporting industry tools.
- Provides assessment and reports on customer-specific network capacity and performance. We use the latest reporting and assessment tools that proactively react to performance changes.

Team MicroTech permits SNMP read-access data feeds that provide the agency with managed equipment information, as applicable. We filter and dedicate traffic for SNM and any protocol in order to remotely monitor all devices according to customer specifications.

Team MicroTech manages network configuration. Activities include the following:

- Adding a protocol
- Adding, moving or removing Customer Premises Equipment (CPE)

- Changing addressing, filtering, and traffic prioritization schemes
- Optimizing network routes
- Updating equipment software and/or configuration, including but not limited to, firewall and VPN security devices
- Upgrading or downgrading bandwidth
- Implementing configuration changes for all agency-specific devices
- Maintaining a configuration database for all agency-specific devices
- Auditing government router configurations

Team MicroTech MNS provides IP address management for IPV4 and IPV6 and submits agency-completed American Registry for Internet Numbers(ARIN) justification requests for specified IP allocations in order to support the service offered. We have vast experience with the ARIN process for IP administration services.

Team MicroTech monitors and controls access to equipment under our control including limiting access to authorized personnel, and implementing passwords and user permissions as directed and approved by the agency.

Team MicroTech maintains a backup of all of its customers devices [REDACTED]

[REDACTED] This database of device backups is accessed remotely via VPN that we provide.

Team MicroTech maintains records of all managed devices and manages patches, upgrades and bug fixes as they become available when device vendors send their advisories. First, we test the upgrade or bug fixes before deployment to avoid disruptions.

Team MicroTech performs preventive and corrective maintenance to all devices it manages. We constantly receive and search for vendor advisories and documentation about preventative and corrective maintenance so that systems are up to date and to prevent systems outages.

Our MNS provides preventative and corrective maintenance on agency-specific devices.

Team MicroTech uses several monitoring tools to proactively detect problems, respond to alerts, and promptly report situations that have an adverse effect to our customers.

Our NMS services provide notification of alarms, network troubles and service

interruptions via email, telephone, SMS, and comply as specified in the TO. We use tools such as; [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] We proactively detect problems, respond to alerts, and promptly report situations that adversely affect output to the agency. We:

- Monitor agency-specific network availability and quality of service (e.g., network delays, packet loss).
- Monitor access circuit availability and QoS.
- Monitor the government's edge router availability and performance.
- Monitor transport service availability at the government's network equipment.
- Monitor agency-specific network performance from government network equipment to government network equipment.
- Monitor transport service availability up to the government's network equipment.
- Monitor transport service performance from government network equipment to government network equipment.
- Provide, monitor and manage circuits for out-of-band government network equipment management.
- Open/close trouble tickets in agency's trouble ticketing system.
- Open/close trouble ticket in contractor's trouble ticketing system.
- Troubleshoot access and transport service faults and coordinate faults resolution/repairs.
- Troubleshoot government network equipment faults and coordinate resolution/repairs.
- Troubleshoot agency-specific network faults.
- Notify agency-specific network users of faults and maintenance via agency alerts.
- Answer NOC Help Desk phones and provide Tier-1 support to agency-specific network users.

- Provide Tier-1/Tier-2/Tier-3 support to agency NOC for contractor access and transport services.
- Provide Tier-1/Tier-2/Tier-3 support to agency NOC for the components of the Agency's network that are managed by the contractor.

Team MicroTech provides the agency with real or near real-time access to the following:

- Installation schedule detailing the progress of activities such as the implementation of equipment, access and transport circuits, and ports, as applicable. This allows agencies to track the provisioning process through completion at any time. Near real-time access to the installation schedule is acceptable.
- Network statistics and performance information including equipment data availability, output and delay statistics, CoS settings, and application-level performance information.
- Trouble reporting and ticket tracking tools.
- Security logs.

Team MicroTech provides inventory tracking tool(s) to maintain and track all agency circuit, transport service and equipment inventory information. We provide real-time project tools to keep track of installation, provisioning, and activities to track project status [REDACTED]. Customers can securely see the progress of their installation or project status and actively interact with their project manager. We provide secure links between the customer and our tools. Customers have a direct and secure access to our trouble reporting ticketing system to track the status and interact with the owner of the ticket. Security Logs are also provided to the customer in a secure manner and real-time.

Team MicroTech NMS provides customers with a secure account to our monitoring systems in order to monitor current and historical information on the health of the Network and all devices. These sensors include: Bandwidth, QoS levels and thresholds, Errors, Delay, End to End Network Views, Network Statistics, CPU utilization, Traffic, Ports, and Protocols views and many other sensors that could be added as needed. We provide the agency with secure access to current and historical information which includes, but is not limited to, the following:

- Bandwidth and service quality information

- Burst analysis identifying under or over utilization instances
- Data errors
- Delay, reliability and data delivery summaries
- End-to-end network views
- Exception analysis
- Link, port, and device utilization
- Network statistics
- Protocol usage
- CPU utilization
- Traffic, port, and protocol views

2.1.3.6 Features

Team MicroTech provides these features:

- GFP and SRE Maintenance. Team MicroTech NMS provides all customers with furnished property maintenance in all technical areas. [REDACTED]
[REDACTED]
[REDACTED] Agency-Specific Network Operations Center (NOC) and Security Operations Center (SOC). The contractor shall provide agency-specific help desk services and shared or dedicated NOCs and SOCs to meet agency requirements.
- Network Testing. Team MicroTech NMS provides the customer with development services which addresses each customers' potential need to test equipment, software, and applications on our network facilities prior to purchase and deployment. These services cover but are not limited to voice, data, video, VPN, and VoIP services. This testing can be performed at customer discretion and structured in collaboration with Team MicroTech.
- Traffic Aggregation Service (DHS Only). Team MicroTech NMS provides agencies with Traffic Aggregation Services. We establish and maintain secure facilities (DHS EINSTEIN Enclaves) where DHS-furnished equipment can be deployed, provide network connectivity from the DHS EINSTEIN Enclave to the DHS data centers, and route all traffic subject to National Policy requirements described in Section C.1.8.8 and in accordance with 6 U.S.C. § 151 through (i.e., deliver to and receive from) a

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

DHS EINSTEIN Enclave for processing by the latest generation of EINSTEIN capabilities. We securely send traffic back to its destination once it is received at the EINSTEIN Enclave and processed. We assume responsibility for maintaining and repairing the traffic aggregation service, including associated commercial security services and all communication links and provide engineering support to integrate the DHS GFP sensor equipment, data center and communications infrastructure into our services. A SOC and/or NOC will manage the baseline for agency traffic normalization and traffic monitoring (signatures). [REDACTED]

[REDACTED] These sites are all highly experienced in co-location and provide COOP redundancy that exceeds the double standard for a tier 3 level facility in addition to being located in some of the nation's highest bandwidth connectivity centers. These sites will also be the physical locations for logical connections of customer and provider enterprises, managing of TICs, and other infrastructure components of our major enclaves. Team MicroTech uses high performance computing platforms as well as scalable offerings to baseline traffic, disambiguate entities, and identify specific traffic for routing through the DHS enclaves. (see section 1.1.3 for additional details regarding security operations and routing for Einstein enclaves). We also provide assistance to DHS in the maintenance and repair of the sensor system to the extent of receiving phone calls or emails requesting "Smart-Hands" service of DHS-supplied equipment.

