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

Appendix 2C

BSS Verification Test Plan

(Draft)

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

Solicitation Number QTA0015THA3003

GSA

REVISION HISTORY

REVISION NUMBER	REVISION DATE	SUMMARY OF REVISION
1440	**04 NOV 16**	**Final Proposal Revision**
1440 Rev. 1	**16 MAR 17**	**Final Proposal Revision Rev. 1**

Draft BSS TEST PLAN for EIS

Prepared By Granite Telecommunications, LLC ("Granite")

Prepared by: Pano Fitopoulos,

Document Approvals

---------- DATE: __/__/__

Business User

---------- DATE: __/__/__

---------- DATE: __/__/__

Pano Fitopoulos

---------- DATE: __/__/__

QA Manager

THIS PAGE INTENTIONALLY LEFT BLANK

1.0 Test Plan-Overview

In accordance with Section E.2.1 Business Support Systems Verification Testing, Granite has prepared a draft BSS Verification Test Plan (Plan) based on the test methodology defined in Sections E.2.1.1 – E.2.1.5. Pursuant to the instructions provided, the draft Plan is being included with the proposal in accordance with Section L.27.2 as Part 4 to the Management Volume, and a final Plan will be provided within 30 days of receipt of Notice to Proceed.

This Plan will be used as a guide to develop a detailed test case matrix where actual and expected results are documented.

This Plan is in response to the the Request for Proposal (RFP) #QTA0015THA3003 for the Network Services 2020 (NS2020) Enterprise Infrastructure Solutions (EIS) acquisition for:

- Granite's Business Support Systems (BSS)
- This Plan applies to the services noted in the below table

RFP Reference (SOW)	Service
C.2.1.1	Virtual Private Network Service (VPNS)
C.2.1.2	Ethernet Transport Service (ETS)
C.2.1.7	Internet Protocol Service (IPS)
C.2.2.1	IP Voice Service (IPVS)
C.2.2.2	Circuit Switched Voice Service (CSVS)
C.2.8.1	Managed Network Service (MNS)
C.2.8.7	Audio Conferencing Service
C.2.10	Service Related Equipment
C.2.11	Service Related Labor
C.2.12	Cable and Wiring

1.1 Test Objective/Goal/Purpose

- The Plan shall meet the following Inspection and Acceptance requirements as set forth by the government in Section E.2.1.1:
- 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.
- BSS testing shall include multiple test cases that are defined in Section E.2.1.3 Test Cases.
- BSS testing shall include test cases for quality, utility, and customer access features.
- Granite shall allow government representatives to observe all or any part of the verification testing.
- Granite shall perform BSS verification testing according to the accepted BSS Test Plan at a mutually acceptable date with the government.

1.2 Test Scope

The scope of this effort includes testing of the web interface that will provide the means for the government to create requests for services (including Pricing catalog), and track those requests through to completion and acceptance of the services. In addition, Granite will include a process for report and requests updates for trouble Tickets, as well as Inventory Management, Billing, and Payment Management based on Technology and Accessibility Standards described on the RFP.

The Functionality Test will include:

1. Validating the Direct Data Exchange [Test Scenario #BSS-TS01 – *RFP Ref: G.5.3.2 and J.2.9*].
2. Web Services:
   - 2.1. Test Business to Business (B2B) Application Program Interfaces (APIs) for system-to-system data exchange between government and contractor systems
     - 2.1.1. Using XML over HTTPS using SOAP as the web services exchange mechanism
       - 2.1.1.1. Bi-directional transactions
     - 2.1.2. Email
3. Test Secure File Transport Protocol (SFTP) Services:
   - 3.1. Test the file-based data exchange between government and contractor systems using government provided FTP service
     - 3.1.1. Bi-directional transactions
   - 3.2. Test Direct Data Exchange of attachments
4. Test the Role-Based Access Control provided by Granite's BSS [Test
5. #BSS-TS03 – *RFP Ref: J.2.3*]
   - 5.1. Allow only authorized users with appropriate permissions access to its BSS including but not limited to,

5.1.1. Ability to place orders and research order,

5.1.2. Billing,

5.1.3. Inventory, and

5.1.4. Performance information.

5.2. Capture and store the authorized users for restricted access

5.3. Restrict all information based on access.

5.4. Managing users and

6. Validate that BSS can support all awarded services as described on [*RFP Ref: C.2*]. The services shall include all C.1.2 Mandatory Services and those optional services that are proposed and awarded.

