Granite Telecommunications, LLC.
100 Newport Ave. Ext.
Quincy, MA 02171

VOLUME II

Management Volume

This proposal or quotation 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 or quoter 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. The data subject to this restriction are contained in sheets marked with the following legend:
"Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal or quotation"

FPR 16:GT-RMG-1440 Rev. 1 **30 MAR 2017**

Solicitation Number QTA0015THA3003

GSA

EIS

TABLE OF CONTENTS

1.0 - OVERVIEW

This proposal volume provides Granite's application of its industry-leading commercial support systems to the EIS model. Granite provides unmatched customer support; including its established single point of contact "Premier" program management model and Granite's Helpdesk, a trained in-house customer service team that is available 24/7/365. Granite's Premier program management model has been a keystone commercial practice for over a decade and virtually seamlessly fits the requirements of EIS. Granite's Premier program is designed to provide a dedicated Premier Account Manager who will work with the customer as their single point of contact on any and all matters for the duration of the contract. Granite is applying this model to its management and support approach to EIS. Allowing Granite to comply with the BSS requirements is Granite's internally developed, customer support system and user-friendly customer service portal "Rock Reports". Granite is electronically bonded to its customers and underlying carriers, allowing for streamlined communication, accurate billing, customized reporting, and efficient repair/trouble ticketing. Granite's team of Electronic Data

Interchange (EDI) experts are able to customize systems to optimize performance for government customers under EIS.

In addition, Granite provides transparent, proactive support rather than the reactive, out of touch support provided by most service providers. Similarly, Granite’s Helpdesk has been designed with the customer’s needs in mind. Unlike the arduous touch tone menus, extended hold times, and off-shore call centers of other carriers, a member of Granite’s customer service team will answer the phone on average in less than ten (10) seconds.

2.0 - CONTRACT ADMINISTRATION

[redacted]

[redacted]

2.1 - TASK ORDER CONTRACT ADMINISTRATION

[redacted]

2.1.1 - Task Order Data – [redacted]

[redacted]

[redacted]

c. [redacted]

[redacted]

[redacted]

3.0 - ORDERING

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3.1 - TELECOMMUNICATIONS SERVICE PRIORITY (TSP)

[redacted]

[redacted]

[redacted]

[redacted] 2-1:

[redacted]

:

[redacted]

3.2 – EXPEDITED SERVICE

[redacted]

[redacted]

[redacted]

[redacted]

3.3 – RAPID PROVISIONING

[redacted]

3.4 – DATA INTERACTION REQUIREMENTS

3.4.1 – Common Operational Requirements

3.4.1.1 - Agency Hierarchy Code (AHC) – [redacted]

[redacted]

3.4.1.2 - Unique Billing Identifier (UBI) – [redacted]

3.4.1.3 - Agency Service Request Number (ASRN) – [redacted]

3.4.1.4 - Contract Line Item Number (CLIN) – [redacted]

3.4.1.5 - Ordering Data Sets – [redacted]

[redacted]

8) Service [redacted]

[redacted]

[redacted]

[redacted]

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

3.4.1.6 - Auto-Sold CLINs – [redacted]

[redacted]

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

[redacted]

[redacted]

- [redacted]
- [redacted]

3.4.2 – Ordering Process:

[redacted]

TABLE 2-2:

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

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

3.4.2.1 – eBuy:

[redacted]

3.4.3 – Protests and FOIA requests:

Granite confirms it understands the requirements and will comply with the terms and conditions of RFP Section G.3.2.3 and G.3.2.3.1.

3.5 – AUTHORIZATION OF ORDERS

Granite will comply with all the terms and conditions of RFP Section G.3.2.5. [redacted]

3.6 – AUTO-SOLD CLINS

Granite will comply with the terms and conditions of RFP Section G.3.3.1.2, Auto-Sold CLINs. [redacted]

3.7 – DISCONNECTION AND CANCELLATION

3.7.1 – Disconnect Orders

Granite will comply with all the terms and conditions of Section G.3.3.2.2.3. [redacted]

3.7.2 – Cancel Orders

Granite will comply with all the terms and conditions of Section G.3.3.2.3.1. [redacted]

[redacted]

[redacted]

[redacted]

4.0 - BILLING

Granite will comply with all requirements as stated in the RFP Section G.4 and J.2.5, [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4.1 – DATA INTERACTION REQUIREMENTS

[redacted].

4.2 - BILLING DISPUTES:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted].

[redacted]

4.2.1 – Data Interaction Requirements related to Disputes

[redacted]

4.2.1.1 - Common Operational Requirements

In accordance with Section J.2.6.1, Granite confirms that the dispute process shall apply under any of the following conditions:

1) The government disputes the contents of a BI submitted by Granite
2) The government disputes the content of an Inventory Reconciliation (IR) submitted by Granite.
3) The government disputes an SLA Credit Request Response submitted by Granite.

4.2.1.2 - Dispute Process

In accordance with Section J.2.6.2, Granite confirms that it shall deliver all deliverables and other data sets included in the dispute process below are defined in Section J.2.6.3, to both the customer and to GSA:

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

4.2.1.3 - Deliverables and Data Exchange

In accordance with Section J.2.6.3, Granite confirms that it shall comply with the deliverables and data exchange requirements as set forth by the government and the detailed contents of such data sets, as set forth in Section J.2.10.2. For each data set, Granite shall support all required transfer mechanisms as defined in Section J.2.9.

4.3 – Billing Requirements

4.3.1 – Billing Start Date and End Date

Granite will comply with all the terms and conditions of RFP Section G.4.1.2. Under each TO, the SOCN date for installation will become the billing start date. The SOCN date for disconnection will service as the billing end date. In accordance with G.4.1.2, unless otherwise specified in the TO, the NRC price billed will be that which was in effect at the time the service order was placed, and the MRC shall be that which was in effect for the billing month. Granite will begin billing both the NRC and MRC on the billing start date unless the exceptions specified in G.4.1.2 apply.

4.3.2 – Ninety (90) Day Billing Requirement

In accordance with RFP Section G.4.1.3, Granite will submit a proper BI deliverable pursuant to Section J.2.5, for all services and SREs up to 90 days after the issuance of the SOCN.

4.3.3 – Central and Direct Billing Requirements

Granite confirms it will accept both billing methods and will comply with the terms and conditions of RFP Sections G.4.2.1 and G.4.2.2. Granite will deliver billing to GSA for all charges incurred by all central-billed agencies. For TOs that specify the direct-billing method, Granite will bill the agency directly for all charges incurred by the agency and its sub-agencies.

4.3.4 – Associated Government Fee (AGF)

Granite will comply with the terms and conditions in Section G.4.6 and collect the AGF from customer agencies on a monthly basis throughout the life of the contract. The total amount of AGF collected for each month shall be remitted to GSA via EFT no later than the 15th business day of the following month. As required by Section G.4.9, Granite will round billing and AGF in accordance with Section J.2.5.1.6.

4.3.5 – Government Purchase Card (GPC)

In accordance with Section G.4.8, Granite will accept payment via GPC when authorized by the Government. [redacted]

4.3.6 – Proration of Charges

As required by Section G.4.10, Granite will prorate billing based on the number of days that the service is provided during the billing period in accordance with Section J.2.5.1.5. Granite will support both Month-Length Proration, as defined in Section J.2.5.1.5.1.1, and Normalized 30-day Month Proration, as defined in Section J.2.5.1.5.1.2. Granite will indicate the proposed proration type in its response to each customer agency solicitation.

4.3.7 – Taxes, Fees and Surcharges

Granite will comply with all the terms and conditions of RFP Section G.4.11; Taxes, Fees and Surcharges. In accordance with G.4.11.1, Granite will charge separate amounts for taxes, fees and surcharges; providing the charges as separate components on the BI, whether they are part of an original charge or adjustment. If an agency requests and Granite proposes prices that include taxes, fees and surcharges in the solicitation and proposal, Granite will bill the prices that were proposed, accepted and included in the TO. In accordance with Section G.4.11.2, Granite will include the aggregated tax for each line item in the billing invoice and shall also provide the detailed composition of the aggregated tax in the tax detail deliverable required by Section J.2.5.1.7.