- The National Cyber Protection System will be installed in a respective SEN in order to monitor all traffic and if any non-participating agency traffic is discovered, our team will report it to DHS following discovery as well as remediate it accordingly.

2.1.3.7 Interfaces

Team MicroTech MNS supports the UNIs for all underlying EIS access and transport services.

2.1.3.8 Performance Metrics

Team MicroTech acknowledges that the MNS performance levels are specified in the TO.

2.1.4 Access Arrangements

[REDACTED]

Team MicroTech's access supports many applications such as voice, data, video, and multimedia. Access is provided from the nearest regional hub to the nearest carrier POP to the SDP.

2.1.4.1 Understanding

Team MicroTech's understanding of the requirement is to serve, at a minimum, 25 of the top 100 CBSAs. We propose to serve the top 25 CBSAs and are prepared to provide global coverage for the CONUS and OCONUS areas included in each of these CBSAs. We provide the mandatory services for the product sets described above in response 1.1. We provide these services to all government locations within these CBSAs.

2.1.4.2 Quality of Services

Team MicroTech delivers all of the required access capabilities as defined in the RFP.

2.1.4.3 Service Coverage

We understand the requirement to serve at least 25 of the top 100 CBSAs. We propose to serve the top 25 CBSAs and are prepared to provide global coverage for the CONUS and OCONUS areas included in each of these CBSAs. We provide the mandatory services for the product sets described above in response 1.1. We provide these services to all government locations within these CBSAs.

We propose to serve the top 25 markets, as follows:

Rank	CBSA Name	CBSA Code
1	Washington-Arlington-Alexandria, DC-VA-MD-WV	47900
2	Baltimore-Columbia-Towson, MD	12580
3	Durham-Chapel Hill, NC	20500

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

Rank	CBSA Name	CBSA Code
4	Dallas-Fort Worth-Arlington, TX	19100
5	Chicago-Naperville-Elgin, IL-IN-WI	16980
6	San Jose-Sunnyvale-Santa Clara, CA	41940
7	Salt Lake City, UT	41620
8	Kansas City, MO-KS	28140
9	Atlanta-Sandy Springs-Roswell, GA	12060
10	Virginia Beach-Norfolk-Newport News, VA-NC	47260
11	St. Louis, MO-IL	41180
12	Nashville-Davidson--Murfreesboro--Franklin, TN	34980
13	Chattanooga, TN-GA	16860
14	Denver-Aurora-Lakewood, CO	19740
15	San Diego-Carlsbad, CA	41740
16	Philadelphia-Camden-Wilmington, PA-NJ-DE-MD	37980
17	New York-Newark-Jersey City, NY-NJ-PA	35620
18	Houston-The Woodlands-Sugar Land, TX	26420
19	Richmond, VA	40060
20	Memphis, TN-MS-AR	32820
21	Huntsville, AL	26620
22	Orlando-Kissimmee-Sanford, FL	36740
23	Gulfport-Biloxi-Pascagoula, MS	25060
24	Hagerstown-Martinsburg, MD-WV	25180
25	San Antonio-New Braunfels, TX	41700

2.1.4.4 Security

Access Arrangements provide the convention to specify the originating and/or terminating access component required to connect the SDP to the agency’s POP when that access component is required to deliver a telecommunications service for EIS. We provide both circuit-switched Access Arrangements and Dedicated Access Arrangements. While these two types of access arrangements provide sub-arrangements within each, Team MicroTech maintains the required security levels across each access arrangement throughout its intended purposes.

2.1.4.5 Service and Functional Description

Team MicroTech meets various requirements at the application level, by first seeking out the specific application and the specific solution to meet the customer requirements.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED]

In the case where access arrangement does not exist or does not have sufficient capacity, and the contractor has to provide special construction through the implementation, rearrangement or relocation of physical plant solely for the government-requested access arrangement requires a site survey and a written method of procedure (MOP) to the subject customer and buy off by both the subject customer and the contractor. [REDACTED]

[REDACTED]

When necessary to fulfill an order, Team MicroTech performs site surveys of potential operational locations to collect and validate floor plans, physical measurements, building power capacity, and external ingress/egress factors. This process is part of the scope of work (SOW) and method of procedure (MOP) which the teaming partners go through prior to construction. The SOW drives the MOP and the MOP is what the subject customer will sign off on with the contractor. This process depends of weather conditions and size of the project, but on average will take three weeks to get to the SOW and another two weeks to define into a project plan known as the MOP.

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

Team MicroTech delivers site survey reports after the completion of the physical site visits. Our partners will deliver these reports in conjunction with J.10 (special access construction template for the site survey). These reports are a matter of policy and the Team MicroTech also steps through a process to get a scope of work (SOW) for internal costing and then we step through the process of building a method of procedure (MOP); we leave this in the hands of the customer and can accommodate an “all of the above” sharing of information with the understanding that the SAC template is the usual and customary document.

2.1.4.6 Standards

Team MicroTech’s access arrangements conform to the following standards:

- ANSI T1.102/107/403/503/510 for T1
- ANSI T1.607/610 for ISDN PRI
- Telcordia PUB GR-499-CORE for T3
- ANSI T1.105 and 106 for SONET
- Telcordia PUB GR-253-CORE for SONET
- ITU-TSS G.702 and related recommendations for E1 and E3
- Frequencies grid and physical layer parameters for Optical Wavelength:
 - DWDM: ITU G.692 and G.694 as mandatory and G.709 and G.872 as optional
 - WDM: ITUG.694.2 and Telcordia GR 253
- Applicable Telcordia for DWDM systems are GR-1073, GR-1312, GR-2918, GR-2979 and GR-3009
- EIA/TIA-559, Single Mode Fiber Optic System Transmission Design
- Telcordia GR-20-CORE for Generic Requirements for Optical Fiber and Optical Fiber Cable GR-253 (SONET), and GR-326 (Connector)
- Digital Subscriber Line (DSL) - ADSL and SDSL:
 - ADSL and DSL Forums
 - ITU-TSS Recommendation G.992 for ADSL (interoperable DSL modem and DSLAM line card)
 - ANSI T1.413 (compatible DSL modem and DSLAM line card from the same manufacturer)
- ISDN based DSL (IDSL): ISDN Forums

- Ethernet Access: IEEE 802.3, including 10 Base-T/TX/FX, 100 Base-TX/FX, 1000 Base-T/FX/ULX/B/BX/PX, and 10/40/100 Gigabit Ethernet (IEEE 802.3ae and 802.3ba)
- Cable High-Speed Service: DOCSIS (Cable Labs) standards

Team MicroTech will comply with all new versions, amendments, and modifications to the above documents and standards.

