CENTURYLINK
EIS SERVICES VERIFICATION TEST PLAN

CDRL 36

November 4, 2016

Qwest Government Services, Inc. dba CenturyLink QGS

4250 N Fairfax Drive, Suite 300

Arlington, VA 22203

REVISION HISTORY

Revision Number	Revision Date	Revision Description	Revised by

TABLE OF CONTENTS

LIST OF TABLES

EIS SERVICES VERIFICATION TEST PLAN (L.30.2.4; E.2.2; F.2.1 CDRL 36; G.3.4)

1.0 TEST PLAN METHODOLOGY SUMMARY (E.2.2.1)

The CenturyLink EIS Services Verification Test Plan addresses the overall verification and acceptance testing approach and methodology for all proposed services. The methodology will:

- Assess requirements for government defined scenarios and identify additional scenarios based on categories of requirements defined for the services proposed by CenturyLink in RFP Section C
- Identify and define the testing techniques that are needed to ensure compliance with the verification and acceptance requirements
- Identify and describe industry standard tests with parameters, procedures, and acceptance criteria that are used for verification tests
- Define how test cases will be created into test books for each task order (TO), to ensure that all relevant tests can be created for each TO-defined service
- Define the sequence of tests by scenario with check points and fall-back test loops identified
- Define the test cases for each scenario by service
- Obtain approval of service verification process from the government.
- Execute tests
- Capture test data, provide test results reports and define the basis for test completion or retesting

2.0 TEST SCENARIOS (E.2.2.2 & E.2.2.2.1)

As described in ***Table 2.0.1***, CenturyLink has grouped EIS services test cases into seven test scenarios, five of which are detailed in this plan. If proposed for addition to EIS, CenturyLink will submit a test case (TS-03) for dark fiber. For TS-07, depending on the mix of services ordered based on TO requirements and the agency locations, test books will be prepared combining relevant TO-specific test cases by scenario.

Table 2.0.1. EIS Services Test Scenarios

Test Scenario#	RFP Sec#	Description	Acceptance Criteria
Service TS-01	C.2	Demonstrate that CenturyLink's Cloud Services are compliant with Federal Risk and Authorization Management Program (**FedRAMP**) requirements as defined. • http://cloud.cio.gov http://cloud.cio.gov/fedramp/csp • NIST.gov publications http://csrc.nist.gov/groups/SMA/ispab/documents/minutes/2013-06/ispab_june2013_goodrich.pdf	CenturyLink will provide FedRAMP certification and ensure that it is verified and accepted by GSA.
Service TS-02	G.8	Demonstrate that awarded services are delivered based on the Key Performance Indicators (**KPIs)** and Service Level Agreement (**SLAs)** defined.	CenturyLink will demonstrate that the service works properly according to KPIs defined in RFP Section C.2.
Service TS-03	C.2.1.6.1.4	Verification Testing of **Dark Fiber Services**	See RFP Section C.2.1.6.1.4 for acceptance criteria. < RESERVED—CenturyLink is not proposing Dark Fiber Services at this time.>
Service TS-04	C.2	Demonstrate the services are delivered based on the **Access and Interfaces**.	CenturyLink will demonstrate that the service works properly using each Access and Interface type ordered
Service TS-05	C.2	Demonstrate the services are delivered with required **Technical Capabilities.**	CenturyLink will demonstrate that the service works properly and supports each Technical Capability ordered
Service TS-06	C.2	Demonstrate the services are delivered with required **Features.**	CenturyLink will demonstrate that each ordered service works properly providing each Feature ordered
Service TS-07	Task Order Content	Demonstrate any Task Order (**TO)-specific requirement** is delivered	CenturyLink will demonstrate that any TO-specific requirement (that is not a variant of the previous 6 Test Scenarios) works properly <RESERVED awaiting Task Order Requirements>

In cases where a new AQL for an existing KPI accompanies a TO, a test case(s) will be added to the **Service TS-02** scenario. In cases where a new KPI accompanies the TO, a new test scenario, **Service TS-07,** will be created including a test case or cases for each new service level and performance standard (threshold) introduced.

3.0 TESTING TECHNIQUES

Table 3.0-1 shows the test techniques applied under CenturyLink's service test methodology. Each test case will be verified using one or more of four different techniques and will be applied depending upon the nature of the test case.

Table 3.0.1. EIS Test Techniques

Test Technique	Application	Expected Outcome for Verified Requirement	Remarks	Example
Analysis (A):	Used when compliance with requirements is determined by models or by interpreting results using established principles.	Defining data parameters for use as the basis to determine if a requirement is met.	Partial data will be extrapolated to determine whether the defined success criteria has been met.	A network's performance might be analyzed by running simulations using a subset of agency locations.
Demonstration (D):	Run at least one test to demonstrate the ability to meet required AQL without special test equipment or instrumentation.	Instantiation of the requirements is validated by observing the item in operation	Defined success criteria actions show successful verification by demonstration. An agency has the ability to download service data in prescribed formats.	The tester would be able to choose the appropriate download options and then receive the data in the formats selected.
Inspection (I):	Using one of the assessor's senses to determine if a requirement is met.	The existence of documentation or other proof that the requirement is met.	An inspection can be conducted to show completed pre-delivery preparations for the delivery site, site security, or storage facilities.	A review of a documented network and service related equipment (SRE) escalation path for IPVS-Managed LAN Service
Measurement (M):	Use of test equipment or instrumentation to collect systems data.	The results reported by the test equipment or instrumentation satisfy the AQLs of the requirements.	Collected data is used in its raw form to determine acceptance.	If the data collected involve further analysis, the test type is the analysis. measurement technique most often applied to KPIs.

4.0 KPI VERIFICATION TESTS

CenturyLink will test performance of EIS services using a standard set of the seven KPIs defined in RFP Section C.1.8.3:

1. Availability (Service) (Av(S))
2. Time to Restore (TTR)
3. Grade of Service (Service) (GOS(S))
4. Latency (Service) (Latency(S))
5. Jitter
6. Event Notification (EN)
7. Response Time (RT)

1. Availability (Av[S])—Av(s) is a time-bound test using the following formula:

$$Av(S) = \frac{RI(HR) - COT(HR)}{RI(HR)} \times 100$$

Unavailability is defined on a service-by-service basis and is the amount of time the service (e.g., VPNS, ETS, IPS, IPVS, CCS, IaaS, PaaS, SaaS, CDNS, UCS, and MSS) is unavailable to users, the amount of time the port (e.g., MTIPS) is not available to users, or when the service experiences measurable degradation(e.g., quantity of consecutive severely errored seconds (SES) for Optical Wavelength Service (OWS) and Private Line Service (PLS)) to a point beneath the minimum acceptable performance threshold.

Service availability for most services will be measured when established access and interfaces exhibit stable operation and each required technical capability and feature has been fully operational for a 24 hour period.