6.1. Data Service

6.1.1. Virtual Private Network Service

6.1.2. Ethernet Transport Service

6.1.3. Internet Protocol Service

6.2. Voice Service

6.2.1. Internet Protocol Voice Service

6.2.2. Circuit Switched Voice Service

6.3. Managed Service

6.3.1. Managed Network Service

6.3.2. Audio Conferencing Service

6.4. Access Arrangements

6.4.1. Access Arrangement Description

6.4.2. Access Diversity and Avoidance

6.4.3. Interfaces

6.5. Service Related Equipment

6.5.1. Warranty Service

6.6. Service Related Labor

6.7. Cable and Wiring

7. Test transaction elements on the BSS for all the above “awarded” services that it can handle the different transaction elements which the government will be exchanging to Granite
   7.1. Test Order Management process based on the one or more Agency Hierarchy Codes (AHCs)
   7.2. Test Order Submission [Test Scenario #BSS-TS04 – *RFP Ref: G. 3 and J.2.4*]
      7.2.1. Orders for New Services
      7.2.2. Orders to Change Existing Services
      7.2.3. Move Orders
      7.2.4. Feature Change Orders
      7.2.5. Disconnect Orders
      7.2.6. Administrative Change Orders
   7.3. Test Positive and negative Order Submission [Test Scenario #BSS-TS07 – *RFP Ref: G.3.5.6 and J.2.4.2.4*]
      7.3.1. Orders for New Services
      7.3.2. Orders to Change Existing Services
      7.3.3. Move Orders
      7.3.4. Feature Change Orders
      7.3.5. Disconnect Orders
      7.3.6. Administrative Change Orders
   7.4. Test Order Tracking
      7.4.1. Including Auto-sold CLINs
      7.4.2. Including order supplements/updates that impact other, in-progress orders [Test Scenario #BSS-TS05 – *RFP Ref: G. 3 and J.2.4*]
         7.4.2.1. Cancel the Order
         7.4.2.2. Change Service Delivery Location
         7.4.2.3. Change Service Features

7.4.2.4. Change the Customer Want Date (CWD)

7.4.2.5. Change in Administrative Data

7.4.3. Test that BSS can support Administrative Change Orders to previously provisioned services based on the restrictions and process for [Test Scenario #BSS-TS06 – *RFP Ref: G. 3 and J.2.4*] :

7.4.3.1. Administrative Change Restrictions

7.4.3.2. Administrative Change Order Process

7.5. Track every order through completion by providing all required CDRLs including (but not limited to) [Test Scenario #BSS-TS04 – *RFP Ref: G. 3 and J.2.4*].

7.5.1.1. Service Order Acknowledgement

7.5.1.2. Service Order Rejection Notice

7.5.1.3. Service Order Confirmation

7.5.1.4. Firm Order Commitment Notice

7.5.1.5. Service Order Completion Notice

7.6. **Including Bulk Ordering**

7.7. Self-Service Provisioning and other Rapid Provisioning orders (*Ref. G.3.5.6 and J.2.4.2.4*)

7.8. Test Customer Management sections [Test Scenario #BSS-TS08 – *RFP Ref: G. 4 J.2.6 J.2.7 and J.2.10*]

7.8.1. Trouble Management

7.8.2. Billing Management

7.8.2.1. Billing Cycle

7.8.2.2. Unique Billing Identifier (UBI)

7.8.2.3. Each billable element is identified by a CLIN (Contract Line Item Number)

7.8.2.4. The Associated Government Fee (AGF) is the fee GSA charges other customers for its services in supporting this contract. It is defined, along with calculation methods:

7.8.2.4.1. Calculation of the AGF.

7.8.2.4.2. AGF is provided as a data element in billing deliverables

7.8.2.4.3. For TOs set up with direct billing Granite shall collect the AGF on behalf of GSA and transfer funds as described in Section G.4.6