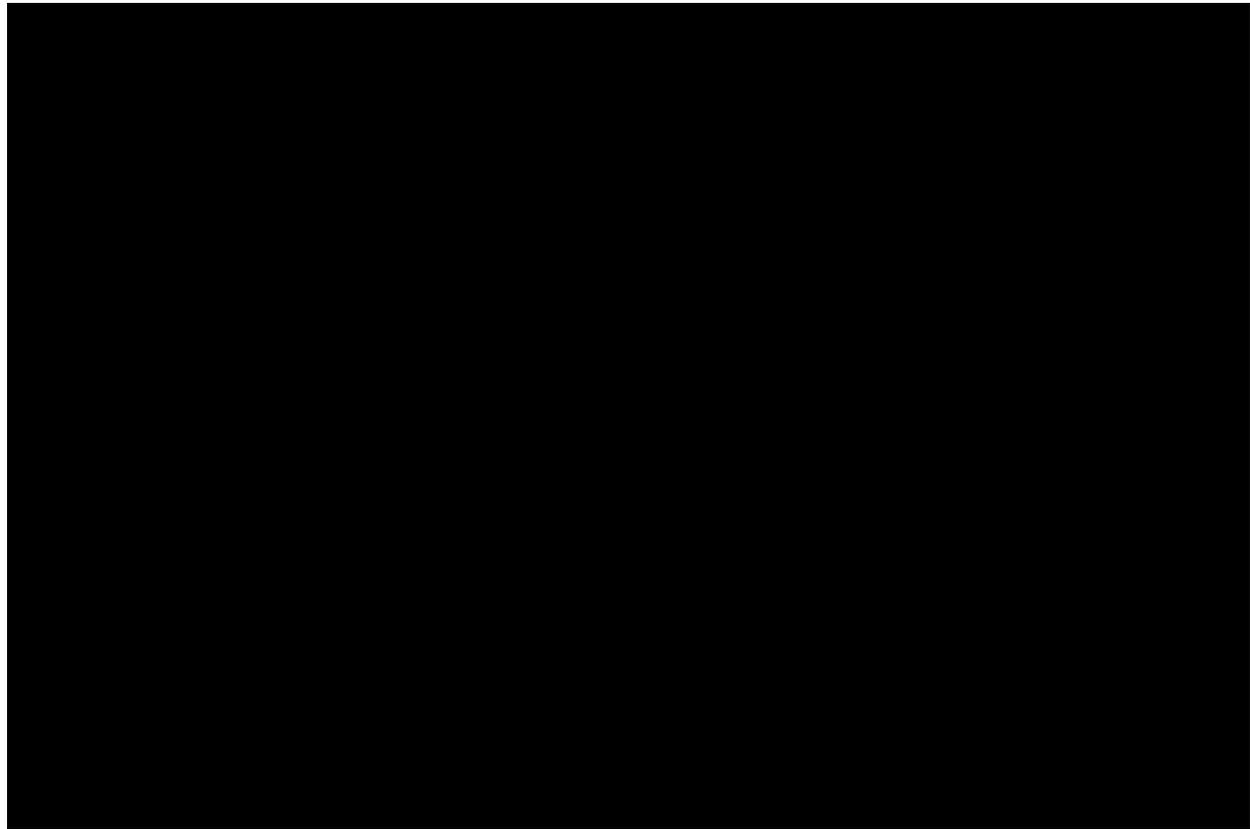
2.1.4.7 Connectivity

Team MicroTech complies with all listed Access Arrangement connectivity needs. We understand and acknowledge that the UNIs at the SDP for Access Arrangement enumerated in Section C.2.9.3 are mandatory and we will comply with the requirement. We perform a site survey of the SDP to determine the required UNI required per Section C.2.9.3. We then determine the SRE needed and add that to our Catalog, as necessary. In addition, we engineer and provision any needed POP upgrade to meet the Access Arrangement network interface, if required.

2.1.4.7.1 Ethernet aggregation

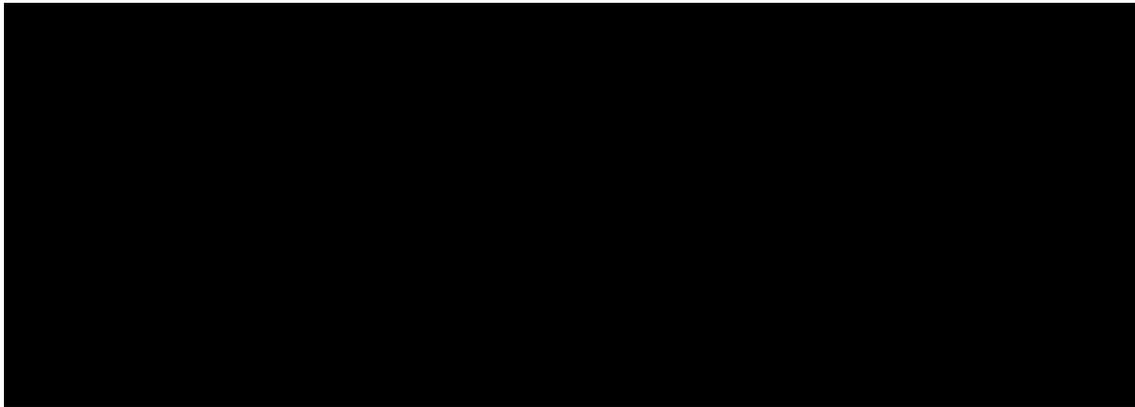
Ethernet Aggregation is a service that allows one hub, Network-to-Network Interface (NNI), to support multiple point-to-point Ethernet access circuits while maintaining logical separation of customer traffic. This service greatly reduces the number of physical Ethernet interfaces at the PE.

[REDACTED]



2.1.4.7.1.1 Point-to-Point Ethernet Service

Point-to-point Ethernet is a highly transparent service that connects user-network interfaces in two locations. This service does not allow for service multiplexing and does not require any coordination of VLANs or other detailed customer information. ■■■



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

Team MicroTech delivers all of the required access capabilities as defined in the RFP.

All of our teaming partners individually may not be able to provide all access arrangements, but our entire Team composition meets and complies with all RFP requirements as defined in Section C.2.9 of the Solicitation..

Integrated access to any protocol can be accomplished through hardware solutions appropriate to the service requirement. This is mainly done at the core of the network, but can also be done through the customer premise gear.

Depending on TO requirements, Transparency to any protocol can be accomplished through a series of solutions in the core of the network to translate or transcode to make the protocol agnostic and have the ability to communicate with one another. For IPVS services, Team MicroTech's contract can do this with time division multiplexing and session initiated protocol.

2.1.4.8 Technical Capabilities

Team MicroTech offers integrated access of different services that are transparent to any protocols.