For all services where unavailability is measured as the quantity of time where service is not available to users, this duration will be measured in terms of trouble ticket duration (ticket opened to ticket closed).

For the services where unavailability is defined by the incidence of consecutive SES, the test will capture the time that SES has exceeded the allowed allocation (ten consecutive SES) until the point where there are no SES outcomes for ten consecutive seconds.

2. Time to Restore (TTR)—This is a time-bounded test that measures the time required to restore lost or degraded service. There are two basic versions of this test: with dispatch and without dispatch. TTR will be tested by inducing a fault (advance site notification is required); isolating the test site as part of the test program; exercising the trouble management process; completing the restoration and closing the ticket. To ensure test validity, these activities will be unannounced to the network operations center (NOC), dispatch and any technical resources supporting the process. TTR with dispatch will be tested at selected service demonstration sites (as set forth in Section

6.0) and TTR without dispatch at all other ordered sites (see further order of operation details in Section 6.0 below).

TTR With Dispatch—In addition to the requirements tested in the TTR without dispatch test, the TTR with dispatch test requires that a technician is available to respond to the site within eight hours. For TTR with dispatch tests, at a site (previously selected during testing plan development and subject to prior agency review and approval), we will induce a fault, and after the service has been restored, measure the time between opening and closing the trouble ticket. Key finding: Timely site response and effective problem resolution by a dispatched technician.

TTR Without Dispatch—Trouble management processes and procedures will be tested—ensuring resources are available and our staff is trained to resolve a service outage back to the AQL window within four hours. To conduct this test we will induce the fault at a select site and after the service has been restored, measure the time between opening and closing the trouble ticket. For this test the CenturyLink technician who induced the fault will assume the role of the on-site customer and respond to the fault repair instructions.

3. Grade of Service (GOS(S))—GOS performance standards vary between EIS service types. CenturyLink will perform the following tests to validate the individual service-specific AQLs for GOS.

ETS, IPS, IPVS GOS tests—these are frame or packet loss tests and will be accomplished with Y.1731 or Internet control message protocol (ICMP) and RFC 5357 two-way active measurement protocol (TWAMP) tests, for Ethernet and IP services, respectively. Analysis of the resulting report of quantity of packets lost will confirm that at least 99.99% of the packets sent are returned to the sending location. In the case of IPVS, since there is only a routine service level, analysis of this data will ensure that at least 99.6% of the packets sent to each CONUS location arrive.

OWS GOS—This test demonstrates that protection switching on 1+1 OWS occurs and traffic successfully reroutes within a set time ($\leq$ 60 or $\leq$ 100 ms). The actual tests will be dependent on the specific agency requirements and SRE selected in the TO.

CDNS GOS—this test will demonstrate that content can be been refreshed in five minutes or less. At the direction of the test director, test content, pre-identified in the test case, will be added to existing content on agency servers and will be examined with a common web browser to confirm delivery of the revised content within five minutes. At the completion of the test (and verification of successful content refresh), the test content will be removed from agency content, again proving a refresh has successfully occurred within the allotted timeframe.

MTIPS GOS—There are four types of GOS tests for MTIPS: failover time, monitoring and correlation, configuration/rule change, and virus protection updates and bug fixes.

- **Failover—**At the direction of the test director, the CenturyLink NOC will contact the EIS security operations center (SOC), establishing a bridge and creating a failure that simulates a whole portal going down on one of the trusted Internet connections (TICs). The time to successfully complete failover to an alternate TIC will be monitored, and confirmed to have occurred in one minute or less. Upon successful completion of this test, the SOC will restore all traffic to normal operation
- **Monitoring and Correlation—**The test director will simulate a security event(s) and confirm that the monitoring and correlation agents in the SOC have detected the event within four hours as evidenced by initiation of real time fusion
- **Configuration/Rule Change—**The test director will initiate a configuration/change request (which will have been pre-identified and marked as test content and “Urgent” in the test case book). It will be observed that the change occurred successfully within two hours of initiation
- **Virus Protection Updates & Bug Fixes—**a test virus protection update, labeled “Urgent,” will be deployed as initiated by the test director. The test content will be pre-identified in the test case book. It will be observed that the deployment occurred successfully within two hours of test initiation.

MSS GOS—Configuration/Rule Change—The test director will initiate a configuration/change request (which will have been pre-identified and marked as test content and “Urgent”) in the test case book). It will be observed that the change occurred successfully within two hours of initiation.

4. Latency (S)—The Latency test is performed measuring the average round trip transmission time between each agency’s premises router and the other agency routers on the network being tested. For this test, Y.1731, ICMP or TWAMP tests will be performed to capture the latency between each site pair, then confirm that the average latency between all the site pairs to verify that the actual latency meets the AQL requirement. A latency test will be performed for each TO service. In test cases involving site pairs separated by extended distances (typically networks having OCONUS sites), special care will be taken to validate results due to the limitations of the speed of light in fiber that will impact the round trip latency due to distance sensitivity.

5. Jitter—Jitter is a KPI that is required for two services (ETS and IPVS) and is tested by measuring the amount of variation in latency for a packet stream from one service delivery point (SDP) to another SDP. The jitter measurement will be performed using Y.1731, ICMP or TWAMP tests to capture the jitter between each site pair. These results will be analyzed to confirm that the variance of arrival time is equal to or less than 10ms in all cases. Variance of arrival time exceeding 10ms constitutes test failure.

6. Event Notification—Event notification tests are required to confirm AQLs for MTIPS, MSS and MMS services and are sub-divided by event categorization (low, medium, or high). Event notification tests measure the elapsed time between event detection and agency notification. These tests will measure objectives including: verification of sufficient resources with capability to correctly categorize the event (L/M/H) and methods; and procedures to notify the affected agency within the AQL threshold. For these tests, agency contacts will be notified by CenturyLink of the event and event categorization within the notification timeframe. Event simulation test planning process details will be agreed upon between the agency and CenturyLink for each TO implementation.

7. Response Time—Response time will be measured as part of TTR with dispatch testing. While the AQL will vary between services, the methodology for performing the monitoring is the same from service to service.

5.0 TEST CASE BOOKS

The EIS test plan includes a test case for every KPI, access and interface type, technical capability, and feature proposed by CenturyLink. Upon receipt of a TO, the CenturyLink Technical Support Team (TST), reporting to the EIS PMO Service Assurance Manager, will perform an analysis of the testing that will be required. TST will prepare a TO-specific test case book, build a TO-specific planning tool and select a relevant test case(s) from each test scenario for each ordered services.

As part of this analysis, the TST will determine if there are new requirements creating the need for a new test scenario with new TO prescribed AQLs for one or more existing KPIs. In this case, a new test scenario will be added to the test plan where the existing scenarios do not address the new test requirement. If only new AQLs are added, individual test cases will be added to the appropriate existing scenario.