4.3.8 – Billing Performance Objectives

In accordance with RFP Section G.4.12, Granite will submit accurate billing that meets the following performance objectives:

- All applicable data elements will be included on the BI in accordance with Section J.2.10.
- The BI will have an associated SOCN for each order.
- The information on the BI will be consistent with that on the SOCN.
- The BI will contain no duplicate records.
- For both initial invoicing and all billing adjustments, there will be no records within the BI that represent charges being billed more than 90 days after the issuance of the SOCN unless waived as described in Section G.4.1.3.
- The prices on the BI will match the prices on the contract or TO.

5.0 - BUSINESS SUPPORT SYSTEMS

In accordance with RFP Section G.5.1, Granite shall have and maintain Business Support Systems (BSS). Granite will comply with RFP Section G.5 as the primary applications that will be utilized to support the BSS requirements are owned, maintained, and administered by Granite. As such, Granite has the ability to customize a module to satisfy the specific BSS requirements, and will do so as required.

[redacted]

[redacted]

[redacted]

5.1.1 - Web Interface Functions

[redacted]

[redacted]

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

[redacted]

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

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

5.1.2 - Technology Standards

[redacted].

5.1.3 - Accessibility

In accordance with Section G.5.3.1.3, Granite shall have readily available a comprehensive list of all offered EIT products that fully comply with Section 508 of the Rehabilitation Act of 1973, per the 1998 Amendments, and the Architectural and Transportation Barriers Compliance Board's Electronic and Information Technology Accessibility Standards at 36 CFR 1194. The [redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

5.2 - DIRECT DATA EXCHANGE

Granite shall comply with the requirements included in the table in Section G.5.4.1 and will provide a secure automated mechanism for direct transfer of data such as order submittal, administration and reporting to the GSA Conexus.

5.2.1 - Direct Data Exchange Methods

In compliance with Section G.5.3.2.1, Granite will maintain a separate SFTP service for the GSA and other government customers to ensure security of transactions. In addition Granite shall comply with the standards of Simple Object Access Protocol (SOAP). As mentioned in Section J.2.9, Granite shall support all the data transfer mechanisms called out in the table J.2.8.3.2 primarily around email and SFTP. Granite shall work the CO of the TO if another data transfer mechanism is required.

5.2.2 - Direct Data Exchange Formats

Granite shall comply with the specific requested formats specified in Section J.2.9.

5.2.3 - Direct Data Exchange Governance

Granite shall establish a governance process with the GSA and other government customers in accordance with Section G.5.3.2.3 and will comply with requested BSS change control process.

5.3 - ROLE BASED ACCESS CONTROL (RBAC)

Granite shall comply with the RBAC request to allow only authorized users with appropriate access permissions to its BSS in accordance with Section J.2.3.1.2. New users will be added within the requested timeline, and users will be removed within 1 business day of notification (or sooner if required), also noted in Section J.2.3.1.2.

5.4 - DATA DETAIL LEVEL

Please refer to 5. 1.1, where Granite overviews its web capabilities. The requirements for the data detail level are all inherently built into the system for ease of use from a human machine perspective. In accordance with RFP Section G.5.3.4, the data provided by the BSS shall be sufficiently detailed to provide all data elements relating to the services listed in Section G.5.4, BSS Component Service Requirements as addressed in Section J.2.

5.5 - BSS COMPONENT SERVICE REQUIREMENTS

Granite shall comply with the table functionality as laid out in Section G.5.4.1 and detailed in Table 2-3 below.

TABLE 2-3:

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

In accordance with Table 2-3 above, Granite shall provide the following services:

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

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

5.6 - BSS DEVELOPMENT

In accordance with section G.5.5, the BSS Development and Implementation Plan is included at Figure 2-4

FIGURE 2-4:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

____

5.6.1 - BSS Change Control

In accordance with Section G.5.5.1, Granite shall provide a BSS Change Control Notification to the government at least 30 days prior to all BSS changes regardless of their impact. In the event of an emergency change, Granite shall notify the government as soon as it discovers that a change is required.

Additionally, for those changes that meet the standard for being subject to change control, Granite shall 1) Obtain Government approval before implementing the change, 2) Use industry-standard change control procedures, 3) Train Government personnel if required, 4) Retest with the Government to ensure functionality continues to meet requirements, 5) Update all relevant documents and information posted on Granite's website as necessary, at no additional cost to the Government and within seven (7) days of completing the change.

Granite shall comply with Section G.5.5.1 and commit to provide notice to the Government at least 30 days in advance to all BSS changes regardless of impact. Granite understands that there may be scenarios where the GSA rejects such enhancements. In the event such upgrades or application enhancements are rejected, the noted upgrade or enhancement will not be added to the module that supports the GSA.

5.7 - BSS SECURITY REQUIREMENTS

Granite shall comply and will allow the Government to audit these efforts to ensure Granite is maintaining and adhering to an up to date BSS System Security Plan.

5.7.1 - General Security Compliance Requirements

In accordance with section G.5.6.1 General Security Compliance Requirements, Granite shall comply with the specific security directives and standards noted in the section and all associated links and publications.

Pursuant to the above section, Granite shall comply with Federal Information Security Management Act (FISMA) guidance and directives to include Federal Information Processing Standards (FIPS), National Institute of Standards and Technology (NIST) Special Publication (SP) 800 series guidelines (see http://csrc.nist.gov/), GSA IT security directives, policies and guides, and other appropriate government-wide laws and regulations for protection and security of government IT.

In addition, Granite shall comply with the current GSA policies, directives and guides listed in the corresponding section of the RFP. Granite shall submit a request for all these current documents via the GSA CO.

5.7.2 - GSA Security Compliance Requirements

In accordance with Section G.5.6.2 GSA Security Requirements, the noted document requested in this section has been included as an appendix:

- BSS Risk Management Framework Plan: Appendix 2G

5.7.3 - Security Assessment and Authorization (Security A&A)

Granite shall comply and complete the formal approval process prior to the award of any TO's. In addition, Granite shall have a new Security Assessment & Authorization conducted every three years.

5.7.4 - BSS System Security Plan (BSS SSP)

Granite shall fully comply with all terms and conditions of RFP Section G.5.6.4. Granite shall complete a formal BSS System Security Plan (BSS SSP) prior to the award of any TOs.   The BSS SSP shall be completed in accordance with NIST SP 800-18, Rev 1 and other relevant guidelines. Granite shall ensure the BSS SSP for the information system will be completed and submitted within 30 days of the NTP to include annual updates.

5.7.4.1 – Security Assessment and Boundary Scope Document (BSD) – To determine the actual security assessment boundary, Granite shall develop and maintain a BSD as identified in NIST SP 800-37. The BSD for the information system shall initially be completed and submitted within 15 days of the NTP to include annual updates.

5.7.4.2 – Interconnection Security Agreements (ISA) – Granite will develop and maintain ISAs in accordance with NIST SP 800-47. Granite will provide and ISAs for the information system with the initial security A&A package to include annual updates.

5.7.4.3 – Control Tailoring Workbook (CTW) – Granite will develop and maintain a GSA NIST SP 800-53 R4 Control Tailoring Workbook (CTW) as identified in GSA IT Procedural Guide 06-30. Column E of said workbook titled "Contractor Implemented Settings" will document all Granite-implemented settings that are different from GSA-defined settings, and where GSA-defined settings allow Granite to deviate. Granite will provide a CTW for the information system with the initial security A&A package to include annual updates.

5.7.4.4 – Control Summary Table – Granite will develop and maintain a GSA Control Summary Table for a Moderate Impact Baseline as identified in GSA IT Security Procedural Guide 06-30 “Managing Enterprise Risk”. Granite will provide a GSA NIST SP 800-53 R4 Control Summary Table for the information system with the initial security A&A package to include annual updates.

5.7.4.5 – Rules of Behavior (RoB) - Granite will develop and maintain a Rules of Behavior (RoB) for information system users as identified in GSA IT Security Procedural Guide 06-30 “Managing Enterprise Risk” and GSA Order CIO 2104.1. Granite will provide a RoB for the information system with the initial security A&A package to include annual updates.

5.7.4.6 – System Inventory - Granite will develop and maintain a System Inventory that includes hardware, software and related information as identified in GSA IT Security Procedural Guide 06-30 “Managing Enterprise Risk”. Granite will provide a System Inventory for the information system with the initial security A&A package to include annual updates.

5.7.4.7 – Contingency Plan (CP) – Granite will develop and maintain a Contingency Plan (CP) including Disaster Recovery Plan (DRP) and Business Impact Assessment (BIA) completed in agreement with NIST SP 800-34. Granite will provide a CP, DRP, and BIA for the information system with the initial security A&A package to include annual updates.