Our access types are summarized below:

- T1.A line rate of 1.544 Mbps, which may be used to provide channelized or unchannelized T1 access arrangement as follows:
 - Channelized T1. In this mode, 24 separate DSOs clear channels of 56/64 kb/s
 - Unchannelized T1. In this mode, a single 1.536 Mbps
- ISDN PRI.
- ISDN BRI.
- T3. This category of a line rate of 44.736 Mbps, which may be used to provide channelized or unchannelized T3 access arrangement as follows:
 - Channelized T3. In this mode, 28 separate DS1 channels of 1.536 Mbps
 - Unchannelized T3. In this mode, a single 43.008 Mbps payload
- E1 (Non-domestic). This category of AA a line rate of 2.048 Mbps, which may be used to provide channelized or unchannelized E1service as follows:
 - Channelized E1.In this mode, 30 separate DSO clear channels
 - Unchannelized E1.In this mode, a single 1.92 Mbps information payload

- E3 (Non-domestic). support a line rate of 34.368 Mbps, which may be used to provide channelized or unchannelized E3 service as follows:
 - Channelized E3. In this mode, 16 separate E1 channels.
 - Unchannelized E3. In this mode, a single 30.72 Mbps information payload.
- DS0. Support information payload data rates of 56 kbps and 64 kbps.
- Digital Subscriber Line (DSL) Access Arrangements:
 - Provide the following types of DSL services, at a minimum:
- Asymmetric DSL (ADSL). Support ADSL asymmetric data rates for upstream and downstream traffic as follows:
 - Upstream: Data rates shall range from 16 to 768 kbps (e.g., 256 kbps).
 - Downstream: Data rates shall range from 1.5 Mbps to 8 Mbps (e.g., at 1.5, 2, 3, 4, 5, 6, 7, and 8 Mbps). Speeds up to 9 50 Mbps are optional.

█ [REDACTED]

- Symmetric DSL (SDSL). Support SDSL symmetric (i.e., same) data rates for both upstream and downstream traffic at data rates up to and including 1.5 Mbps. 2.3 Mbps is optional.

█ [REDACTED]

Ethernet Access Arrangements:

- a) Ethernet Access Arrangements shall support both dedicated access and/or shared access (multiplexed Ethernet connections) over a Metro Ethernet service from SDP to POP. The contractor shall support access speeds of:

- 1 Mbps to 10 Mbps at 1 Mbps increments
- 10 Mbps to 100 Mbps at 10 Mbps increments
- 100 Mbps to 1 Gbps at 100 Mbps increments
- (Optional) 2 Gbps to 10 Gbps at 1 Gbps increments
- (Optional) 10 Gbps to 100 Gbps at 10 Gbps increments

For each of the access connections, the contractor shall maintain appropriate committed bandwidth or CIR (Committed Information Rate), as supported by the MEF 33 - Ethernet Access Services standard and the MEF Bandwidth Profiles for Ethernet Services and as specified in the RFP.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] All Ethernet access arrangements follow the complete MEF guidelines for hardware and service including committed information rate (CIR) and an overall approach to the best of practices and standards

- SONET OC-3.
 - Channelized OC-3. In this mode, three separate OC-1 channels, each with an information payload data rate of 49.536 Mbps.
 - Concatenated OC-3c. In this mode, a single channel equivalent to information payload data rate of 148.608 Mbps.
- SONET OC-12.
 - Channelized OC-12. In this mode, 4 separate OC-3 channels, each with an information payload data rate of 148.608 Mbps.
 - Concatenated OC-12c. In this mode, a single channel equivalent to an information payload data rate of 594.432 Mbps.
- SONET OC-48.
 - Channelized OC-48. In this mode, 4 separate OC-12 channels, each with an information payload data rate of 594.432 Mbps.

- Concatenated OC-48c. In this mode, a single channel equivalent to an information payload data rate of 2.377728 Gbps.
- SONET OC-192.
 - Channelized OC-192. In this mode, 4 separate OC-48 channels, each with an information payload data rate of 2.488 Gbps.
 - Concatenated OC-192c. In this mode, a single channel equivalent to an information payload data rate of 9.510912 Gbps
- DS0. This category of AA will support information payload data rates of 56 kbps and 64 kbps.
- Optical Wavelength(s). Bi-Directional Wavelengths (WDM) connections to an optical network for the following speeds:
 - 1 Gbps
 - OC-48
 - OC-192
- Wireless Access Arrangements:
 - Cellular Service - 4G Long Term Evolution (LTE): 100 mbps (downstream) and 50 mbps (upstream)
 - Line of sight connection, using licensed frequencies:
 - DS1
 - NxDS1 (where N=2 through 27)
 - DS3
 - E1 (Non-domestic)
 - Nx E1 (where N=2 through 15) (Non-domestic)
 - E3 (Non-domestic)
 - SONET OC-3
 - 1 Gbps, 5 Gbps, and 10 Gbps

Team MicroTech supports Ethernet connectivity from speeds of 1Mbps to 10G for access arrangements. Our Partner's Ethernet access is MEF compliant.

2.1.4.9 Access Diversity and Avoidance

2.1.4.9.1 Access Route or Path Diversity

Team MicroTech's partner network provides a unique capability to supply at least two physically-separated routes for access diversity with the following options:

- Between an SDP and its associated connecting network's PCL or POP, or
- Between an SDP and at least two connecting network PCL/POPs.
- Access from the same or different access providers (e.g., ILEC and a CLEC) for two separate routes, using any mix of access arrangements.

This may require the alternative service providers to make sure there are separate paths and geographically diverse routes to the subject service. Team MicroTech designs and implements based on the above requirements to confirm with the contract guidelines.

These diverse routes meet the following requirements:

- Not share any common telecommunications facilities or offices including a common building entrance.
- Maintain a minimum separation of 30 feet throughout all diverse routes between premises/buildings where an SDP and its associated network connecting point are housed.
- Maintain a minimum vertical separation of two feet, with cables encased (separately) in steel or concrete for cable crossovers.

[REDACTED]

Team MicroTech provides the capability for the automatic switching of transmission in real-time, negotiated on an individual case basis:

- From the primary access route to the one or more diverse access routes, including satellite connection, and
- From the diverse access route to the primary access route.

The formation of a service level agreement (SLA) which includes the process and procedure of switching and diverting the traffic in the event of a service interruption and then back again to the primary route with secondary back up. [REDACTED]

[REDACTED]

[REDACTED]

Team MicroTech exercises the following control measures on the configuration or the reconfiguration of the diverse access route:

- Provide a graphical representation (e.g., diagrams, maps) of access circuit routes to show where diversity has been implemented to the OCO within 30 calendar days of the implementation of access diversity and again thereafter when a change is made.
- Prior to any proposed reconfiguration of routes previously configured for access diversity, the contractor shall provide to the agency written notification and revised PCLs for OCO approval in accordance with the requirements of the TO.