A distance and service matrix will be built, showing the community of services (which ordered services are required at each specific agency location). Additionally, the line-of-sight distance between each agency location in the TO will be documented. This information will be used to minimize the quantity of tests, while ensuring each ordered service capability is tested to ensure performance meets or exceeds the required design intent. This information will be site task input for implementation planning.

The master listing of test scenarios and their subtending test cases will be filtered as follows:

- From Scenario TS-01, select FedRAMP accreditation documentation only for TO-Specified Cloud services
- From Scenario TS-02, select those cases to be used to test TO-specific KPI/AQL performance
- From Scenario TS-04, select those cases to be used to test TO-specific Access Types and Interface rates

- From Scenario TS-05, select those cases to be used to test TO-specific Technical Capabilities
- From Scenario TS-06, select those cases to be used to test TO-specific Features
- Scenario TS-07 test cases will be added as needed to support TOs

From this collection of test cases shown above, the test book will be further filtered to select which cases will be performed at TO-identified agency locations. The TST will finalize the test cases to be performed at each site (and between sites) to ensure all tests are allocated to the appropriate sites and that site-specific testing activity is included in the TO implementation schedule.

6.0 SERVICES TESTING—ORDER OF OPERATION

Testing of EIS services will be scheduled with check points and fall-back schedule loops planned to ensure all testing for a site is done on an empirical basis. As part of the implementation planning process, acceptance testing will be performed to ensure all services and service features will be tested and acceptable to the government, unless specified otherwise in the TO. Testing will be scheduled to ensure full testing of every ordered feature and capability. Service testing validates the overarching architecture and design of agency-specific configurations in accordance with the requirements of RFP Section G.3.4. Site-specific acceptance testing will also be conducted for installed services and features at all sites as they are activated in accordance with the requirements in RFP Section G.3.3.3.3 item 11 to ensure that all capabilities at all sites are verified to the government's satisfaction.

The predecessor/successor TO is generally as follows:

- Schedule delivery of security compliance (FedRAMP) documents to the Contracting Officer (CO)/Contracting Officer's Technical Representative (COTR) for any ordered Cloud service.

  Milestone > Security certification has been validated

- Schedule test cases for access testing and for Interface testing. These would be completed, including fall back, repair and retest as required until access at the select set of service demonstration sites, representing each ordered interface

and speed, are proven to work to design intent.

Milestone > One or more examples of each ordered access and Interface is in place and exhibits stable operation

- Schedule testing of each ordered technical capability and feature at the representative service demonstration sites to ensure that each works to design intent, including fall-back, repair and revalidation as required.

  Milestone > Access and interfaces are in place, exhibit stable operation, and each required technical capability and feature works to design intent, meeting its individual technical requirement

- Schedule testing of network KPIs: jitter, Av(S), latency (S), and GOS(S) at the service demonstration sites. These four types of tests require testing to measure performance over time, and should not occur until the site pairs required for the tests are implemented and previous tests are completed.

  Milestone > Required sites (including all access, interfaces, technical capabilities and features) are in place and stable, and the network performance in terms of jitter, availability, latency, and GOS have been tested for a set period of time and found to be performing to AQL or better

- Schedule testing of network management related performance at the service demonstration sites: EN, TTR, and RT. These three KPIs measure response times of personnel to events/outages and will be performed by those groups responsible in the event.

  Milestone > With all access and interfaces in place, all capabilities and feature working as intended, and the performance of the network meeting all AQLs, prove that these three functions work to design intent (all happen within allotted permissible timeframes)

- Schedule acceptance testing of all other ordered agency sites, accepting each on the basis of proven success of the KPI tests required for each service ordered at the site.

  Milestone > Finish bringing all sites onto the ordered network with all services

and performance operating in accordance with all technical requirements and to design intent

7.0 TEST CASES (E.2.2.3)

This section describes the test cases by scenario that will be applied against each TO as appropriate. Each test case has an ID that provides an intelligent identifier to show which scenario it is used for. The format for this ID is: TS-XX-AA where XX is the scenario number and AA is the ordinal test case number within that scenario. The ordinality of AA is based on the sequence of services in Section C of the RFP, so if a service is not proposed by CenturyLink at this time, that number will be skipped and reserved for such time CenturyLink may bid that service.

For the five test scenarios for initial CenturyLink EIS services (S-TS-01 for Cloud Security Accreditations, S-TS-02 for Service (KPI/SLA) Performance, S-TS-04 for Access and Interfaces, S-TS-05 for Technical Capabilities, and S-TS-06 for Features), the tables in Section 7.0 show the identity and desired outcome for each test case.

7.1 TS-01 Test Cases

The test cases for test scenario 1 (TS-01, Cloud Security Accreditation) are contained ***Table 7.1***.

Table 7.1. TS-01 Test Cases

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-01-01.1	Demonstrate FedRAMP Compliance—IaaS	C.2	I	Provide Compliance documentation.
TS-01-02.1	Demonstrate FedRAMP Compliance—PaaS	C.2	I	Provide Compliance documentation.
TS-01-03.1	Demonstrate FedRAMP Compliance—SaaS	C.2	I	Provide Compliance documentation.
TS-01-04.1	Demonstrate FedRAMP Compliance—CDNS	C.2	I	Provide Compliance documentation.

7.2 TS-02 Test Cases

The test cases for test scenario 2 (TS-02, KPI/SLA Performance) are contained in ***Table 7.2***

Table 7.2. TS-02 Test Cases

Test Case ID	Test Case Description	Requirements References	A, D. I or M	Expected Output(s)
TS-02-01.1	Routine Latency (CONUS)—VPNS	C.2.1.1.4	M	CONUS Latency $\leq$ 70 ms
TS-02-01.2	Routine Latency (OCONUS)—VPNS	C.2.1.1.4	M	OCONUS Latency $\leq$ 150 ms
TS-02-01.3	Routine Availability (VPN)—VPNS	C.2.1.1.4	A	Availability $\geq$ 99.9%
TS-02-01.4	Critical Availability (VPN)—VPNS	C.2.1.1.4	A	Availability $\geq$ 99.99%
TS-02-01.5	Time to Restore w/o Dispatch—VPNS	C.2.1.1.4	D	Restoration $\leq$ 4 hours
TS-02-01.6	Time to Restore with Dispatch—VPNS	C.2.1.1.4	D	Restoration $\leq$ 8 hours
TS-02-02.1	Routine Availability (Single Connection)—ETS	C.2.1.2.4	A	Availability $\geq$ 99.9%
TS-02-02.2	Critical Availability (Double Connection)—ETS	C.2.1.2.4	A	Availability $\geq$ 99.99%
TS-02-02.3	Latency (CONUS)—ETS	C.2.1.2.4	M	CONUS Latency $\leq$ 100 ms
TS-02-02.4	Latency (OCONUS)—ETS	C.2.1.2.4	M	OCONUS Latency $\leq$ 200 ms
TS-02-02.5	Routine GOS (Packet Delivery)—ETS	C.2.1.2.4	M	Packet Delivery $\geq$ 99.95% throughout test