7.8.2.5. Proration Requirements are followed

7.8.2.6. Rounding Requirements are followed

7.8.2.7. Taxes, Fees and Surcharges Requirements are followed

7.8.2.8. Billing Levels Requirements are followed

7.8.2.9. Billing Data Sets Requirements are followed

7.9. Test Financial Management for [Test Scenario #BSS-TS09 – *RFP Ref: G.4.4 and J.2.6*]

7.9.1. Billing Disputes

7.9.2. Inventory Disputes

7.9.3. SLA Disputes

7.9.4. Credit Management

7.9.5. Payment Tracking [*RFP Ref G.4.4 and J.2.6*]

7.9.6. Dispute Reports

7.10. Test the Inventory Management section [Test Scenario #BSS-TS08 – *RFP Ref: G. 4 J.2.6 J.2.7 and J.2.10*]

7.10.1. Inventory Management [*RFP Ref (G.4, J.2.5, J.2.6, J.2.7 and J.2.10)*]

7.10.1.1. Data Elements

7.10.1.2. Records of EIS services in the EIS inventory

7.10.1.3. IR deliverable each month

7.10.1.4. EIS Inventory Maintenance including reflect all additions, deletions, or changes to the EIS services being provided

7.10.1.5. EIS Inventory Data Availability

7.10.1.5.1. Electronic Access

7.10.1.5.2. Online viewing or data file download

7.10.1.5.2.1. Common industry standard formats

7.10.1.5.2.2. No minimum on number of records

7.10.1.5.2.3. Monthly Snapshots maintenance and availability

7.10.1.5.2.4. Meeting security and performance requirements

7.11. Test the Service Management section of the BSS [Test Scenario #BSS-TS10 – *RFP Ref: G. 8 and J.2.8*]

7.11.1. Service Assurance

7.11.2. SLA Management by measuring each applicable SLA in accordance with its definition, capturing its performance relative to each KPI associated with the SLA

7.11.3. SLA Reporting

7.11.3.1. SLA Credit Request handling and response [*RFP Ref G.4.4 and J.2.6]*

7.12. Test the Program Management section of the BSS

7.12.1. Administration

7.12.2. Project Management

7.13. Test all Reports and Reporting and Reporting Services [Test Scenario #BSS-TS11 – *RFP Ref: G. 4 J.2.6 J.2.7 and J.2.10*]

7.13.1. Monthly Billing Information Memorandum

7.13.1.1. Trouble Management Incident Performance Report

7.13.1.2. Trouble Management Performance Summary Report [*RFP Ref J.2*]

7.13.1.3. Service Catalog

7.14. Test that BSS is using the applicable System Reference Data using consistent codes for common transactional data [including the Test Scenario #BSS-TS02 – *RFP Ref: J.2.3.2.1*](Ex: Technical features such as Access Circuit Type and Bandwidth, Business features such as Agency Bureau Codes and Dispute Reasons and Status features such as Yes/No and True/False codes

7.15. Intentionally Left Blank

7.16. Test that BSS complies with the Direct Billed Agency Setup as described by [Test Scenario #BSS-TS02 – *RFP Ref: J.2.10.2.1.8*] Data Transaction Code: DBAS

7.17. Test that BSS complies with the predefined process for submitting a Telecommunications Service Priority (TSP) order as described in [*RFP Ref G.3.3.3.1*] and to include:

7.17.1. Appropriate prioritizations applicable to TSP orders Telecommunications Service Priority Orders and/or National Security and Emergency Preparedness.

7.17.2. Ensure the non-delay delivery of services in any way based on the need to submit deliverables specified in this process.

7.18. Verify that BSS complies with the security requirements as defined in the BSS System Security Plan (BSS SSP) [Test Scenario #BSS-TS13 – *RFP Ref G.5.6*]

- Validate that BSS comply with the Security General Security Compliance Requirements
- Federal Information Security Management Act (FISMA) of 2002, available at: http://csrc.nist.gov/drivers/documents/FISMA-final.pdf.
- Federal Information Security Modernization Act of 2014; (to amend Chapter 35 of 44 U.S.C.) available at: https://www.congress.gov/113/bills/s2521/BILLS-113s2521es.pdf.

- Clinger-Cohen Act of 1996 also known as the "Information Technology Management Reform Act of 1996," available at: https://www.fismacenter.com/clinger%20cohen.pdf.
- Privacy Act of 1974 (5 U.S.C. § 552a).
- Homeland Security Presidential Directive (HSPD-12), "Policy for a Common Identification Standard for Federal Employees and contractors," August 27, 2004; available at: http://www.idmanagement.gov/.
- OMB Circular A-130, "Management of Federal Information Resources," and Appendix III, "Security of Federal Automated Information Systems," as amended; available at: http://www.whitehouse.gov/omb/circulars_a130_a130trans4/.
- OMB Memorandum M-04-04, "E-Authentication Guidance for Federal Agencies." (Available at: http://www.whitehouse.gov/omb/memoranda_2004).
- OMB Memorandum M-05-24, "Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors." (Available at https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-24.pdf.)
- OMB Memorandum M-11-11, "Continued Implementation of Homeland Security Presidential Directive (HSPD) -12 – Policy for a Common Identification Standard for Federal Employees and Contractors." (Available at https://www.whitehouse.gov/sites/default/files/omb/memoranda/2011/m11-11.pdf.)
- OMB Memorandum M-14-03, "Enhancing the Security of Federal Information and Information Systems." (Available at

https://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf.)