5.7.4.8 – Contingency Plan Test Plan (CPTP) - Granite will develop and maintain a Contingency Plan Test Plan (CPTP) completed in agreement with GSA IT Security Procedural Guide 06-29 “Contingency Planning Guide”. Granite will provide a CPTP for the information system with the initial security A&A package to include annual updates.

5.7.4.9 - Contingency Plan Test Report (CPTR) - Granite will test the CP and document the results in the Contingency Plan Test Report (CPTR), in agreement with GSA IT Security Procedural Guide 06-29 "Contingency Planning Guide". Granite will provide a CPTR for the information system with the initial security A&A package to include annual updates.

5.7.4.10 – Privacy Impact Assessment (PIA) – Granite shall perform a Privacy Impact Assessment (PIA) completed as identified in GSA IT Procedural Guide 06-30, "Managing Enterprise Risk". Granite will provide a PIA for the information system with the initial security A&A package to include annual updates.

5.7.4.11 – Configuration Management Plan (CMP) - Granite will develop and maintain a Configuration Management Plan (CMP) (Reference: NIST SP 800-53 R4 control CM-9; NIST SP 800-128; GSA CIO-IT Security 01-05). Granite will provide a CMP for the information system with the initial security A&A package to include annual updates.

5.7.4.12 – System Baseline Configuration Standard Document – Granite will develop and maintain a System(s) Baseline Configuration Standard Document (Reference: NIST SP 800-53 R4 control CM-2; NIST SP 800-128; GSA CIO-IT Security 01-05). Granite confirms it will provide a well-defined, documented, and up-to-date specification to which the information system is built. Granite will provide the System Baseline Configuration for the information system as part of the CMP and shall be submitted with the initial security A&A package to include annual updates.

5.7.4.13 – System Configuration Settings - Granite will develop and maintain System Configuration Settings (Reference: NIST SP 800-53 R4 control CM-6; NIST SP 800-128; GSA CIO-IT Security 01-05). Granite will establish and document mandatory configuration settings for information technology products employed within the information system that reflect the most restrictive mode consistent with operational requirements. Granite will configure settings in accordance with GSA technical guides, NIST Standards, Center for Internet Security (CIS) guidelines (Level 1), or industry best practices in hardening systems , as deemed appropriate by the AO. System Configuration Settings shall be included as part of the CMP and will be updated and/or reviewed on an annual basis.

5.7.4.14 – Incident Response Plan (IRP) - Granite will develop and maintain an Incident Response Plan (IRP) (Reference: NIST SP 800-53 R4 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02). Granite will provide an IRP for the information system with the initial security A&A package to include annual updates.

5.7.4.15 – Incident Response Test Report (IRTR) - Granite will test the IRP and document the results in an Incident Response Test Report (IRTR) (Reference: NIST SP 800-53 R4 control IR-8; NIST SP 800-61; GSA CIO-IT Security 01-02). Granite will provide an IRTR for the information system with the initial security A&A package to include annual updates.

5.7.4.16 – Continuous Monitoring Plan – Granite will develop and maintain a Continuous Monitoring Plan to document how continuous monitoring of the information system will be accomplished. Granite will provide a Continuous Monitoring Plan for the information system with the initial security A&A package to include annual updates.

5.7.4.17 – Plan of Action and Milestones (POA&M) - Granite will develop and maintain a POA&M in accordance with GSA IT Security Procedural Guide 06-30. All scans associated with the POA&M will be performed as an authenticated user with elevated privileges. Vulnerability scanning results will be managed and mitigated in the POA&M and submitted together with the quarterly POA&M submission. Scans shall include all networking components that fall within the security accreditation boundary. The appropriate scans are also submitted with the initial security A&A package and an annual information system User Certification / Authorization Review will be annotated on the

POA&M. Granite will provide the POA&M for the information system with the initial security A&A package followed by quarterly updates.

5.7.4.18 – Penetration Test – All FIPS 199 Low, Moderate, and High Impact information systems will complete an independent internal and external penetration test and provide an Independent Penetration Test Report on an annual basis in accordance with GSA CIO-IT Security Guide 11-51. The tests will be coordinated through the GSA Office of the Chief Information Security Officer (OSISO) Security Engineering Division.

5.7.4.19 – Code Analysis Reviews - All FIPS 199 Low, Moderate, and High Impact information systems will conduct code analysis reviews in accordance with GSA CIO Security Procedural Guide 12-66. Results will be documented in a Code Review Report. If applicable, a Code Review Report will be submitted as an initial deliverable prior to placing the information system into production, when there are changes to code on an annual basis.

5.7.4.20 – Security/Risk Assessment and Penetration Tests – Granite will allow GSA employees (or GSA-designated third party contractors) to conduct security A&A activities to include control reviews in accordance with NIST SP 800-53 R4 / NIST SP 800 53A R4 and GSA IT Security Procedural Guide 06-30.

5.7.4.21 – Security Risk Assessment Report (SAR) – All identified gaps between required 800-53 R4 controls and Granite's implementation as documented in the SAR will be tracked by Granite for mitigation in a POA&M document completed in accordance with GSA IT Security Procedural Guide 09-44.

5.7.4.22 – Security Risks – Granite will mitigate all security risks found during the security A&A and continuous monitoring activities. All critical and high-risk vulnerabilities will be mitigated within 30 days and moderate risks will be mitigated within 90 days from the date the vulnerabilities are identified, Granite will provide updates on a monthly basis on the status of all critical and high vulnerabilities that have not been closed within 30 days.

5.7.4.24 – FISMA Assessment – Granite will deliver the results of the annual FISMA assessment conducted per GSA CIO IT Security Procedural Guide 04-26.

5.7.4.23 – Policy and Procedure Documents – Granite will develop and keep current all policy and procedure documents. The following documents will be verified and reviewed during the initial security assessment and updates provided to the GSA COR/ISSO/ISSM biennially:

a. Access Control Policy and Procedures (NIST SP 800-53 R4: AC-1).
b. Security Awareness and Training Policy and Procedures (NIST SP 800-53 R4: AT-1).
c. Audit and Accountability Policy and Procedures (NIST SP 800-53 R4: AU-1).
d. Security Assessment and Authorization Policies and Procedures (NIST SP 800-53 R4: CA-1).
e. Configuration and Management Policy and Procedures (NIST SP 800-53 R4: CM-1).
f. Contingency Planning Policy and Procedures (NIST SP 800-53 R4: CP-1).
g. Identification and Authentication Policy and Procedures (NIST SP 800-53 R4: IA-1).
h. Incident Response Policy and Procedures (NIST SP 800-53 R4: IR-1).
i. System Maintenance Policy and Procedures (NIST SP 800-53 R4: MA-1).
j. Media Protection Policy and Procedures (NIST SP 800-53 R4: MP-1).
k. Physical and Environmental Policy and Procedures (NIST SP 800-53 R4: PE-1).
l. Security Planning Policy and Procedures (NIST SP 800-53 R4: PL-1).
m. Personnel Security Policy and Procedures (NIST SP 800-53 R4: PS-1).
n. Risk Assessment Policy and Procedures (NISTSP 800-53 R4: RA-1).
o. Systems and Services Acquisition Policy and Procedures (NIST SP 800-53 R4: SA-1).

p. System and Communication Protection Policy and Procedures (NIST SP 800-53 R4: SC-1).

q. System and Information Integrity Policy and Procedures (NIST SP 800-53 R4: SI-1).

5.7.5 - Additional Security Requirements

Granite will fully comply with all terms and conditions set forth in RFP Section G.5.6.6. Granite will ensure that proper privacy and security safeguards are adhered to in accordance with FAR Part 52.239-1. Granite shall house all GSA data separately and where appropriate, Granite will ensure the implementation of FAR requirements (see Section I, 52.224-1 and 52.224-2). Granite understands that the GSA data is confidential and will not provide this information to outside sources. Further, Granite will operate in good faith in defining non-disclosure agreements that other third parties must sign when acting as the federal government’s agent.

5.7.5.1 – Controlled Unclassified Information (CUI) – The deliverables identified in RFP Section G.5.6.4 will be labeled CONTROLLED UNCLASSIFIED INFORMATION (CUI) or Granite-selected designation per document sensitivity.