Test Case ID	Test Case Description	Requirements References	A, D. I or M	Expected Output(s)
TS-02-02.6	Critical GOS (Packet Delivery)—ETS	C.2.1.2.4	M	Packet Delivery ≥ 99.99% throughout test
TS-02-02.7	Time to Restore w/o Dispatch—ETS	C.2.1.2.4	D	Restoration ≤ 4 hours
TS-02-02.8	Time to Restore with Dispatch—ETS	C.2.1.2.4	D	Restoration ≤ 8 hours
TS-02-02.9	Routine GOS (Fail Over Time)—ETS	C.2.1.2.4	M	1 minute
TS-02-02.10	Critical GOS (Fail Over Time)—ETS	C.2.1.2.4	M	≤ 100 ms
TS-02-03.1	Routine Availability (over WDM)—OWS	C.2.1.3.4	A	Availability ≥ 99.9%
TS-02-03.2	Critical Availability (over WDM)—OWS	C.2.1.3.4	A	Availability ≥ 99.99%
TS-02-03.3	Time to Restore w/o Dispatch—OWS	C.2.1.3.4	D	Restoration ≤ 4 hours
TS-02-03.4	Time to Restore with Dispatch—OWS	C.2.1.3.4	D	Restoration ≤ 8 hours
TS-02-03.5	Routine GOS (Restoration Time)—OWS	C.2.1.3.4	M	Reroute traffic ≤ 100 ms
TS-02-03.6	Critical GOS (Restoration Time)—OWS	C.2.1.3.4	M	Reroute traffic ≤ 60 ms
TS-02-04.1	Routine Availability (POP-to-POP)—PLS	C.2.1.4.4	A	Availability ≥ 99.9%
TS-02-04.2	Critical Availability (POP-to-POP)—PLS	C.2.1.4.4	A	Availability ≥ 99.99%
TS-02-04.3	Routine Availability (SDP-to-SDP)—PLS	C.2.1.4.4	A	Availability ≥ 99.9%
TS-02-04.4	Critical Availability (SDP-to-SDP)—PLS	C.2.1.4.4	A	Availability ≥ 99.99%
TS-02-04.5	Time to Restore w/o Dispatch—PLS	C.2.1.4.4	D	Restoration ≤ 4 hours
TS-02-04.6	Time to Restore with Dispatch—PLS	C.2.1.4.4	D	Restoration ≤ 8 hours
TS-02-07.1	Routine Availability (Port)—IPS	C.2.1.7.4	A	Availability ≥ 99.95%
TS-02-07.2	Critical Availability (Port)—IPS	C.2.1.7.4	A	Availability ≥ 99.995%
TS-02-07.3	Routine Latency (CONUS)—IPS	C.2.1.7.4	M	CONUS Latency ≤ 60 ms
TS-02-07.4	Critical Latency (CONUS)—IPS	C.2.1.7.4	M	CONUS Latency ≤ 50 ms
TS-02-07.5	Routine GOS (Data Delivery Rate)—IPS	C.2.1.7.4	M	Data Delivery ≥ 99.9% throughout test
TS-02-07.6	Critical GOS (Data Delivery Rate)—IPS	C.2.1.7.4	M	Data Delivery ≥ 99.99% throughout test
TS-02-07.7	Time to Restore w/o Dispatch—IPS	C.2.1.7.4	D	Restoration ≤ 4 hours
TS-02-07.8	Time to Restore with Dispatch—IPS	C.2.1.7.4	D	Restoration ≤ 8 hours
TS-02-08.1	Routine Latency—IPVS	C.2.2.1.4	M	Latency ≤ 200 ms
TS-02-08.2	Routine GOS (Packet Loss)—IPVS	C.2.2.1.4	M	Dropped Packets ≤ 0.4%

Test Case ID	Test Case Description	Requirements References	A, D. I or M	Expected Output(s)
TS-02-08.3	Routine Availability—IPVS	C.2.2.1.4	A	Availability ≥ 99.6%
TS-02-08.4	Critical Availability—IPVS	C.2.2.1.4	A	Availability ≥ 99.9%
TS-02-08.5	Routine Jitter—IPVS	C.2.2.1.4	M	Average delay variation ≤ 10 ms
TS-02-08.6	Routine Voice Quality—IPVS	C.2.2.1.4	I	Mean Opinion Score ≥ 4.0
TS-02-08.7	Time to Restore w/o Dispatch—IPVS	C.2.2.1.4	D	Restoration ≤ 4 hours
TS-02-08.8	Time to Restore with Dispatch—IPVS	C.2.2.1.4	D	Restoration ≤ 8 hours
TS-02-09.1	POP-to-POP Availability—CSVS	C.2.2.2.4	A	Availability ≥ 99.95%
TS-02-09.2	SDP-to-SDP Availability—CSVS	C.2.2.2.4	A	Availability ≥ 99.95%
TS-02-09.3	Time to Restore w/o Dispatch—CSVS	C.2.2.2.4	D	Restoration ≤ 4 hours
TS-02-09.4	Time to Restore with Dispatch—CSVS	C.2.2.2.4	D	Restoration ≤ 8 hours
TS-02-09.5	Routine GOS (Call Blockage SDP-to-SDP) —CSVS	C.2.2.2.4	M	Calls not complete < 0.07
TS-02-09.6	Routine GOS (Call Blockage (POP-to-POP) —CSVS	C.2.2.2.4	M	Calls not complete < 0.01
TS-02-09.7	Critical GOS (Call Blockage) —CSVS	C.2.2.2.4	M	Calls not complete < 0.01
TS-02-12.1	Critical Availability (Internet)—CHS	C.2.4.5.1	A	Availability ≥ 99.99%
TS-02-12.2	Time to Restore w/o Dispatch—CHS	C.2.4.5.1	D	Restoration ≤ 4 hours
TS-02-13.1	Routine Availability (IaaS Cloud Service)—IaaS	C.2.5.1.4	A	Availability ≥ 99.95%
TS-02-13.2	Time to Restore w/o Dispatch—IaaS	C.2.5.1.4	D	Restoration ≤ 4 hours
TS-02-13.3	Time to Restore with Dispatch—IaaS	C.2.5.1.4	D	Restoration ≤ 8 hours
TS-02-14.1	Routine Availability (PaaS Cloud Service)—PaaS	C.2.5.2.4	A	Availability ≥ 99.95%
TS-02-14.2	Time to Restore w/o Dispatch—PaaS	C.2.5.2.4	D	Restoration ≤ 4 hours
TS-02-14.3	Time to Restore with Dispatch—PaaS	C.2.5.2.4	D	Restoration ≤ 8 hours
TS-02-15.1	Routine Availability (IaaS Cloud Service)—SaaS	C.2.5.3.4	A	Availability ≥ 99.95%
TS-02-15.2	Time to Restore w/o Dispatch—SaaS	C.2.5.3.4	D	Restoration ≤ 4 hours
TS-02-15.3	Time to Restore with Dispatch—SaaS	C.2.5.3.4	D	Restoration ≤ 8 hours
TS-02-16.1	Routine Availability (CDNS network)—CDNS	C.2.5.4.4	A	Availability ≥ 99.99%
TS-02-16.2	Routine GOS (Time to refresh content)—CDNS	C.2.5.4.4	M	Content Refresh ≤ 5 minutes
TS-02-16.3	Time to Restore w/o Dispatch—CDNS	C.2.5.4.4	D	Restoration ≤ 4 hours