- FIPS PUB 199, “Standards for Security Categorization of Federal Information and Information Systems.”
- FIPS PUB 200, “Minimum Security Requirements for Federal Information and Information Systems.”
- FIPS PUB 140-2, “Security Requirements for Cryptographic Modules.”
- NIST SP 800-18, Revision 1, “Guide for Developing Security Plans for Federal Information Systems.”
- NIST SP 800-30, Revision 1, “Guide for Conducting Risk Assessments.”
- NIST SP 800-34, Revision 1, “Contingency Planning Guide for Federal Information Systems.”
- NIST SP 800-37, Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach.”
- NIST SP 800-39, “Managing Information Security Risk: Organization, Mission, and Information System View.”
- NIST SP 800-41, Revision 1, “Guidelines on Firewalls and Firewall Policy.”
- NIST SP 800-47, “Security Guide for Interconnecting Information Technology Systems.”
- NIST SP 800-53, Revision 4, “Security and Privacy Controls for Federal Information Systems and Organizations.”
- NIST SP 800-53A, Revision 4, “Assessing Security and Privacy Controls in Federal Information Systems and Organizations: Building Effective Security Assessment Plans.”
- NIST SP 800-61, Revision 2, “Computer Security Incident Handling Guide.”
- NIST SP 800-88, Revision 1, “Guidelines for Media Sanitization.”

- NIST SP 800-128, “Guide for Security-Focused Configuration Management of Information Systems.”
- NIST SP 800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations.”
- NIST SP 800-171, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations.”
- In addition to complying with the requirements identified in the government policies, directives and guides specified above, the contractor shall comply with the current GSA policies, directives and guides listed below (the current documents are referenced within the GSA IT Security Policy and are available upon request submitted to the GSA CO):
- GSA Information Technology (IT) Security Policy, CIO P 2100.1(I).
- GSA Order CIO P 2181.1 “GSA HSPD-12 Personal Identity Verification and Credentialing Handbook.”
- GSA Order CIO 2104.1, “GSA Information Technology (IT) General Rules of Behavior.”
- GSA Order CPO 1878.1, “GSA Privacy Act Program.”
- GSA IT Security Procedural Guide 01-01, “Identification and Authentication.”
- GSA IT Security Procedural Guide 01-02, “Incident Response.”
- GSA IT Security Procedural Guide 01-05, “Configuration Management.”
- GSA IT Security Procedural Guide 01-07, “Access Control.”
- GSA IT Security Procedural Guide 01-08, “Audit and Accountability Guide.”
- GSA IT Security Procedural Guide 05-29, “IT Security Training and Awareness Program.”
- GSA IT Security Procedural Guide 06-29, “Contingency Planning Guide.”
- GSA IT Security Procedural Guide 06-30, “Managing Enterprise Risk.”

- GSA IT Security Procedural Guide 06-32, “Media Protection Guide.”
- GSA IT Security Procedural Guide 07-35, “Web Application Security Guide.”
- GSA IT Security Procedural Guide 08-39, “FY 2014 IT Security Program Management Implementation Plan.”
- GSA IT Security Procedural Guide 10-50, “Maintenance Guide.”
- GSA IT Security Procedural Guide 11-51, “Conducting Penetration Test Exercise Guide.”
- GSA IT Security Procedural Guide 12-63, “GSA’s System and Information Integrity.”
- GSA IT Security Procedural Guide 12-64, “Physical and Environmental Protection.”
- GSA IT Security Procedural Guide 12-66, “Continuous Monitoring Program.”
- GSA IT Security Procedural Guide 12-67, “Securing Mobile Devices and Applications Guide.”
- GSA IT Security Procedural Guide 14-69, “SSL / TLS Implementation Guide.”
- NIST SP 800-144 Guidelines on Security and Privacy in Public Cloud Computing December 2011.
- The Committee on National Security Systems Instruction (CNSSI) No. 5000, “Guidelines for Voice over Internet Protocol (VoIP) Computer Telephony,” April 2007.