Team MicroTech adheres to and completes diagrams, network maps, overlay networks of access routes to show where diversity has been implemented to the OCO within the given time frame and the majority of the time these maps are built with the MOP and signed off on my subject customer and contractor. Any proposed reconfiguration or scheduled maintenance will be done with written notification to be compliant with subject contract. This includes all PCL's for OCO and in accordance with the requirements of the TO.

2.1.4.9.2 Access route or Path Avoidance

Team MicroTech supplies the capability for a customer to define a geographic location or route to avoid between an SDP and its associated connecting network point.

Our partners exercise the following control measures on the configuration or reconfiguration of the avoidance access route:

- The contractor shall provide a graphical representation (e.g., diagrams, maps) of access circuit routes to show where avoidance has been implemented to the OCO within 30 calendar days of the implementation of avoidance and again thereafter when a change is made.

- Prior to any proposed reconfiguration of routes previously configured for avoidance, the contractor shall provide to the agency written notification and revised PCLs for OCO approval in accordance with the requirements of the TO.

Team MicroTech adheres to and completes diagrams, network maps, overlay networks of access routes to show where diversity has been implemented to the OCO within the given time frame and the majority of the time these maps are built with the MOP and signed off on my subject customer and contractor. Any proposed reconfiguration or scheduled maintenance will be done with written notification to be compliant with subject contract. This includes all PCLs for OCO and in accordance with the requirements of the TO.

2.2 Optional EIS Services

MicroTech is not offering any optional services at this time. We anticipate increasing our service offerings post-award in order to leverage the full global scope of services Team MicroTech can provide.

2.3 Information Security

Team MicroTech has provided a complete Risk Management Framework plan (ref. Section 3.0) which addresses the delivery and security risk plans for EIS services.

Team MicroTech is not including the MTIPS optional managed service as part of our initial response. In the event Team MicroTech provide MTIPS services during the life of the contract, we will develop the MTIPS risk management framework plan to detail all connections, POPs, interfaces, and speeds.

2.3.1 System Security Requirements

Team MicroTech's Information System Security Officer (ISSO); or the Information System Security Manager (ISSM) provides quarterly and/or annually as updates regarding the security of the network services. Examples of specific reporting on the security of the EIS service include: specific traffic that has a variety of traffic that simulates malicious activity, actions such as spoofed IPs, VOIP data exfoliating efforts, and TCP 3 way handshakes that are of anomalous nature. Additionally, the SISO will provide the government customer (and OCO) monthly updated information on how government can access carriers system for audit, testing and evaluation

2.4 Traffic Identification and Routing Policy

[REDACTED]

[REDACTED] We will work to establish the use of high performance computing platforms as well as other scalable offerings to baseline traffic, disambiguate entities, and identify specific traffic for routing actions to assure delivery and reduce impact on bandwidth.

[REDACTED]

3 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 encryption 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.

Team MicroTech's Risk Management Framework Plan complies with the requirements of NIST SP 800-37, R1, Chapter 3, Sections 3.0 through 3.6, and is presented as Attachment A to Volume 1.

3.1 System Security Compliance Requirements

MicroTech and our team partners 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 will 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 April 2007.
- 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.

3.2 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 enterprise-wide information security for 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 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 minimum security requirements for “Moderate Impact Levels,” as specified under FedRAMP. We are prepared to provide 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 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.

3.3 Security Assessment and Authorization (Security A&A)

Team MicroTech’s carrier partners’ network information systems 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. Since application security is critical to the overall security of the system, Software applications, (such as database applications), and Web applications (hosted by an information system), are included in the Security A&A process. 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.

3.4 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 Publication 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 detailed accounting system security requirements. It describes the controls in place and the plan for meeting additional requirements. The SSP will also detail responsibilities and expected behavior of personnel who access the system. The documentation planning process provides adequate, cost-effective security protection for the system. The SSP reflects input from various managers with responsibilities concerning the system. These include 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 with which we interconnect on the EIS contract. The SSP includes all appendices and attachments related to each specific TO we are awarded on EIS.

3.5 System Security Plan Deliverables

Each TO specifies all required security deliverables. Following award, all required security documents are delivered to the Ordering Contracting Officer (OCO); the Information System Security Officer (ISSO); or the Information System Security Manager (ISSM). Our Team provides quarterly and/or annual updates, as required.

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.

3.6 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.

3.7 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 (NISPO), compiled May 2, 2014, or its latest revision. The NISPO 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.

MicroTech provides our draft Risk Management Framework Plan in **Appendix B**.

4 MTIPS RISK MANAGEMENT FRAMEWORK PLAN

MicroTech is not offering MTIPS Services, therefore we are not providing the MTIPS Risk Management Framework Plan.

APPENDIX A. ADDITIONAL MANDATORY ITEMS

Voluntary Product Accessibility Template

MicroTech posts our Voluntary Product Accessibility Template (VPATs) for each service identified in paragraphs C.4.4 to our web site, in order to demonstrate that offerings comply with Section 508 standards.

Section 508 Applicability to Technical Requirements

MicroTech services that execute mission operations meet the relevant provisions of Section 508, Subparts B, C, and D as identified in Section C.4.4, or we provide equivalent facilitation

Section 508 Provisions Applicable to Reporting and Training

- MicroTech reports required information via the Internet, email, or telephone. Our services providing the required information meet the relevant provisions of Section 508, Subparts B, C, and D, or we provide equivalent facilitation.
- MicroTech delivers training via meeting and briefings, classroom, seminars, instructor-led and non-instructor on-line web based self-study, and manuals or desk top guides.
- For training delivered via meeting and briefings, classroom, and seminars, MicroTech provides assistance such as signers and Braille products to disabled trainees when requested in advance by the government.
- For training delivered via instructor-led and non-instructor on-line web based, MicroTech provides the same capabilities for Internet reporting shall be provided to disabled trainees.

Section 508 Additional Information

Section 508 of the Rehabilitation Act of 1973 requires federal agencies to make their electronic IT accessible to people with disabilities. Section 508 compliance requires that the user interface to the service include informational attributes that can be parsed by automated reading software, such as JAWS or WAVE. Such interface attributes allow sight, hearing, speech, or motor-impaired individuals to access service capabilities via an alternate means appropriate for individuals with their disability. Team MicroTech has strong experience developing and testing applications to ensure 508 compliance. We have more than 10 years of experience using tools such as Watchfire Bobby and JAWS to ensure that software and websites meet Section 508 standards.