Test Case ID	Test Case Description	Requirements References	A, D. I or M	Expected Output(s)
TS-02-16.4	Time to Restore with Dispatch—CDNS	C.2.5.4.4	D	Restoration ≤ 8 hours
TS-02-19.1	Routine Availability—UCS	C.2.8.3.4	A	Availability ≥ 99.5%
TS-02-19.2	Time to Restore w/o Dispatch—UCS	C.2.8.3.4	D	Restoration ≤ 4 hours
TS-02-19.3	Time to Restore with Dispatch—UCS	C.2.8.3.4	D	Restoration ≤ 8 hours
TS-02-20.1	Routine Availability (TIC Portal)—MTIPS Portal	C.2.8.4.4	A	Availability ≥ 99.5%
TS-02-20.2	Routine GOS (Failover Time)—MTIPS Portal	C.2.8.4.4	M	Failover ≤ 1 minute
TS-02-20.3	Routine GOS (Monitoring & Correlation)—MTIPS Portal	C.2.8.4.4	M	Detect event ≤ 4 hours 90% of the time
TS-02-20.4	Critical GOS (Monitoring & Correlation)—MTIPS Portal	C.2.8.4.4	M	Detect event ≤ 4 hours 99.9% of the time
TS-02-20.5	Routine GOS (Config Rule Change Normal)—MTIPS Portal	C.2.8.4.4	M	Change completed ≤ 5 hours
TS-02-20.6	Routine GOS (Config Rule Change Urgent)—MTIPS Portal	C.2.8.4.4	M	Change completed ≤ 2 hours
TS-02-20.7	Routine EN Low (Firewall Security EN)—MTIPS Portal	C.2.8.4.4	M	Time to notification ≤ 24 hours
TS-02-20.8	Routine EN Med (Firewall Security EN)—MTIPS Portal	C.2.8.4.4	M	Time to notification ≤ 4 hours
TS-02-20.9	Routine EN High (Firewall Security EN)—MTIPS Portal	C.2.8.4.4	M	Time to notification ≤ 30 minutes
TS-02-20.10	Routine EN Low (Intrusion Detection EN)—MTIPS Portal	C.2.8.4.4	M	Time to notification ≤ 24 hours
TS-02-20.11	Routine EN High (Intrusion Detection EN)—MTIPS Portal	C.2.8.4.4	M	Time to notification ≤ 10 minutes
TS-02-20.12	Routine GOS Normal (Protection Updates & Bug Fixes) Portal	C.2.8.4.4	M	Time to patch deployment ≤ 24 hours
TS-02-20.13	Routine GOS Urgent (Protection Updates & Bug Fixes) Portal	C.2.8.4.4	M	Time to patch deployment ≤ 2 hours
TS-02-20.14	Routine Availability (Port)—MTIPS TC&D	C.2.8.4.4.2	A	Availability ≥ 99.95%
TS-02-20.15	Critical Availability (Port)—MTIPS TC&D	C.2.8.4.4.2	A	Availability ≥ 99.995%
TS-02-20.16	Routine Latency (CONUS)—MTIPS TC&D	C.2.8.4.4.2	M	Latency ≤ 60 ms
TS-02-20.17	Critical Latency (CONUS)—MTIPS TC&D	C.2.8.4.4.2	M	Latency ≤ 50 ms
TS-02-20.18	Routine GOS (Data Delivery Rate)—MTIPS TC&D	C.2.8.4.4.2	M	Successful delivery ≥ 99.95%
TS-02-20.19	Critical GOS (Data Delivery Rate)—MTIPS TC&D	C.2.8.4.4.2	M	Successful delivery ≥ 99.995%
TS-02-20.20	Time to Restore w/o Dispatch—MTIPS TC&D	C.2.8.4.4.2	D	Restoration ≤ 4 hours
TS-02-20.21	Time to Restore with Dispatch—MTIPS TC&D	C.2.8.4.4.2	D	Restoration ≤ 8 hours
TS-02-20.22	Routine EN (Security Incident Reporting)—MTIPS TC&D	C.2.8.4.4.2	M	Report to CERT ≤ 30 minutes
TS-02-21.1	Routine Availability—MSS	C.2.8.5.4	A	Availability ≥ 99.5%

Test Case ID	Test Case Description	Requirements References	A, D. I or M	Expected Output(s)
TS-02-21.2	Routine EN (MPS)—MSS	C.2.8.5.4	M	Notification ≤ 10 minutes
TS-02-21.3	Routine EN Low (INRS)—MSS	C.2.8.5.4	M	Notification ≤ next business day of 24 hours
TS-02-21.4	Routine EN Medium (INRS)—MSS	C.2.8.5.4	M	Notification ≤ 4 hours
TS-02-21.5	Routine EN High (INRS)—MSS	C.2.8.5.4	M	Notification ≤ 1 hour
TS-02-21.6	Routine GOS (Config Change, Protection Update, Normal)—MSS	C.2.8.5.4	M	Change completed ≤ 5 hours (MPS) and ≤ 24 Hours (VSS)
TS-02-21.7	Routine GOS (Config Change, Protection Update, Urgent)—MSS	C.2.8.5.4	M	Change completed ≤ 2 hours (all)
TS-02-21.8	Routine Incidence Response Time Low (Telephone)—MSS	C.2.8.5.4	D	Time to implement ≤ 1 hour
TS-02-21.9	Routine Incidence Response Time High (Telephone)—MSS	C.2.8.5.4	D	Time to implement ≤ 15 minutes
TS-02-21.10	Routine Incidence Response Time Low (On-Site)—MSS	C.2.8.5.4	D	Arrival in site ≤ 36 hours
TS-02-21.11	Routine Incidence Response Time High (On-Site)—MSS	C.2.8.5.4	D	Arrival in site ≤ 24 hours
TS-02-21.12	Time to Restore w/o Dispatch—MSS	C.2.8.5.4	D	Restoration ≤ 4 hours
TS-02-21.13	Time to Restore with Dispatch—MSS	C.2.8.5.4	D	Restoration ≤ 8 hours
TS-02-25.1	Performance - IPSS	C.2.8.9.4	tbd	“Performance metrics for this service will be defined in the TO.”