5.7.5.2 – Other Privacy and Security Safeguards – Granite acknowledges the government’s right to perform audits, reviews, scans, or other inspections of Granite’s IT environment used to provide or facilitate services to the government and will comply with the responsibilities required by FAR Part 52.239. In accordance with 52.239-1, Granite shall be responsible for the following safeguards:

5.7.5.2.1 – Non-Disclosure – Granite will not publish or disclose in any manner, without the CO’s written consent, the details of any safeguards either designed or developed by

Granite under the EIS contract or otherwise provided by the government (except for disclosure to a consumer agency for purposes of security A&A verification).

5.7.5.2.2 – Physical Access – To the extent required to carry out a program of inspection to safeguard against threats and hazards to the security, integrity, and confidentiality of any non-public government data collected and stored by Granite, Granite will provide the government logical and physical access to its facilities, installations, technical capabilities, operations, documentation, records, and databases within 72 hours of the request.

5.7.5.2.3 – Automated Audits - Automated audits shall include, but are not limited to, the following methods:

- Authenticated and unauthenticated operating system/network vulnerability scans
- Authenticated and unauthenticated web application vulnerability scans
- Authenticated and unauthenticated database application vulnerability scans
- Internal and external penetration testing

5.7.5.2.4 – Automated Scans – Granite will support automated scans as defined in Section G.2.6.6. Granite may choose to run its own scan and understands that the results may be accepted in lieu of government-performed vulnerability scans. In these cases, scanning tools and their configurations shall be approved by the government. In addition, the results of Granite-conducted scans will be provided in full to the government.

5.7.5.3 - Personnel Security Suitability - Granite shall comply with FAR 52.204-9 and require that employees with access to government information that is within the security A & A scope under applicable TO’s shall successfully complete a background investigation in accordance with RFP Section G.5.6.6.1.

5.8 - DATA RETENTION

In accordance with RFP Section G.5.7 and FAR Subpart 4.7, Granite will ensure that, upon request, Granite shall supply any and all records to satisfy an audit, negotiation, or general administration for a period of 3 years.

6.0 - SERVICE ASSURANCE

In accordance with RFP section G.6, Granite shall provide the GSA and agency customers, access to Granite's Customer Support Office (CSO), specifically designed for EIS. [redacted]

[redacted]

6.1 - CUSTOMER SUPPORT OFFICE (CSO): [redacted]

[redacted]

[redacted]

[redacted]— [redacted]

[redacted]

[redacted] [redacted] the [redacted]

[redacted]

5) [redacted]

[redacted]

a) [redacted]

6.3 - SUPPLY CHAIN RISK MANAGEMENT (SCRM): Granite's SCRM plan, Appendix 2B, addresses counterfeit and illegally modified products in accordance with RFP Section G.6.3. [redacted]

6.4 - TROUBLE TICKET MANAGEMENT

Granite shall implement a procedure for processing trouble tickets that are in accordance with RFP Section G.6.4.1, additionally Granite's current process goes above and beyond commercial best practices for trouble ticket response.

Trouble Ticket Management General Requirements: Granite's trouble ticket management infrastructure meets all the government requirements including the following:

1) Creating a trouble ticket for any reported and discovered service issues
2) Providing status updates on a regular basis, even when there has been no change to keep the government informed of efforts for timely resolution.
3) Providing online real-time access to trouble ticketing and system status information.
4) Updating open trouble tickets, as needed.
5) Escalating any trouble ticket in accordance with Granite's internal trouble ticket escalation procedures.
6) Reporting the resolution to the government contact who initiated the trouble ticket, or the designated representative.

Additionally, as a first priority, Granite will restore any TSP restoration coded services using our best efforts, as quickly as possible.

Reporting Information: Granite will provide the government with the flexibility and capability to query and sort trouble complaint records by any field or combination or formatted fields in each record. The government will have the option of saving these records in multiple formats including PDF/CSV or standard/structured file formats.

In addition, Granite shall process any credits applicable to the service outage based on this record of information.

As required, Granite confirms that upon request from the PMO and agencies, Granite will deliver archived trouble and complaint report data within five (5) days of the request for such information.

7.0 - INVENTORY MANAGEMENT

Granite will establish and keep current a complete and accurate inventory of EIS services provided to the GSA and other government customers in accordance with RFP Section G.7 and Section J.2.7. This interface has been developed as per the requirements as defined in RFP Section G.5.3.1.

Granite's Inventory Management Process has been established to perform the following key tasks as set forth by RFP Section G.7.1:

1) Meet the minimum inventory data elements required by service as part of the Inventory Reconciliation (IR) deliverable as specified in Section J.2.7.
2) As new and enhanced services are added by contract modification, additional inventory data elements will be added to the IR deliverable.
3) Granite shall investigate EIS inventory data discrepancies report by the government and work with the government to resolve them.
4) Granite shall make corrections to the EIS inventory as needed to maintain its accuracy and completeness and issues corrected SOCNs or billing as needed.
5) Granite shall meet the inventory requirements for transition as defined in RFP Section C.3.

7.1 - INVENTORY MANAGEMENT FUNCTIONAL REQUIREMENTS

Granite's Inventory Management Process is fully equipped to meet all the key functional requirements by the government as noted in Section G.7.1.1:

1) Granite will fully populate the EIS Inventory with the data elements of the IR as defined in Section J.2.7.
2) Granite will initially populate records of EIS services in the EIS inventory within one (1) business day of the issuance of SOCNs for EIS services delivered to customers.
    a. Granite will establish an inventory for all EIS services provided to its customers.
    b. Granite will maintain and update the EIS inventory for all EIS services provided to the GSA and other government customers.
    c. Granite will make the EIS inventory data available to the government.
3) Granite will deliver IR deliverable each month as defined in Section J.2.7.

7.1.2 - EIS Inventory Maintenance

Granite confirms that it complies with all the EIS inventory maintenance requirements set forth by the government in RFP Section G.7.1.2:

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

7.1.3 - EIS Inventory Data Availability

Granite confirms that it complies with all the EIS inventory data availability requirements set forth by the government in RFP Section G.7.1.3:

1) Granite will provide government users secure electronic access to the current view and to the monthly snapshots of EIS services in the contractor-maintained EIS inventory.
2) For secure web-based queries against Granite's maintained EIS inventory, Granite will, at a minimum:
    a. Provide government users the option to select a user choice of online viewing, data file downloading.
    b. Provide and maintain on its EIS BSS web interface a link for secure, electronic access to the contractor-maintained EIS inventory information.
3) For data export or data file delivery in response to a serious query against Granite-maintained EIS inventory, Granite will, at a minimum:
    a. Support common industry standard formats and file structures
    b. Impose no limit on the number of records that is less than the limit imposed by the file format specification.
4) Granite will make older monthly snapshots of the EIS inventory available to the government as requested, within five (5) days of the government's request.
5) Granite will retain monthly snapshots of the EIS inventory and provide them to the government as requested for three (3) years following the expiration or termination of the contract.
6) Granite will meet or exceed the access security and performance requirements specified in Section G.5.6 BSS Security Requirements for the system used for the EIS inventory.
7) Granite will, at the request of the government, at no additional expense to the government, provide a copy of the records, in the format requested by the government, with data field labels, in the current EIS inventory or any of the monthly snapshots either in their entirety or for a subset specified in the government's request.

8) Granite will, at the request of the government, at no additional expense to the government, provide a copy of the records in the current EIS inventory, in the format requested by the government, in their entirety or for a subset specified in the government's request.
9) Granite will not restrict the use by the government of any and all EIS inventory data related to the contract for the duration of the contract and for three (3) years following the expiration or termination of the contract.

7.1.4 - EIS Inventory Data Discrepancies and Accuracy

Granite confirms that it complies with all the EIS inventory data discrepancies requirements set forth by RFP Section G.7.1.4:

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

Granite confirms that it complies with the EIS inventory data accuracy requirements set forth by RFP Section G.7.1.4.2:

7.1.5 - EIS Inventory Reconciliation

In accordance with RFP Section G.7.1.5, Granite shall comply with the requirements and provide the monthly IR deliverable in accordance with RFP Section J.2.7.

7.2 – DATA INTERACTION REQUIREMENTS

7.2.1 - Common Operational Requirements

7.2.1.1 - GSA Conexus Inventory: In accordance with Section J.2.7.1.1, Granite complies with the government's requirement that the government will maintain a separate inventory based on input from the contractor.