Approach to Section 508 Compliance

Team MicroTech’s approach for ensuring compliance with 508 accessibility standards is to use our extensive experience, toolsets, processes, and understanding of accessibility to design, develop, and retrofit to achieve compliant applications, products, and systems. As shown in **Figure A-1** our processes for assessing the EIS services provides the greatest degree of compliance with Section 508. [REDACTED]

[REDACTED]

[REDACTED]

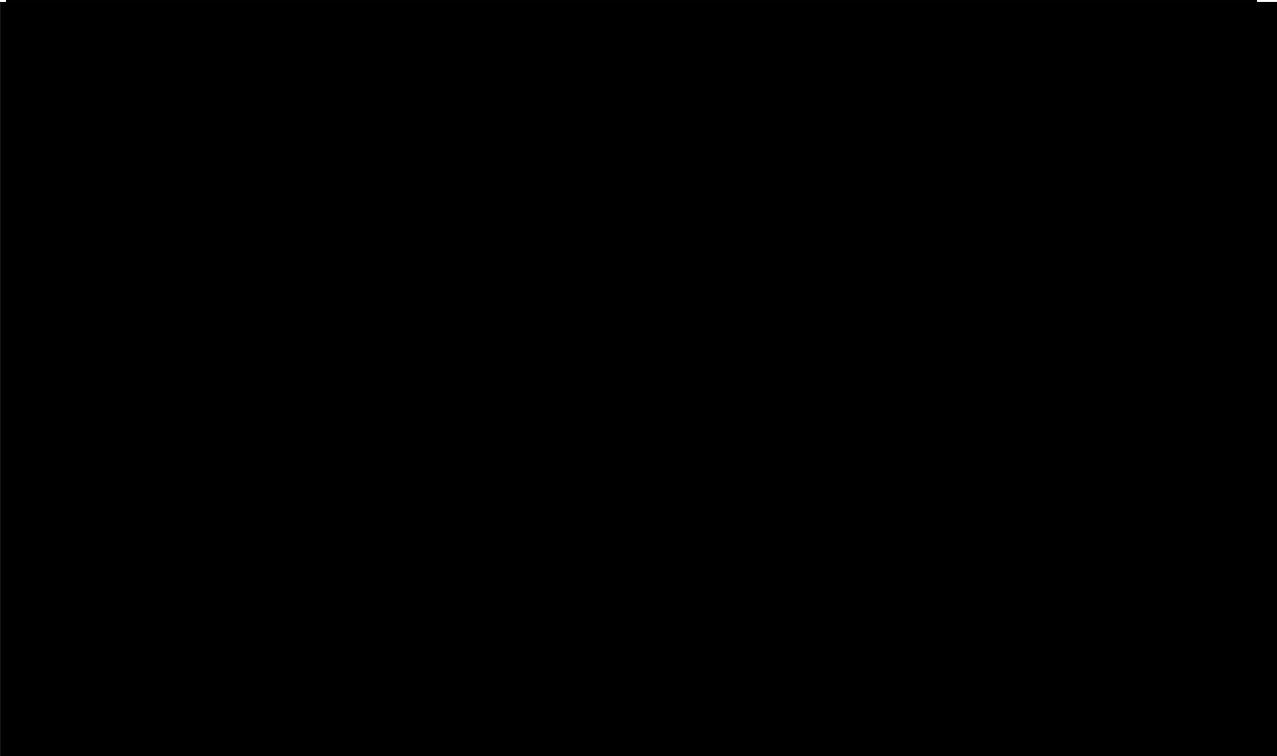
[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] These routine procedures validate where 508 compliance required.



Once internal 508 compliance testing on a product is complete, we coordinate with an independent auditor to schedule the formal 508 evaluation. By engaging the auditor during the development and test phase, we avoid non-compliance issues when moving the application to the deployment phase. Team MicroTech includes experienced developers and communications engineers adept at designing and maintaining Section 508 compliance. For COTS products and services, compliance personnel coordinate with partners to supply VPAT documentation. For products we develop, we follow the process show above and create a VPAT. All of these VPATs are made available on the Team MicroTech EIS website.

Team MicroTech's approach to Section 508 compliance is based on CMMI-best practices tailored to the phase and needs of the project. Key interfaces and opportunities where we demonstrate Section 508 compliance include:

- [Redacted]

[REDACTED]

[REDACTED]

[REDACTED]

In addition to the operation of the EIS program, our Program Manager understands the role of 508 compliance as it relates to program reporting and training. Our PM uses communications means that support 508 compliance and use report formats and templates from our ISO 9001:2008 Quality Management System (QMS) designed to ensure 508 compliance. We treat our training products, curriculum, and programs the same as any customer-facing service and apply the process show in **Figure A-1** to ensure MicroTech EIS customers achieve training outcomes in a manner suited to their abilities. For in-person training, Team MicroTech is prepared to provide other assistive capabilities such as Braille products or signers if requested.

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

APPENDIX B. DRAFT RISK MANAGEMENT FRAMEWORK PLAN

INTRODUCTION

The delivery of services to constituents of the United States Government, and within and among Federal Agencies is a massive undertaking. The use of Information Technology as a core foundational element of that service delivery cannot be understated. Among the most critical aspects of such service delivery is the comprehensive protection of information belonging to the Agency (internal data); information shared between Agencies to enable joint delivery of services (external data); and the vast repositories of constituent information (private data).

In a time when even the most secure data centers have experienced detrimental incursions on an unprecedented scale, a renewed imperative for the protection of Government Agency information has arisen. Traditional measures of security management such as Certification and Accreditation have given way to multi-layer, multi-step IT and network security architectures, specifically the six-step Risk Management Framework, which applies a combination of application-level-, subsystem-level, and system-level protections. Significant participation by Agency leadership is a hallmark of new approaches to security.

MicroTech has prepared this Risk Management Framework Plan (RMFP) in accordance with NIST Special Publication 800-37, augmented by NIST Special Publication 800-53, the Federal Information Security Management Act (FISMA), the Clinger-Cohen Act, OMB Circular A-130, and other relevant statutes and regulations. This RMFP addresses the steps required for the Plan sequentially for ease of presentation. However, it should be understood by the reviewer(s) that steps in the RMFP can be completed outside of the sequence outlined, to allow Government Agencies, Agency leadership, and IT and telecommunications contractors to design, develop, build, test, implement, and maintain the most critical information systems and subsystems in the Agency's technology portfolio.

1.0 RMF STEP 1 – [REDACTED]

1.1 TASK 1-1: [REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED]

Under the Federal Information Security Management Act of 2002 (FISMA), as detailed in FIPS Publication 199, Federal information systems are defined by three security objectives: *Confidentiality*, where: “A loss of confidentiality is the unauthorized disclosure of information”; *Integrity*, where: “A loss of integrity is the unauthorized modification or destruction of information”; and *Availability*, where: “A loss of availability is the disruption of access to or use of information or an information system.” This is further subdivided into levels of impact including *Low* (resulting in a limited adverse effect on organizational operations, organizational assets, or individuals; *Moderate* impact where: “The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.” The potential impact is *High* when “the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.”

The goal of the Risk Management Framework Plan is to evaluate and implement requisite security standards, regulations, and best practices to control access to and external impacts to Agency information systems. Systems are to be categorized by the level of access to the individual system or subsystem, and appropriate security controls are designed to prevent access by unauthorized users. Equally important are the boundaries established for the information system during the security categorization process. Restraining the information system boundaries helps to limit the complexity of the system architecture, and prevents overly complex risk management processes.