7.19. Demonstrate that the contractor’s Cloud Services is compliance with Federal Risk and Authorization Management Program (FedRAMP) requirements as defined [Test Scenario #Service-TS-01 – *RFP Ref C.2*]

7.19.1. http://cloud.cio.gov

7.19.2. http://cloud.cio.gov/fedramp/csp

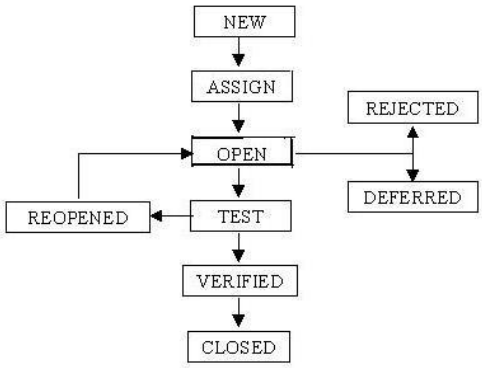
7.19.3. NIST.gov publications http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/201306/ispab_june2013_goodrich.pdf

7.20. Demonstrate that awarded services are delivered based on the KPIs and SLAs defined [Test Scenario #Service-TS-02 – *RFP Ref G.8*]

7.21. Verification Testing of Dark Fiber Services [Test Scenario #Service-TS-03 – *RFP Ref C.2.1.6.1.4*]

1.3 Test Approach

Granite's strategy is to test all listed components of the application and its functionalities by p*erforming nightly building and smoke testing. In order to reveal defects early in the software development process. During these builds, software is compiled, linked, and (re)tested with the goal of validating its basic functionality.* Defects analyzed and assessed for severity based on business requirements. The defect life cycle for Granite's software systems described below:



- The testing of defects will be performed on the following environments
  - DEV Environment (Unit Testing)
  - SIT Environment Testing (Test all interconnecting modules)
  - UAT Environment (End User approval)
  - PROD Environment
- Team to determine testing levels and testing methods [Manual/Automated]

- **Granite Internal Testing**

1. Granite QA team will be performing the SIT testing i.e. writing and executing the SIT test cases.
2. Granite QA will be writing the UAT test cases and will be provided to users for UAT testing.
3. Granite QA will provide all the necessary guidelines to End Users in performing the UAT testing

- **GSA SIT Testing**

1. Granite QA will be performing high level regression testing once the system is integrated to validate the exchange of structured data.
    - Since Granite's Application Code is modulated its easy to identify what other modules/functions are affected by the change and they will be tested in this phase.
2. Successful demonstration of Task Order (TO) Data Management initial setup.

- GSA UAT

1. See 6.19 – 6.21 above for specific test scenarios noted in RFP E.2.2.2.1.
2. NOTE – separate EIS Test Plan will be submitted that references the specific services detailed in section C.2 of the RFP.

1.4 Regression Test Plan

The objective of the Regression Test phase [Test Scenario #BSS-TS12 – *RFP Ref: J.2*] is to ensure that all code changes that occurred in later executions of project integration and large volume testing have not had a negative impact on the validity of earlier tests. During the regression test phase we will cover all applications that may have been affected by some program change implemented during the project integration or large volume test phases. All previous executed Test Cases will become Regression Test Cases for the next phase of the project. It should be noted that for problems, which have a data origin, part or all of the conversion tests may need to be rerun in regression testing.

Purpose

The purpose of Regression testing is the retesting of the BSS that has been modified to ensure that any Defects have been fixed and that no other previously working functions have failed as a result of the reparations and that newly added features have not created problems with previous versions of the software.

High Level Components/Requirements for Testing

- Retest of all previously identified Defects and their fixes.
- Testing will include all Test Cases for the following:
    - Contract Administration
    - Ordering
    - Billing
    - Business Support Systems
    - Service Assurance
    - Inventory Management
    - Service Level Management

- Program Management

Regression Test Plan Exit Criteria

- Positive Exit
  - Completion and acceptance of Project by Granite team.
  - Completion and acceptance of Project by GSA.
  - No Level 1, 2, 3, or 4 defects are left outstanding.
- Negative Exit
  - Level 1, 2, 3, or 4 defects outstanding.
  - Deliverable product not meeting user requirements.
  - Major changes made in the requirements.