7.2.1.2 - Agency Hierarchy Code: In accordance with Section J.2.7.1.2, Granite confirms that the Agent Hierarchy Code (AHC) shall be tracked for all services from order through disconnection. Granite confirms that it shall comply with the AHC requirements for inventory management as set forth by the government, including:

1) Granite shall support AHC changes without an interruption of service.
2) Granite shall provide the AHC as a data element in the Inventory Reconciliation (IR) deliverable.

7.2.1.3 - Unique Billing Identifier: In accordance with Section J.2.7.1.3 and Section J.2.10.1.1.2, Granite confirms that it will ensure the UBI reported on the IR matches the UBI included on the SOCN and BI for a particular element.

7.2.2 - Inventory Management Process

In accordance with Section J.2.7.2, Granite confirms that inventory management shall follow the process as set by the government. Granite confirms that it shall submit all deliverables in the process below to GSA and, if requested, to the customer. The process will be as follows:

1) Granite shall submit an IR deliverable monthly, no later than the 15th day of the month.
2) If Granite identifies a discrepancy in a previously submitted IR, it shall submit a corrected IR within 3 days of identifying the discrepancy.

3) If the government identifies a discrepancy in the IR, it will follow the dispute process, in accordance with Section J.2.6.

7.2.3 - Deliverables and Data Exchange

In accordance with Section J.2.7.3, Granite confirms that it shall comply with the deliverables and data exchange requirements as set forth by the government and the detailed contents of such data sets, as set forth in Section J.2.10.2. For each data set, Granite shall support all required transfer mechanisms as defined in Section J.2.9.

8.0 - SERVICE LEVEL MANAGEMENT

Granite confirms that it will comply with the approach to Service Level Management as defined in Section G.8 and Section J.2.8.

8.1 - OVERVIEW

Granite will provide the GSA and other agency customers with Service Level Agreements (SLAs) to provide a service at a performance level that meets or exceeds the specified performance objective(s) in RFP Section G.8.1. Granite will comply with the Key Point Indicators (KPIs) as set forth by the government. For each KPI, Granite will meet specified Acceptable Quality Levels (AQLs). For certain services that are deemed essential to government operations, Granite will issue specified credits if the specified service levels are not met.

8.2 - SERVICE LEVEL AGREEMENT TABLES

Granite confirms that it will offer, at a minimum, the SLAs associated with the services in the table provided by EIS in RFP Section G.8.2.1.1.1. Granite understands that agencies may define additional or different SLAs, KPIs, or AQLs during the TO process. Granite understands that if it is awarded a TO and there are TO-specific SLAs, that those SLAs will be equally binding, and Granite will be subject to the terms and conditions stated after agreeing to the measurement and price.

8.2.1 - Service Performance SLAs

[redacted]

[redacted]

[redacted]

[redacted]

a. [redacted]

[redacted]

[redacted]

[redacted]

1) [redacted]

8.2.1.3 - Service-Related Labor SLAs - In reference to RFP Section G.8.2.1.3 Granite confirms that it shall comply with the SPIs and SLAs specified to and defined in each TO. Granite shall also comply with the measurement methods, SLA credit formulations, and tracking methodology, as defined in the specific TO.

8.2.2 - Service Provisioning SLAs

Granite confirms that it shall comply with RFP Section G.8.2.2 with the SLAs for the provisioning of services. Granite will measure the provisioning interval for orders in days from the TO submission date if no service orders are used, or else from the service order date to the completion in the Service Order Completion Notices (SOCNs) in accordance with Section J.2.4 Ordering.

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

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

8.2.2.1 - Standard Provisioning SLAs - Granite confirms that it shall complete orders in accordance with the table in RFP Section G.8.2.2.1.1 within the provisioning intervals as defined by the government. Granite understands that failure to complete the provisioning of service within the specified timeframes shall constitute a failure to meet the SLA for that provisioning incident.

8.2.2.2 - Individual Case Basis Provisioning SLAs - Granite understands in accordance with RFP Section G.8.2.2.2 that certain services provisioning tasks do not have predefined provisioning intervals and that for these services, the performance objective shall be defined on an individual case basis (ICB) with the required delivery schedule established in the TO. Granite understands that failure to complete the provisioning of service within the timeframe specified in the TO shall constitute a failure to meet the SLA for that provisioning incident.

8.2.2.2.1 - Services Subject to ICB Provisioning Intervals - Granite confirms that it has reviewed the table in RFP Section 8.2.2.2.1 listing the services subject to ICB provisioning intervals. These services include but are not limited to: Audio Conferencing Service, Contact Center Service, Internet Protocol Service, Managed Network Service, Video Teleconferencing Service, and Voice Services.

8.2.2.3 - Project Provisioning SLAs - Granite confirms that for project orders (orders that require special treatment by the contractor due to the size, complexity, or importance of the services ordered), shall comply with RFP Section G.8.2.2.3 for the performance objective shall be based on the baseline completion dates in the Task Order Project Plan (TOPP) agreed upon and documented by the government and Granite at the time orders are placed and confirmed by Granite. For these services, the performance objective shall be defined on an individual case basis (ICB) with the required delivery schedule established in the TO.

Granite understands that failure to complete the provisioning of service within the timeframes specified in the TOPP shall constitute a failure to meet the SLA.

8.2.2.4 - Rapidly Provisioned Services - Granite is not currently proposing services subject to Rapid Provisioning (i.e., cloud services), however is teaming with companies with cloud capability. In the event services can be provided for a specific task order, Granite will propose the addition of services to the base contract and provide rapid provisioning details including provisioning intervals at such time.

8.2.2.5 - Service Provisioning SLA Credit Formulas - Granite confirms that for each failed SLA, Granite shall apply the associated credit in accordance with Section G.8.4 SLA Credit Management Methodology using the following formulas:

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

8.2.3 - Billing Accuracy SLA

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

[redacted]

8.3 - SERVICE LEVEL GENERAL REQUIREMENTS

Granite confirms that it shall meet all SLA Billing Accuracy requirements as defined in Section G.8.3, and the Service Level Agreement Tables found in RFP Section G.8.2. This includes delivering the service, maintaining the service at specified AQLs, measuring the

KPIs, reporting on compliance, and issuing the specified credit when performance fails to meet the performance objective.

8.3.2 - Reporting

Granite confirms that it will provide service level management reports as detailed in Section G.8.5 Service Level Reporting Requirements.

8.3.3 - Credits and Adjustments

In accordance with RFP Section G.8.3.3 Granite confirms that in cases where Granite does not meet the defined contractual or TO SLA, Granite shall provide credits and/or adjustments to the government agency of record or GSA as required by G.8.4.

8.4 - SLA CREDIT MANAGEMENT METHODOLOGY

Granite shall comply with RFP Section G.8.4, and if it fails to meet the performance objectives specified in the SLAs defined by the government, then the government is entitled to receive credit in the next available billing cycle. The amount of credit shall be calculated as specified in the applicable portion of Section G.8.2 Service Level Agreement Tables.

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

Granite understands that the government may grant a waiver from all or part of a credit if exceptional circumstances warrant.

Granite understands that the TO on the bill defines the customer that will receive the credit and may grant a waiver for all SLAs except the Account Billing Accuracy Credit for

Central Billed TOs. Granite understands that for this exception, GSA will receive the credit and may grant the waiver.

8.4.1 - Credit Management

Granite confirms that it has reviewed and shall comply with the Credit Management process as defined in RFP Section G.8.4.1. Granite understands that the government reserves the right to subject a SLA Credit Request (SLACR) at any time within six (6) months of the original SLA failure. Thereafter, Granite will respond to the SLACR within 30 days by submitting a SLACR response. Should Granite accept the request, Granite will issue a credit within two (2) business cycles of the response.

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

8.5 - SERVICE LEVEL REPORTING REQUIREMENTS

8.5.1 - Report Submission

In accordance with RFP Section G.8.5.1 Granite shall create and submit each Service Level Report specific to each TO and address only those actions and metrics applicable to the TO in question. As indicated in Section G.5, Granite shall submit these reports electronically via Granite's web interface and via direct data exchange.

8.5.2 - Report Definitions

8.5.2.1 - Service Level Agreement Report - In accordance with RFP Section G.8.5.2.1 Granite has created and will issue Service Level Agreement Reports (SLARs) which will document monthly SLA performance covering all aspects of service including incident-based SLAs, service-specific SLAs, service provisioning SLAs, and program management SLAs. Granite shall deliver this report on the 15th day of each month or as per specific TO preferences.