7.3 TS-03 Test Cases <RESERVED>

<RESERVED>

7.4 TS-04 Test Cases

The test cases for test scenario 4 (TS-04, Access and Interfaces) are contained in ***Table 7.4.***

Table 7.4. TS-04 Test Cases

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-04-01.1	Ethernet Interface—VPNS	C.2.1.1.3	D	IPv4/v6 over Ethernet works for speeds 1 Mbps up to 10/40/100 Gbps IAW TO
TS-04-01.2.1	PLS @ DS0—VPNS	C.2.1.1.3	D	IPv4/v6 over PLS works with DS0 Interface

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-04-01.2.2	PLS @ T1—VPNS	C.2.1.1.3	D	IPv4/v6 over PLS works with T1 Interface
TS-04-01.2.3	PLS @ T3—VPNS	C.2.1.1.3	D	IPv4/v6 over PLS works with T3 Interface
TS-04-01.2.4	PLS @ OC-3c—VPNS	C.2.1.1.3	D	IPv4/v6 over PLS works with OC-3c Interface
TS-04-01.2.5	PLS @ OC-12c—VPNS	C.2.1.1.3	D	IPv4/v6 over PLS works with OC-12c Interface
TS-04-01.2.6	PLS @ OC-48c—VPNS	C.2.1.1.3	D	IPv4/v6 over PLS works with OC-48c Interface
TS-04-01.2.7	PLS @ OC-192c—VPNS	C.2.1.1.3	D	IPv4/v6 over PLS works with OC-192c Interface
TS-04-01.2.8	PLS @ OC-768c—VPNS	C.2.1.1.3	D	IPv4/v6 over PLS works with OC-768c Interface
TS-04-01.3.1	SONET @ OC-3c—VPNS	C.2.1.1.3	D	IP/PPP over SONET works with OC-3c Interface
TS-04-01.3.2	SONET @ OC-12c—VPNS	C.2.1.1.3	D	IP/PPP over SONET works with OC-12c Interface
TS-04-01.3.3	SONET @ OC-48c—VPNS	C.2.1.1.3	D	IP/PPP over SONET works with OC-48c Interface
TS-04-01.3.4	SONET @ OC-192c—VPNS	C.2.1.1.3	D	IP/PPP over SONET works with OC-192c Interface
TS-04-01.3.5	SONET @ OC-768c—VPNS	C.2.1.1.3	D	IP/PPP over SONET works with OC-768c Interface
TS-04-01.4	DSL @ 1.5 to 6 Mbps Up and 384 Kbps to 50 Mbps Down—VPNS	C.2.1.1.3	D	P-to-P Protocol, IPv4/v6 over DSL with uplink and downlink IAW TO
TS-04-01.5	Cable High Speed Access @ 320 Kbps up to 150 Mbps—VPNS	C.2.1.1.3	D	P-to-P Protocol, IPv4/v6 over Cable with speed IAW TO
TS-04-01.6.1	Wi-Fi Wireless Access—VPNS	C.2.1.1.3	D	P-to-P Protocol, IPv4/v6 works over WiFi Interface
TS-04-01.6.2	LTE Wireless Access—VPNS	C.2.1.1.3	D	P-to-P Protocol, IPv4/v6 works over LTE Interface
TS-04-01.6.3	Satellite Wireless Access—VPNS	C.2.1.1.3	D	P-to-P Protocol, IPv4/v6 works over Satellite Interface
TS-04-02.1	Optical (1310 nm fiber, 1.25 Gbps, Gigabit Ethernet)—ETS	C.2.1.2.3	D	ETS over 1310 nm/1.25 Gbps/GigE UNI
TS-04-02.2	Optical (850 nm fiber, 1.25 Gbps, Gigabit Ethernet)—ETS	C.2.1.2.3	D	ETS over 850 nm/1.25 Gbps/GigE UNI
TS-04-02.3	Optical (1310 nm fiber, 100 Mbps, Fast Ethernet)—ETS	C.2.1.2.3	D	ETS over 1310 nm/100 Mbps/Fast Ethernet UNI
TS-04-02.4	Optical (optional) (1310 nm, 10/40/100 Gbps, 10/40/100GBASE-SR (65 meters))—ETS	C.2.1.2.3	D	ETS with Optical (1310 nm @10/40/100 Gbps @10/40/100GBASE-SR (65 meters))
TS-04-02.5	Optical (optional) (850nm, 10/40/100 Gbps, 10/40/100GBASE-SW)—ETS	C.2.1.2.3	D	ETS with Optical (850nm @10/40/100 Gbps @10/40/100GBASE-SW)
TS-04-02.6	Optical (optional) (1550 nm, 10/40/100 Gbps, 10/40/100GBASE-ER)—ETS	C.2.1.2.3	D	ETS with Optical (1550 nm @10/40/100 Gbps @10/40/100GBASE-ER)
TS-04-02.7	Optical (optional) (1310 nm, 10/40/100 Gbps, 10/40/100GBASE-LR	C.2.1.2.3	D	ETS with Optical (1310 nm @10/40/100 Gbps @10/40/100GBASE-