1.4 Out Of Scope

2.0 References

TITLE	LOCATION
Document 1	<Document 1 Location>
Document 2	<Document 2 location>
Document 3	<Document 3 Location>

3.0 Test Cases/Test Results

Test Cases are written in reference to above documents provided.

BSS Test Cases Tiered Approach: In accordance with Section E.2.1, BSS testing shall follow a tiered approach. The government will group them into test subcases. Each test subcase shall include at least two complete test data sets. The test subcases will be grouped by:

- Testing Data Properties
- Page Validations
- Process Functionalities

Test Case Results: In accordance with Section E.2.1: the sample test case results matrix is provided below:

Test Scenario #	Test Case #	Test Data Set #	Test #	Date of Test Performed	Acceptance Criteria	Test Results (Pass/Fail)

3.1 Relevant URLs

Below is the list of URLs used for testing purpose.

Name of site	Address	Relevance to the Test Plan
DEV	http://XXXXX	<URL for the DEV environment>
SIT	http://XXXXX	<URL for the SIT environment> environment>
Test/UAT	http://XXXXX	<URL for the TEST environment>
Production	http://XXXXX	<URL for the Production environment>

3.2 Assumptions and Constraints

None

4.0 User Acceptance Testing

User Acceptance testing verifies a user's interaction with the software. The goal of UAT is to ensure that the User Interface provides the user with the appropriate access and navigation through the functions of the target-of-test.

4.1 User Participation

During UAT, actual software users will be testing the software to make sure it can handle required tasks in real-world scenarios, according to specifications defined during the requirements gathering..

4.2 Test Plan Exit Criteria

Positive Exit

- Completion and acceptance of Project by Granite team.
- Completion and acceptance of Project by GSA.
- No Level 1, 2, 3, or 4 defects are left outstanding.

Negative Exit

- Level 1, 2, 3, or 4 defects outstanding.
- Deliverable product not meeting user requirements.
- Major changes made in the requirements.

5.0 Test Schedule

In accordance with Section E.2.1.5.1, item 3, Granite's timeline and test sequencing is set forth below. The "Planned Start Date" column will be populated when dates are known. The estimated effort for each action is provided in the table below. Once the start date for step 1 is defined, the remaining steps will be scheduled in accordance with the estimated effort shown for each step in the test sequence.

Milestone	Planned Start Date	Estimated Effort
Granite Internal Testing 1) Finalize Test Plan (GRT)	TBD	24 Hrs
2) Review Final Test Plan and Test Schedule w/ GSA and Get approval	TBD	16 Hrs
3) Write Test Cases (GRT)	TBD	60 hrs
4) Review Test Cases with GSA and receive approval (GSA)	TBD	16 Hrs
5) Perform Initial Testing (GRT)	TBD	40 Hrs
SIT Testing 6) Write/Revise SIT Test Cases (GRT)	TBD	24 Hrs
7) Review SIT Test Cases with GSA	TBD	16 Hrs
8) Perform SIT Testing (GRT)	TBD	60 Hrs
9) Perform SIT Testing with GSA	TBD	40 Hrs
10) Get SIT approval from GSA	TBD	16 Hrs
UAT Testing 11) Write/Revise UAT Test Cases (GRT)	TBD	24 Hrs
12) Review UAT Test Cases with GSA	TBD	16 Hrs
13) Perform UAT Testing (GRT)	TBD	60 Hrs
14) Perform Testing GRT and GSA	TBD	40 Hrs
15) Perform UAT Regression Testing GRT and GSA	TBD	16 Hrs
16) Get UAT approval from GSA	TBD	16 Hrs

6.0 Defect Tracking

Defects will be tracked and recorded using the Team Foundation Server Defect Tracking Tools. A summary report will be distributed every Friday.

<Defect review meetings will be held on every TBD>

Severity of the defects defined as follows:

Level	Name	Description
1	**Blocker**	Such an error prevents test engineers from further **functional testing**, compatibility testing, **load testing** or other testing works
2	**Critical**	An error of this type is connected with security, leads to the program crash, data loss or other serious damage
3	**Major**	It is often an error in the main functionality of the program
4	**Minor**	It may be an insignificant problem of the program functioning
5	**Cosmetic**	As a rule, such errors are found in course of **user interface testing**; it may be a wrong size of a button, too bright color of an object and so on. Errors of this type have little impact on the program functioning

7.0 Approvals

Name (Print)	Signature	Date
1.		
2.		
3.		
4.		
5.		