8.5.2.2 - SLA Credit Request (SLACR) Response - Upon the submission of a Service Level Agreement Credit Request (SLACR), as required by RFP Section G.8.5.2.2 Granite shall submit a response which shall document Granite's response to the government's request for SLA credits. Granite shall deliver this response to the government within 30 days of receipt of the SLACR.

8.5.2.3 - Trouble Management Performance Summary Report - Granite shall document and submit a trouble management performance summary report as required by RFP Section G.8.5.2.3 which will include information on the number of trouble tickets opened and resolved during the reporting period. Granite will submit this report within 14 days after the end of each FY quarter.

8.5.2.4 - Trouble Management Incident Performance Report - Granite shall document and submit a trouble management incident-level performance report as required by RFP Section G.8.5.2.4, which will include the following information: trouble report number, agency and AHC, UBI, time opened, and time resolved. Granite will submit this report within 14 days after the end of each FY quarter.

8.6 - DATA INTERACTION REQUIREMENTS

8.6.1 - Common Operational Requirements

8.6.1.1 - SLA Measurement - In accordance with Section J.2.8.1, Granite confirms that it will proactively measure each applicable SLA in accordance with its definition, capturing its performance relative to each KPI associated with the SLA as described in Section G.8.3.1.

8.6.1.2 - SLA Credit Requests - In accordance with Section J.2.8.1.2, Granite confirms that the government shall have six (6) months of the SLAR containing the SLA failure, to issue a credit request. Granite confirms that it will review such requests and respond as required in Section G.8.4.1.

8.6.2 - SLA Management Process

In accordance with Section J.2.8.2, Granite confirms that it shall comply with that all deliverables and other data sets, including the processes defined in Section J.2.8.3. Unless otherwise specified, Granite shall submit all deliverables in the process below to GSA and, if requested, to the customer.

8.6.2.1 - SLA Reporting Process - In accordance with Section J.2.8.2.1, Granite confirms that it shall measure each KPI associated with the applicable SLA, as described in Section G.8.

In accordance with Section J.2.8.2.1, Granite shall submit a Service Level Agreement Report (SLAR), which captures our performance on all applicable SLAs and associated KPIs monthly, NLT the 15th day of the month.

In accordance with Section J.2.8.2.1, Granite shall submit supplementary reports quarterly, including the Trouble Management Performance Summary Report in accordance with G.8.5.2.3 and the Trouble Management Incident Performance Report in accordance with Section G.8.5.2.4.

8.6.2.2 - SLA Credit Process - In accordance with Section J.2.8.2.2 and Section G.8.4, credits for failed SLAs shall be managed with the following process:

1) The government shall issue a SLA Credit Request (SLACR) within six (6) months of the SLAR containing the SLA failure.

2) Granite shall submit a SLACR response within 30 days of the SLACR.

3) If Granite accepts the government's finding, the credit shall be reflected on a BA within two (2) billing cycles of the SLACR response.

4) If Granite disagrees with the government's finding, the government may use the dispute process as defined in Section G.4.4 and Section J.2.6.

8.6.3 - Deliverables and Data Sets

In accordance with Section J.2.8.3, Granite confirms that it shall comply with the deliverables and data exchange requirements as set forth by the government and the detailed contents of such data sets, as set forth in Section J.2.10.2. For each data set, Granite shall support all required transfer mechanisms as defined in Section J.2.9.

9.0 - PROGRAM MANAGEMENT

Granite's PMP included at Appendix 2A provides a detailed overview of Granite's entire program management model for EIS in accordance with the requirements of RFP Section G.9.

9.1 – Project Management

[redacted]

9.1.1 – Task Order Project Plan (TOPP)

[redacted]

9.2 – Performance Management

Granite will comply with the terms and conditions of Section G.3.5, Performance Management: For completion timeframes associated with orders for services as defined in Section G.3.3, Granite will meet and comply with the requirements for service provisioning intervals as defined in Section G.8.

10.0 - TRAINING

This Granite Training Plan (Training Plan) is carefully designed to ensure the development and delivery of high-level training for all government users of telecommunication services on Granite's platform as requested by the government throughout the life of the contract. Granite's philosophy is customization. This philosophy extends beyond Granite's ability to work with a government user to customize a telecommunications package best suited for its needs, it also includes the customization of a training program.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

10.3 - TRAINING ADMINISTRATION

[redacted]

[redacted]

[redacted]

[redacted]

10.4 - COURSE OFFERINGS

[redacted]

[redacted]

TABLE 2-6:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

11.0 - NATIONAL SECURITY AND EMERGENCY PREPAREDNESS

[redacted]

12.0 - CLIMATE CHANGE ADAPTATION, SUSTAINABILITY & GREEN INITIATIVES

[redacted]

13.0 - INSPECTION AND ACCEPTANCE

13.1 - FAR CLAUSES INCORPORATED BY REFERENCE

[redacted]

[redacted]

[redacted]

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

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

13.2 TEST METHODOLOGY

13.2.1 - Business Support Systems Verification Testing

In accordance with Section E.2.1 Business Support Systems Verification Testing, the Draft BSS Verification Test Plan has been provided herewith at Appendix 2C.

Granite understands that updates may be needed and is eager for feedback from the GSA team. Granite shall comply with a timeline of 14 days from the receipt of government comments to submit an updated test plan. Granite further understands that some projects may require a modified testing plan and shall edit the current BSS plan as needed to support different task orders.

Granite recognizes the importance of a comprehensive and secure testing plan. As specific task orders run through many departments it's important to ensure that all departments comply with the overall BSS testing methodology. BSS testing will be performed on all Granite internal departments that manage the different life of contract. Government representatives will be allowed to observe all or any part of verification testing on a non-interference basis. If a retest is requested, updated results will be provided within seven (7) business days. Granite shall utilize the government team's schedule to schedule tests.

13.2.1.1 - Scope

In accordance with Section E.2.1.1 Scope, Granite shall meet the following Inspection and Acceptance requirements:

- BSS testing shall verify that all BSS functional, regression and security requirements have been successfully met.
- BSS testing shall be performed for all management and operation functions supporting Ordering, Billing, Inventory Management, Disputes, SLA Management and Trouble Ticketing processes described in Section G and Section J.2.
- Security testing shall be based on the requirements described in Section G.5.6 BSS Security Requirements. The security requirements acceptance shall be based on:
    - Assessment and Authorization (A&A)
    - FedRAMP certification (if applicable)
- BSS testing shall include multiple test cases that are defined in Section 0 Test Cases.
- BSS testing shall include use cases for quality, utility and customer access features.
- Granite shall allow government representative(s) to observe all or any part of the verification testing on a non-interference basis.
    - If the government so requests, Granite shall perform tests to ensure continued compliance each time a new service is offered or Granite modifies features/functionality of the BSS that affect the functional requirements described in Section G and Section J.2.
    - If the government requests this retest, Granite shall provide a BSS Verification Test Results report, including analysis, within seven (7) days after performance of the tests. The government reserves 14 days to

accept or reject the test results, in part or in whole. If the government rejects the test results Granite shall retest until such time the results are acceptable to the government.

Granite shall perform BSS verification testing according to the accepted BSS Test Plan at a mutually acceptable date with the government.

13.2.1.2 - BSS Test Scenarios

13.2.1.2.1 - Testing Prerequisites **-** In accordance with Section E.2.1.2.1 Testing Prerequisites, Prior to initiating BSS testing, Granite shall: Provide written notice to the government that Granite's BSS has passed its internal testing and is ready to begin BSS interface testing with GSA Conexus. Provide a finalized BSS Test Plan that is accepted by GSA. Granite shall ensure that the BSS meets requirements in Section G and Section J.2. Granite shall support BSS security and functional testing as defined in Section G.5.6 BSS Security Requirements and Section G.5.5.1 BSS Testing.

13.2.1.2.2 - Testing Scenarios **-** In accordance with Section E.2.1.2.2 Testing Scenarios, Granite shall ensure testing scenarios and the associated results pass the defined acceptance criteria noted in the table. Additionally, per Table 2-9 below (per Section E.2.1.2.2), Granite shall address the test scenarios based on the functional requirements defined in the relevant portions of Section G and/or Section J.2.The scenarios shall address relevant data exchange mechanisms and validation of data exchanged. Each Test Scenario is associated with one or more Test Cases defined in Section E.2.1.3.