Each Agency operates under a Risk Management Strategy that is based on how they conduct their business, the level of system security required (up to and including Top Secret/SCI), and the accessibility to Agency information. The Risk Management Strategy is designed to provide not only protection to the Agency, but to give its executives appropriate guidance and authority to manage risk. Individual organizations have varying levels of risk tolerance, employ differing methods to evaluate risks, and may have unique ways of aggregating risks from internal and external systems.

[REDACTED]

[REDACTED] The goal is to design systems that meet the Agency's business and mission objectives. Under the Agency's system development life cycle, each component, subsystem, or new system will go through a rigorous process of requirements definition, including articulating the security requirements. Security controls are an imperative during system initiation. [REDACTED]

[REDACTED]

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

[REDACTED]

[REDACTED] At all times, MicroTech considers cost and security requirements. [REDACTED]

[REDACTED]

[REDACTED] When the requirements are fully documented, and the security environment has been rigorously tested, these activities are laid against the Agency's Risk Management Framework to ensure that the initial concept for the system/subsystem meets both architectural and security requirements.

[REDACTED]

[REDACTED] With this volume of information, MicroTech is prepared to evaluate the system's registration with Agency owners and managers. Again, all information is documented in the System Security Plan. If the volume of data is large, we will incorporate it as attachments to the plan.

1.3 TASK 1-3: [REDACTED]

[REDACTED]

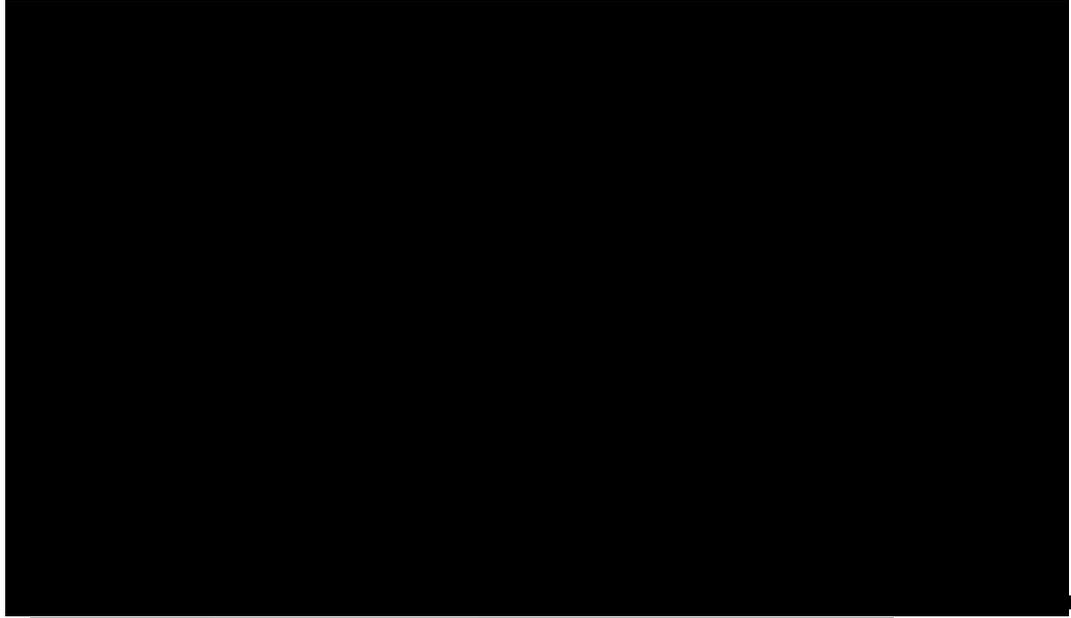
Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this document.

security status reports are required by and are prepared in accordance with applicable laws, directives, regulations, Executive Orders, policies, standards, and guidance.

[REDACTED]

[REDACTED] All documentation and recommendations are added to the Security Plan. **Figure B-1** shows the processes in Step One of the Risk Management Framework Plan.

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



2.0 RMF STEP 2— [redacted]

2.1 TASK 2-1: [redacted]

Formulating and documenting common security and system controls is important to managing the performance and security of the Agency's systems. Integral to the process of defining common controls are the CIO or the designated Senior Information Security Officer; the Information Security Architect; and the Common Control Provider, among other participants. These individuals have the authority and technical expertise to identify the intrinsic rules by which to classify the Agency's systems, and the level of security required by subsystem or system. In addition to common controls, many systems receive *inherited controls* from the Agency's overarching system security architecture. Common control providers can include system owners, whose knowledge of a specific system includes insight into security controls already embedded in the system.

Security experts and system owners may augment common security controls with system-specific controls and hybrid controls to bring the system's security to the standards established for the overall system security architecture. [redacted]

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

[REDACTED]

All variations of security controls are documented in a Security Plan at the system level, which rolls up to the Agency Security Architecture Plan. Ongoing development and implementation of common controls requires continued independent assessment to ensure that the controls are operationally effective in the Agency's business environment. Those found less than effective are inscribed in a Plan of Action and Milestones (POA&M) and revised until they meet Agency security standards. Common control providers are ultimately responsible for securing authorization for the common controls from the cognizant Agency official and for monitoring their ongoing effectiveness once placed in the system's security architecture.

When agencies share a system and information to jointly provide constituent services, the Agency that owns the system must promulgate the common security controls to the other Agency, and immediately inform the partner Agency of any potential risks that arise in the owning Agency's security posture. For this reason, agencies are encouraged, and in some instances, mandated, to use electronic security monitoring systems that maintain records regarding the common controls deployed in each Agency's information systems. In instances where systems are external to both agencies (i.e., provided by a third party, such as a telecommunications carrier), the agencies must ensure that the third-party security controls meet all of the Federal Government standards and regulations for those systems.

It is important that all Agency personnel understand the importance of the system security planning process. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] We participate in system testing, or directly do the system testing on behalf of the Agency, to ensure that no issues discovered during testing are allowed into the information system once it goes live.

2.2 TASK 2-2: [REDACTED]

Agencies depend on an established security baseline from which all other elements of system security are built. [REDACTED]

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

[REDACTED]

[REDACTED] Should the Agency determine to replace an aging system, we will work with them to define the “look, feel, and operation” of the new system environment. If the Agency desires a design that is net-centric, we will evaluate security products and software that operate successfully in an environment with dynamic subsystems. [REDACTED]

[REDACTED]

[REDACTED] MicroTech documents all security common control recommendations in the overarching system Security Plan. Our activities will be governed by *NIST SP 800-37, Section 3.2, Select Security*

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

Controls, which specifies that security controls must be selected based on the security categorization of the information system. It includes establishing a security control baseline, and requires that the Agency organization apply a tailoring process to align security controls with conditions in the organization, as detailed in the paragraph above.