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
	)—ETS			LR)
TS-04-02.8	Optical (optional) (1550 nm, 10/40/100 Gbps, 10/40/100GBASE-LW)—ETS	C.2.1.2.3	D	ETS with Optical (1550 nm @10/40/100 Gbps @10/40/100GBASE-LW)
TS-04-02.9	Optical (optional) (1300 nm Multimode, 10/40/100 Gbps, CWDM 10/40/100GBASE-LX4 (300 meters))—ETS	C.2.1.2.3	D	ETS with Optical (1300 nm Multimode @10/40/100 Gbps, CWDM 10/40/100GBASE-LX4 (300 meters))
TS-04-02.10	Optical (optional) (1310 nm Single Mode, 10/40/100 Gbps, CWDM 10/40/100GBASE-LX4 (10,000 meters))—ETS	C.2.1.2.3	D	ETS with Optical (1310 nm Single Mode @10/40/100 Gbps, CWDM 10/40/100GBASE-LX4 (10,000 meters))
TS-04-02.11	Optical (optional) (1310 nm Single Mode, 10/40/100 Gbps, 10/40/100GBASE-LW (10,000 Meters))—ETS	C.2.1.2.3	D	ETS with Optical (1310 nm Single Mode @10/40/100 Gbps @10/40/100GBASE-LW (10,000 Meters))
TS-04-02.12	Optical (optional) (1550 nm Single Mode, 10/40/100 Gbps, 10/40/100GBASE-EW (40,000 meters))—ETS	C.2.1.2.3	D	ETS with Optical (1550 nm Single Mode @10/40/100 Gbps @10/40/100GBASE-EW (40,000 meters))
TS-04-02.13	Electrical (optional) (N/A, 10 Mbps, 10Base)—ETS	C.2.1.2.3	D	ETS with Electrical @ 10 Mbps, 10Base
TS-04-02.14	Electrical (N/A, 100 Mbps, 100 Base)—ETS	C.2.1.2.3	D	ETS with Electrical @100 Mbps, 100 Base
TS-04-02.15	Optical (1 Gbps, 1000Base)—ETS	C.2.1.2.3	D	ETS with Optical @ 1 Gbps, 1000Base
TS-04-02.16	Optical (optional) (1300 nm, STM-4, SDH STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4)—ETS	C.2.1.2.3	D	ETS with Optical (1300 nm, STM-4, SDH STM-1, VC-11 (DS1), VC-12 (E1), VC-3 (DS3, E3, other), VC-4)
TS-04-02.17	Optical (Optional) (1300 nm, STM-4c, VC-4-4c)—ETS	C.2.1.2.3	D	ETS with Optical (1300 nm, STM-4c, VC-4-4c)
TS-04-02.18	Optical (Multimode, 1 Gbps, 1000BASE-LX)—ETS	C.2.1.2.3	D	ETS with Optical (Multimode @ 1 Gbps, 1000BASE-LX
TS-04-02.19	Optical (Multimode, 1 Gbps, 1000BASE-SX)—ETS	C.2.1.2.3	D	ETS with Optical (Multimode @ 1 Gbps, 1000BASE-SX
TS-04-02.20	Electrical (Copper) (optional) (N/A, 1 Gbps, 1000BASE-CX)—ETS	C.2.1.2.3	D	ETS with Electrical (Copper) @ 1 Gbps, 1000BASE-CX
TS-04-02.21	Electrical (Twisted Pair) (Optional) (N/A, 1 Gbps, 1000BASE-T)—ETS	C.2.1.2.3	D	ETS with Electrical (Twisted Pair) @ 1 Gbps, 1000BASE-T
TS-04-02.22	Optical (optional) (1310 nm, 10/40 Gbps, SONET or SDH)—ETS	C.2.1.2.3	D	ETS with Optical (1310 nm @10/40 Gbps, SONET or SDH)
TS-04-03.1	Optical (1310 nm, 2.5Gpbs, SONET or SDH)—OWS	C.2.1.3.3	D	OWS works over SONET or SDH @ 1310 nm/2.5Gpbs,
TS-04-03.2	Optical (1310 nm, 2.5Gbps, SONET or SDH Concatenated)—OWS	C.2.1.3.3	D	OWS works over SONET or SDH Concatenated @ 1310 nm/2.5Gpbs,
TS-04-03.3	Optical (1310 nm, 10Gbps, SONET or SDH)—OWS	C.2.1.3.3	D	OWS works over SONET or SDH @ 1310 nm/10Gpbs,
TS-04-03.4	(optional)—Optical (over 12 fibers) (850 nm, 10 Gbps (12 fibers), SONET or SDH)—OWS	C.2.1.3.3	D	OWS works over SONET or SDH @ 850 nm/10 Gbps (12 fibers)

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-04-03.5	(optional)—Optical (over 1 fiber) (1310nm, 10 Gbps (1 fiber), SONET or SDH)—OWS	C.2.1.3.3	D	OWS works over SONET or SDH @ 1310nm/10 Gbps (1 fiber)
TS-04-03.6	(optional)—Optical (over 4 fibers) (850nm, 10 Gbps (4 fibers), SONET or SDH)—OWS	C.2.1.3.3	D	OWS works over SONET or SDH @ 850nm/10 Gbps (4 fibers)
TS-04-03.7	(optional)—Optical (over 1 fiber) (850 nm, 10 Gbps (1 fiber), SONET or SDH)—OWS	C.2.1.3.3	D	OWS works over SONET or SDH @ 850 nm/10 Gbps (1 fiber)
TS-04-03.8	(optional)—Optical (850 nm, 40 Gbps, SONET or SDH)—OWS	C.2.1.3.3	D	OWS works over SONET or SDH @850 nm/40 Gbps
TS-04-04.1	ITU-TSS V.35 (Up to 1.92 Mbps, Transparent)—PLS	C.2.1.4.3	D	PLS works up to 1.92 Mbps w/Transparent UNI
TS-04-04.2	EIA RS-449 (Up to 1.92 Mbps, Transparent)—PLS	C.2.1.4.3	D	PLS works up to 1.92 Mbps w/Transparent UNI
TS-04-04.3	EIA RS-232 (Up to 1.92 Kbps, Transparent)—PLS	C.2.1.4.3	D	PLS works up to 1.92 Mbps w/Transparent UNI
TS-04-04.4	EIA RS-530 (Up to 1.92 Mbps, Transparent)—PLS	C.2.1.4.3	D	PLS works up to 1.92 Mbps w/Transparent UNI
TS-04-04.5	T1 (with ESF), Up to 1.536 Mbps, Transparent—PLS	C.2.1.4.3	D	PLS works with T1 (w/ESF) up to 1.536 Mbps w/Transparent UNI
TS-04-04.6	T3, Up to 43.008 Mbps, Transparent—PLS	C.2.1.4.3	D	PLS works with T3 up to 43.008 Mbps w/Transparent UNI
TS-04-04.7	E1, Up to 1.92 Mbps, Transparent—PLS	C.2.1.4.3	D	PLS works with E1 up to 1.92 Mbps w/Transparent UNI
TS-04-04.8	E3, Up to 30.72 Mbps, Transparent—PLS	C.2.1.4.3	D	PLS works with E3 up to 30.72 Mbps w/Transparent UNI
TS-04-04.9	(Optional) (Optical: SONET OC-1, 49.536 Mbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with Optical interface w/SONET OC-1 @ 49.536 Mbps w/Transparent UNI
TS-04-04.10	(Optional) (Electrical: SONET STS-1/EC-1, 49.536 Mbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with Electrical Interface w/SONET STS-1/EC-1 @ 49.536 Mbps w/Transparent UNI
TS-04-04.11	(SONET OC-3, 148.608 Mbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with SONET OC-3 @148.608 Mbps w/Transparent UNI
TS-04-04.12	(SONET OC-3c, 148.608 Mbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with SONET OC-3c @148.608 Mbps w/Transparent UNI
TS-04-04.13	(SONET OC-12, 594.432 Mbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with SONET OC-12 @594.432 Mbps w/Transparent UNI
TS-04-04.14	(SONET OC-12c, 594.432 Mbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with SONET OC-12c @594.432 Mbps w/Transparent UNI
TS-04-04.15	(SONET OC-48, 2.377728 Gbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with SONET OC-48 @2.377728 Gbps w/Transparent UNI