TABLE 2-9:

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

[redacted]

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

[redacted]

[redacted]

13.2.1.3 - BSS Test Cases

In accordance with RFP Section E.2.1.3 BSS Test Cases, Granite shall accept, incorporate into the BSS Test Plan, and successfully execute test cases provided for each of the test scenarios in the above Table 2-9 and RFP Section E.2.1.2.2.

Granite [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

TABLE 2-10:

[redacted]	[redacted]

[redacted]

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

13.2.1.4 - Test Results

In accordance with Section E.2.1.4 Test Results, Granite shall demonstrate that it successfully meets the BSS acceptance criteria for the various test scenario #/test case #/ Test Data Set #; Date of Test performed, Acceptance Criteria, Test Result (Pass/Fail) defined in Sections E.2.1.2 and E.2.1.3.

[redacted]

[redacted]

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

[redacted]

[redacted]

13.2.1.5 - Deliverables

13.2.1.5.1 – BSS Verification Test Plan

In accordance with Section E.2.1.5.1 Verification Test Plan for Contractor's BSS, Granite shall submit a BSS Verification Test Plan (BSS Test Plan) based on the following timeline:

- Draft: with proposal (Provided herewith at Appendix 2C)
- Final: 30 days after NTP
- Revisions: 14 days after receipt of government comments

The BSS Test Plan shall:

- Reflect the test methodology defined in Section E.2.1.
- Include Granite's approach to testing each test scenario and test case

- Include Granite’s timeline and test sequencing

13.2.1.5.2 - Verification Test Results Report for Granite’s BSS - In accordance with Section E.2.1.5.2 Verification Test Results Report for Contractor’s BSS, Granite shall provide a BSS Verification Test Results Report that includes analysis of the current testing and a summary table of all previously submitted test results, within seven (7) days after performance of the tests. Granite shall perform re-test of test cases with test data sets that failed until they are accepted by the government. Granite shall rerun tests, in part or in whole, as deemed necessary by the government, to verify that the government’s comments on the test results are satisfactorily addressed.

13.2.2 - EIS Services Verification Testing

In accordance with Section E.2.2 EIS Services Verification Testing, Granite shall provide an EIS Services Verification Test Plan (EIS Test Plan) based on the test methodology defined in Section E.2.2 (test scenarios, test cases, test data sets, acceptance criteria) in response to the RFP for each of the proposed EIS services.

- Please see Appendix 2D: EIS Services Verification Test Plan

13.2.2.1 - General Testing Requirements

In accordance with Section E.2.2.1 General Testing Requirements, Granite shall meet the following EIS Services testing requirements:

- Provide a verification and acceptance testing approach for all awarded EIS services defined in Section C.2.
- Develop an EIS Test Plan that includes, but is not limited to:
    - The test methodology for each EIS Service with test cases that will define the parameters to be measured, the measurement procedure, and the acceptance (pass/fail) criteria.

  - Fallback approach to describe the fallback process and procedures in case of testing failure.
  - An EIS Test Plan shall be required for all new services during the life of the contract.

Granite is aware that the following conditions also apply:

- An agency may define additional testing in the TO.
- Granite shall allow government representative(s) to observe all or any part of the EIS services verification testing.

Granite shall provide all necessary test equipment: data terminals, load boxes, test cables, and any other hardware and software required for testing.

In the report referenced in E.2.2 Granite lays out its testing methodology for the mandatory and optional services defined in Section C.2. This verification test will be augmented as requested by GSA officials as test plans evolve over the course of the contract. Granite is open to additional testing when requested by the TO as well as observation from government officials. Granite understands and complies that in such a testing scenario Granite may need to provide hardware for testing purposes at no additional cost to the government. AS Granite is a small business and in many instances adheres to the specifications laid out in the requirements of TS01-TS03 referenced in Section E.2.2.2.1, Granite shall have to and has begun pursuing Fedramp certification in order to meet the requirements of TS01. Granite shall utilize it's current test plan to meet the requirements of TS02. Granite, as a wholesale provider of lines does not own any last mile services or it's own dark fiber. As such, Granite shall utilize tier 1 carriers for such services that do utilize BSS testing methodologies.

13.2.2.2 - Test Scenarios

In accordance with Section E.2.2.2 Test Scenarios, the EIS Test Plan shall include, but not be limited to, the following test scenarios (see Section E.2.2.2.1 and the corresponding table below).

13.2.2.2.1 - EIS Services Verification Test Scenarios

In accordance with Section E.2.2.2.1 EIS Services Verification Test Scenarios, the EIS Test Plan shall include, but not be limited to, the following test scenarios (see Table 2-11 below).

TABLE 2-11:

[redacted]

[redacted]

[redacted]

13.2.2.3 - Test Cases

In accordance with Section E.2.2.3 Test Cases, Granite shall provide test cases for each of the test scenarios defined in Section E.2.2.2. The test cases are defined in the EIS Test Plan.

- Please see Appendix 2D: EIS Services Verification Test Plan

13.2.2.4 - Test Data Sets

In accordance with Section E.2.2.4 Test Data Sets, Granite shall successfully test all of the test cases defined in the EIS Test Plan using one or more test data sets proposed by Granite. Granite shall test all services and service features proposed at the TO. Granite shall use test data sets that reflect real-world service conditions and locations and shall address all relevant test cases.

13.2.2.5 - Test Results and Acceptance

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

the [redacted]

13.2.2.6 - Deliverables

13.2.2.6.1 – EIS Services Verification Test Plan

In accordance with Section E.2.2.6 Deliverables, Granite has provided herewith the EIS Services Verification Test Plan at Appendix 2D. The Plan describes the testing of EIS Services based on test methodology described in Sections E.2.2.1 – E.2.2.5. Updates will be submitted for any new services that are added to the contract.

13.2.2.6.2 – EIS Testing Report

Granite will provide an EIS Testing Report as defined in Section E.2.2.5 within 3 days of service installation and testing.

14.0 - KEY PERSONNEL

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

14.2.1 - Escalation – Escalation contacts for resolving critical issues are provided in Appendix 2A, PMP at Tables 2A-8 and 2A-9. [redacted]

14.3 – COORDINATION AND COMMUNICATION

[redacted]

14.3.1 – COORDINATION OF TECHNICAL PERSONNEL

[redacted]

14.3.2 – CUSTOMER COMMUNICATION MANAGEMENT

[redacted]

[redacted]

[redacted]

14.3.3 – NETWORK MANAGEMENT COORDINATION AND COMMUNICATION

[redacted]

14.3.4 – CAPABILITY AND AUTHORITY

[redacted]

[redacted]

- [redacted]

[redacted]

[redacted]

15.0 - DATA INTERACTION PLAN

Granite understands and will comply with the data deliverables and processes for EIS Management and Operations as defined in RFP Section J.2. Granite fully understands the roles, responsibilities, timeframes and overall process presented in Section J.2.1.1. The primary applications that will be utilized to support the EIS requirements are owned, maintained, and administered by Granite. As such, Granite has the ability to customize a module to satisfy the specific data requirements of EIS, and will do so as required.

15.1 - COMMON DATA INTERACTION REQUIREMENTS

Granite understands and will comply with the submission authority as defined by J.2.2.1, the resubmission requirements outlined in J.2.2.2, the format and transfer mechanisms as defined by J.2.2.3 and scope of deliverables in accordance with J.2.2.4.

15.1.1 - Task Order Data Management – The requirements for Task Order Data Management as required by RFP Section J.2.3 are addressed above under Contract Administration in Proposal Volume II – Management Section 2.0 and Appendix 2A, PMP.

15.1.1.1 – Task Order Initial Setup – In accordance with RFP Section J.2.3.2.2, the following process will be followed at the initial setup of each TO, to be completed prior to provisioning or providing any services under the TO:

Task Order SET UP PROCESS:

a.) Granite shall submit the following deliverables to GSA:
   a. TO Services and CLINs awarded
   b. TO County/Jurisdiction Awarded by Service / TO Locations awarded by Service
   c. TO Officials
   d. TO Customer Requirements Document Set
   e. TO Financials
   f. TO Key Performance Indicators

b.) Granite shall collect from the customer the list of users and user permissions for RBAC.

c.) Granite shall set up or modify appropriate RBAC permissions within its BSS as described in Section G.5

d.) Granite shall submit the Direct Billed Agency Setup (DBAS) to GSA.15.1.2 - Ordering - The Data Interaction requirements related to Ordering as required by RFP Section J.2.4 are addressed above in Proposal Volume II – Management Section 3.015.1.3 - Billing - The Data Interaction requirements related to Billing as required by RFP Section J.2.5 are addressed above in Proposal Volume II – Management Section 4.0.