2.3 TASK 2-3: [REDACTED]

[REDACTED]

[REDACTED] as detailed in *NIST SP 800-137, Information Security Monitoring for Federal Information Systems and Organizations*. A vigorous continuous monitoring program ensures that an organization will be aware of the security state of its information systems. In turn, this enables it to counter threats, incursions, and vulnerabilities. Similarly, maintaining the organization's business systems in a sound security posture will allow the Agency to carry out its mission.

[REDACTED]

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

[REDACTED]

[REDACTED]

3.0 RMF STEP 3— [REDACTED]

3.1 TASK 3-1: [REDACTED]

Implementing security controls within the organization requires best practices to ensure that controls are allocated appropriately to individual subsystems and systems. [REDACTED]

[REDACTED]

[REDACTED] as recommended in NIST SP 800-36. [REDACTED]

[REDACTED]

As we implement the security controls, we will ensure that all Federal policies and regulations, including FIPS Pub 200 are met. [REDACTED]

[REDACTED]

3.2 TASK 3-2: [REDACTED]

[REDACTED]

Applying best practices to documenting the implementation of the security controls and the hardware and software of the security architecture is critical to managing the information system environment over its life cycle. [REDACTED]

[REDACTED] We include the functional description as part of the system documentation in the Security Plan. This information set comprises descriptions of common controls, hybrid controls, and system-specific controls. The use of security controls from NIST SP 800-53A (including the baseline controls as a starting point in the control selection process), enables a consistent level of security for federal information systems and organizations. In the same manner, the guidance of NIST SP 800-53A provides the flexibility and agility the Agency needs to address an increasingly sophisticated and hostile threat space; specific organizational missions/business functions; persistently changing technologies; and in some cases, unique operational environments.

Also included in the system security documentation is information about system components (e.g., hardware, software, and firmware) from vendors whose products are part of the security solution. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Working with the Agency's Senior Security Specialist and technical staff, [REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED]

4.0 RMF STEP 4— [REDACTED]

4.1 TASK 4-1: [REDACTED]

[REDACTED]

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

[REDACTED]

Under the guidance prescribed in NIST SP 800-53A, [REDACTED]

[REDACTED]

[REDACTED] Once the plan is completed, we will present it to the Senior Information Security Officer, the CIO, and system owner for review and approval.

[REDACTED]

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

[REDACTED]

MicroTech has the expertise in software, hardware, and systems engineering, and in security best practices to develop the Security Controls Assessment Plan. We bring the independence necessary to prepare the plan and conduct system security assessments using state-of-the-art methods, concepts, and automated tools to conduct the level of security assessment required. Our approach supports the concepts of continuous monitoring and near-real-time risk management, and is cost-effective. An approved Security Controls Assessment Plan will ensure that the appropriate resources are applied to determining security control effectiveness.

4.2 TASK 4-2: [REDACTED]

[REDACTED]

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

[Redacted text block]

4.3 TASK 4-3: [Redacted]

[Redacted text block]

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

[REDACTED]

4.4 TASK 4-4: [REDACTED]

Once the Security System Assessment Report is completed, it is presented to top Agency officials for review and recommended action. [REDACTED]

[REDACTED]

[REDACTED] These will be categorized by the type of threat or vulnerability, and prioritized for corrective action. Those representing the highest probability of exploitation will be immediately addressed. Others may be considered very low risk, or not severe enough to warrant immediate correction.

Weaknesses with potential adverse impact on organizational operations and assets, individuals, other organizations, or the Nation will warrant further investigation and remediation. [REDACTED]

[REDACTED]

[Redacted content]

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



5.0 RMF STEP 5— [REDACTED]

5.1 TASK 5-1: [REDACTED]

The system owner will prepare a Plan of Action and Milestones (POA&M) in accordance with OMB Memorandum M-02-0, *Guidance for Preparing and Submitting Security Plans of Action and Milestones*, dated 17 October 2001, for the Authorizing Official. The POA&M “provides a roadmap for continuous agency security improvement, assists with prioritizing corrective action and resource allocation, and is a valuable management and oversight tool for agency officials, Inspectors General, and OMB.” [REDACTED]

[REDACTED]

■ [REDACTED]

[REDACTED]

■ [REDACTED]

■ [REDACTED]

■ [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED]

The complete Security Authorization Package is comprised of the Security Plan; the Security Assessment Report; and the Plan of Action and Milestones (POA&M). These documents allow the Authorizing Officials to make risk-based decisions regarding the security posture of the information system. In addition, the Security Authorization Package may contain documentation related to systems that will inherit common controls for specific security capabilities. Should security controls be provided by an external entity (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), provider information for Authorizing Officials making risk-based decisions is included. Other information requested by the Authorizing Official can be added to the Security Authorization Package.

The information in the Security Authorization Package is protected by Federal and Agency policies and regulations. The use of automated tools to prepare and maintain the content of the package provides an effective way to maintain and update information and status of the Agency's system security information for Authorizing Officials. Regular and timely updates to the Security Authorization Package support near-real-time risk management, ongoing authorization, and more cost-effective reauthorizations if necessary. Version control is critical and can be achieved with the automated tools, and gives the Agency's leadership insight into the status of security in the information system.

MicroTech personnel, at the Agency's direction, will help prepare the Security Authorization Package. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

This plan draws on the components of risk management, as specified in Chapter 2, Section 2.1 of *NIST SP 800-39, Managing Information System Risk*; and on Chapter 3, Task 2, Subtask 2.2, *Risk Determination*. [REDACTED]

[REDACTED] Agencies can respond to identified risks in different ways, including:

- Accepting risk
- Avoiding risk
- Mitigating risk
- Sharing risk
- Transferring risk
- A combination of the above.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

MicroTech is aware that threat and vulnerability determinations apply to missions and business functions; and that specific requirements associated with the missions/business functions, including operational environments, may lead to different risk determination results. Such differences in missions, business functions, and operating environs can lead to differences in the applicability of threat information. It can ultimately result in threats causing substantial harm. Understanding the threat component of the risk assessment requires insight into the particular threats facing

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

[Redacted text block]

5.2 TASK 5-2: [Redacted text]

[Redacted text block]

[Redacted text block]

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

[REDACTED]

[REDACTED]

6.0 RMF STEP 6— [REDACTED]

6.1 TASK 6-1: [REDACTED]

[REDACTED]

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

[REDACTED]

6.2 TASK 6-2: [REDACTED]

Following the security authorization of the information system, and during continuous monitoring, the Agency regularly assesses the system's security controls. The information system owner and/or common control provider determine the frequency of monitoring the system's operational, technical, and management controls. [REDACTED]

[REDACTED]

[REDACTED] in accordance with NIST SP 800-53A and SP 800-137.

[REDACTED]

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

6.3 TASK 6-3: [REDACTED]

6.4 TASK 6-4: [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

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

[Redacted content]

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

[Redacted text block]

6.6 TASK 6-6: [Redacted text]

[Redacted text block]

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