15.1.4 - Disputes - The Data Interaction requirements related to Disputes as required by RFP Section J.2.6 are addressed above in Proposal Volume II – Management Sections 4.2, 7.0 and 8.0

15.1.5 - Inventory Management - The Data Interaction requirements related to Inventory Management as required by RFP Section J.2.7 are addressed above in Proposal Volume II – Management Section 7.0

15.1.6 - SLA Management - The Data Interaction requirements related to SLA Management as required by RFP Section J.2.8 are addressed above in Proposal Section 8.0

15.1.7 - Data Transfer Mechanisms - In accordance with Sections J.2.3.3.1, J.2.3.3.2, and J.2.3.3.3, for each data set, Granite shall support all data transfer mechanisms as defined in RFP Section J.2.9; Data Transfer Mechanisms

15.1.7.1 - Common Operational Requirements

15.1.7.1.1 - Governance of Exceptions - In accordance with Section J.2.9.1.1 Governance of Exceptions, Granite shall only allow exceptions in the data transfers mechanism subsection to be requested by a GSA official when related to data submitted to the GSA or the relevant Ordering Contracting Officer if submitting data directly to a customer. (Ref: Section J.2.2.1 Relevant Contracting Officer)

15.1.7.1.2 - Multiple Transfer Mechanisms - In accordance with Section J.2.9.1.2 Multiple Transfer Mechanisms, Granite shall maintain the capability to accept all required data transfer mechanisms for data sets transferred from the government to the contractor.

Granite shall submit data to the government using the listed data transfer mechanisms unless an exception is approved by the relevant CO.

Granite shall maintain the ability to accept initiate data transfers via Secure FTP, Email, and Granite's proprietary web interface rock reports which is available 24/7 via a secure web portal. If a task order requires a specific different form of data transfer, Granite shall work with the relevant contracting officer to develop a secure method of transportation.

15.1.7.1.3 – Task Orders - In accordance with Section J.2.4.1.1, once a TO is issued, Granite will follow the process described in J.2.2.4 and J.2.3, Task Order Data Management.

15.1.7.2 - Direct Data Exchange

15.1.7.2.1 - Direct Data Exchange Mechanisms - In accordance with Section J.2.9.2.1 Direct Data Exchange Mechanisms, Granite shall support direct data exchange between its BSS and GSA based on the requirements captured in Section G.5.3.2 Direct Data Exchange using the following methods:

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

[redacted]

15.1.7.2.2 - Attachments via Direct Data Exchange - In accordance with Section J.2.9.2.2 Attachments via Direct Data Exchange, Granite shall also submit any Binary Large Object (BLOB) attachments required in the definitions of the various data sets in Section J.2.10.2. Granite shall transfer these files separately via SFTP as described above and name the files based on the following template

[redacted]

[redacted]

[redacted]

[redacted]

15.1.7.3 - Contractor's Web Interface

[redacted]

[redacted]

[redacted]

[redacted]

15.1.7.4 - Email

In accordance with Section J.2.9.4 Email, Granite shall following the specified instructions when emailing data to the government:

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

Pursuant to Section J.2.9.4 Email, Email is specified as the data transfer mechanism in cases where the data is unstructured or not intended for automated analysis. Data emailed from the government to the contractor may be included in the body of the email or in one or more attachments.

15.1.7.5 - GSA Systems

[redacted]

[redacted]

[redacted]

15.1.7.6 - Other Means as Agreed or Required in the TO

[redacted]

[redacted]

15.1.8 – Data Dictionary

Granite has reviewed and confirmed its ability to support all data dictionary elements and values as detailed in solicitation Section J.2.10. The primary applications that will be utilized to support the EIS requirements are owned, maintained, and administered by Granite. As such, Granite has the ability to customize a module to satisfy the specific data requirements of EIS, and will do so as required.

15.1.8.1 – Unique Billing Identifier (UBI)

In accordance with Section J.2.10.1.1.2.2, Granite will create and assign the UBI for each installed service instance grouping (as defined in J.2.10.1.1.2.2) in compliance with the

UBI specifications detailed in RFP Section J.2.10.1.1.2.1, even if there is only one member of the group. For SRE, the UBI is assigned as above with each associated SRE Pricing Element using the same UBI.

15.1.8.2 – TO Financials

[redacted]

16.0 – INDEX OF TABLES, FIGURES, AND EXHIBITS

TABLE 2-14	REMOVED (moved to PMP)

17.0 – INDEX OF ACRONYMS

Acronym	Description
A&A	Assessment & Authorization
ACH	Automated Clearing House
AGF	Associated Government Fee
AHC	Agency Hierarchy Code
AGFD	Associated Government Fee Detail
ASRN	Agency Service Request Number
ATO	Authorization to Operate
ATR	AGF Electronic Funds Transfer Report
BA	Billing Adjustment
BI	Billing Invoice
BLOB	Binary Large Object
CBAS	Central-Billed Agency Setup
CBASR	Central-Billed Agency Setup Reply
CBSA	Core-Based Statistical Area
CEO	Chief Executive Officer
CLIN	Contract Line Item Number
CO	Contracting Officer
COO	Chief Operating Officer
COTS	Commercial Off-The-Shelf
CPCM	Certified Professional Contracts Manager

CSO	EIS Customer Support Office
CSV	Comma Separated Value
CTW	Control Tailoring Workbook
CWD	Customer Want Date
DBAS	Direct-Billed Agency Setup
DR	Dispute Report
DSS	Decision Support Systems
EDI	Electronic Data Interchange
EIS PM	Base IDIQ Level Granite Program Manager
EFT	Electronic Funds Transfer
ERP	Enterprise Resource Planning
FA	Granite EIS Lead Financial Analyst
FIPS	Federal Information Processing Standards
FISMA	Federal Information Security Management Act
FOCN	Firm Order Commitment Notice
FOIA	Freedom of Information Act
GHG	Greenhouse Gas
GPC	Government Purchase Card
HTTPS	Secure Hypertext Transfer Protocol
ILEC	Incumbent Local Exchange Carrier
ICB	Individual Case Basis
IPP	Invoice Processing Platform
KPI	Key Performance Indicator
MAC	Moves, Adds, Changes

NIST	National Institute of Standards and Technology
NOC	Granite Network Operating Center
PDF	Portable Document Format
PMP	Program Management Plan
POC	Point of Contact
PON	Provisioning Order Number
PPM	Premier Project Manager
PSV	Pipe-Separated Value
QPMR	Quarterly Program Management Review
QPSR	Quarterly Program Status Report
RBAC	Role-Based Access Control
RBOC	Regional Bell Operating Company
SE	Granite EIS Lead Solutions Engineer
SFTP	Secure File Transfer Protocol
SLACR	Service Level Agreement Credit Request
SLAR	Service Level Agreement Report
SO	Service Order
SOA	Service Order Acknowledgement
SOAC	Service Order Administrative Change
SOAP	Simple Object Access Protocol
SOC	Service Order Confirmation
SOCN	Service Order Completion Notice
SORN	Service Order Rejection Notice
SP	Special Publication

SPOC	Single Point of Contact
SSCN	Service State Change Notice
TO	Task Order
TO PM	Task Order Level Granite Program Manager
TOPP	Task Order Project Plan
TSM	Technology Service Manager
TSP	Telecommunications Service Priority
UBI	Unique Billing Identifier
USOC	Universal Service Order Code
VCCS	Vendor And Customer Self Service
WAWF	Wide Area Work Flow
XML	Extensible Markup Language
VCCS	Vendor And Customer Self Service
WAWF	Wide Area Work Flow

18.0 INDEX OF APPENDICIES

Appendix	Description
2A	Program Management Plan
2B	Supply Chain Risk Management (SCRM) Plan
2C	Draft BSS Verification Test Plan
2D	EIS Verification Test Plan
2E	Climate Risk Management Plan
2F	Sample Financial Status Report
2G	BSS Risk Management Framework Plan

2H NS/EP Functional Requirements Implementation Plan