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-04-04.16	(SONET OC-48c, 2.377728 Gbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with SONET OC-48c @2.377728 Gbps w/Transparent UNI
TS-04-04.17	(SONET OC-192, 9.510912 Gbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with SONET OC-192 @9.510912 Gbps w/Transparent UNI
TS-04-04.18	(SONET OC-192c, 9.510912 Gbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with SONET OC-192 @9.510912 Gbps w/Transparent UNI
TS-04-04.19	(Optional) (SONET OC-768, 38.486016 Gbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with SONET OC-768 @38.486016 Gbps w/Transparent UNI
TS-04-04.20	(Optional) (SONET OC-768c, 38.486016 Gbps, Transparent)—PLS	C.2.1.4.3	D	PLS works with SONET OC-768c @38.486016 Gbps w/Transparent UNI
TS-04-07.1	(Optional) (Cable High Speed Access, 320 Kbps up to 150 Mbps, Point-to-Point Protocol, IPv4/v6)—IPS	C.2.1.7.2	D	P-to-P Protocol, IPv4/v6 over Cable @ 320 Kbps up to 150 Mbps
TS-04-07.2.1	(Ethernet Interface, 1 Mbps up to 1 GbE (Gigabit Ethernet), IPv4/v6 over Ethernet)—IPS	C.2.1.7.2	D	IPv4/v6 over Ethernet works for speeds 1 Mbps up 1GbE
TS-04-07.2.2	(Ethernet Interface, 10 GbE (Optional), IPv4/v6 over Ethernet)—IPS	C.2.1.7.2	D	IPv4/v6 over Ethernet works for 10 GbE (Optional)
TS-04-07.2.3	(Ethernet Interface, Burstable, IPv4/v6 over Ethernet)—IPS	C.2.1.7.2	D	IPv4/v6 over Ethernet with burstable speeds
TS-04-07.3.1	(IP over SONET Service, OC-3c, IP/PPP over SONET)—IPS	C.2.1.7.2	D	IP/PPP over SONET works with OC-3c Interface
TS-04-07.3.2	(IP over SONET Service, OC-12c, IP/PPP over SONET)—IPS	C.2.1.7.2	D	IP/PPP over SONET works with OC-12c Interface
TS-04-07.3.3	(IP over SONET Service, OC-48c, IP/PPP over SONET)—IPS	C.2.1.7.2	D	IP/PPP over SONET works with OC-48c Interface
TS-04-07.3.4	(IP over SONET Service, OC-192c, IP/PPP over SONET)—IPS	C.2.1.7.2	D	IP/PPP over SONET works with OC-192c Interface
TS-04-07.4.1	(Private Line Service, DS0, IPv4/v6 over PLS)—IPS	C.2.1.7.2	D	IPv4/v6 over PLS works with DS0 Interface
TS-04-07.4.2	(Private Line Service, T1, IPv4/v6 over PLS)—IPS	C.2.1.7.2	D	IPv4/v6 over PLS works with T1 Interface
TS-04-07.4.3	(Private Line Service, T3, IPv4/v6 over PLS)—IPS	C.2.1.7.2	D	IPv4/v6 over PLS works with T3 Interface
TS-04-07.4.4	(Private Line Service, OC-3c, IPv4/v6 over PLS)—IPS	C.2.1.7.2	D	IPv4/v6 over PLS works with OC-3c Interface
TS-04-07.4.5	(Private Line Service, OC-12c, IPv4/v6 over PLS)—IPS	C.2.1.7.2	D	IPv4/v6 over PLS works with OC-12c Interface
TS-04-07.4.6	(Private Line Service, OC-48c, IPv4/v6 over PLS)—IPS	C.2.1.7.2	D	IPv4/v6 over PLS works with OC-48c Interface
TS-04-07.4.7	(Private Line Service, OC-192c, IPv4/v6 over PLS)—IPS	C.2.1.7.2	D	IPv4/v6 over PLS works with OC-192c Interface
TS-04-07.5	(Optional) (DSL Service, xDSL access at 1.5 to 8 Mbps downlink, and	C.2.1.7.2	D	P-to-P Protocol, IPv4/v6 over DSL w/xDSL access @ 1.5 to 8 Mbps

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
	384 Kbps to 1.5 Mbps uplink, Point-to-Point Protocol, IPv4/v6)—IPS			downlink, and 384 Kbps to 1.5 Mbps uplink
TS-04-07.6	(Optional) (FTTP, 10 to 300 Mbps, Point-to-Point Protocol, IPv4/v6)—IPS	C.2.1.7.2	D	P-to-P Protocol, IPv4/v6 over FTTP access @ 10 to 300 Mbps
TS-04-07.7.1	(Optional) (Wireless Access, LTE, Point-to-Point Protocol, IPv4/v6)—IPS	C.2.1.7.2	D	P-to-P Protocol, IPv4/v6 with Wireless Access, LTE
TS-04-07.7.2	(Optional) (Wireless Access, Satellite, Point-to-Point Protocol, IPv4/v6)—IPS	C.2.1.7.2	D	P-to-P Protocol, IPv4/v6 with Wireless Access over Satellite
TS-04-08.1	(Router or LAN Ethernet port: RJ-45, Up to 100 Mbps, SIP (IETF RFC 3261), H.323, MGCP, or SCCP)—IPVS	C.2.2.1.3	D	Router or LAN Ethernet port: RJ-45 interface up to 100 Mbps using SIP (IETF RFC 3261), H.323, MGCP, or SCCP
TS-04-16.1	Ethernet Interface—CDNS	C.2.5.4.3	D	IPv4/v6 over Ethernet works for speeds 1 Mbps up to 10/40/100 Gbps IAW TO
TS-04-16.2.1	PLS @ DS0—CDNS	C.2.5.4.3	D	IPv4/v6 over PLS works with DS0 Interface
TS-04-16.2.2	PLS @ T1—CDNS	C.2.5.4.3	D	IPv4/v6 over PLS works with T1 Interface
TS-04-16.2.3	PLS @ T3—CDNS	C.2.5.4.3	D	IPv4/v6 over PLS works with T3 Interface
TS-04-16.2.4	PLS @ OC-3c—CDNS	C.2.5.4.3	D	IPv4/v6 over PLS works with OC-3c Interface
TS-04-16.2.5	PLS @ OC-12c—CDNS	C.2.5.4.3	D	IPv4/v6 over PLS works with OC-12c Interface
TS-04-16.2.6	PLS @ OC-48c—CDNS	C.2.5.4.3	D	IPv4/v6 over PLS works with OC-48c Interface
TS-04-16.2.7	PLS @ OC-192c—CDNS	C.2.5.4.3	D	IPv4/v6 over PLS works with OC-192c Interface
TS-04-16.2.8	PLS @ OC-768c—CDNS	C.2.5.4.3	D	IPv4/v6 over PLS works with OC-768c Interface
TS-04-16.3.1	SONET @ OC-3c—CDNS	C.2.5.4.3	D	IP/PPP over SONET works with OC-3c Interface
TS-04-16.3.2	SONET @ OC-12c—CDNS	C.2.5.4.3	D	IP/PPP over SONET works with OC-12c Interface
TS-04-16.3.3	SONET @ OC-48c—CDNS	C.2.5.4.3	D	IP/PPP over SONET works with OC-48c Interface
TS-04-16.3.4	SONET @ OC-192c—CDNS	C.2.5.4.3	D	IP/PPP over SONET works with OC-192c Interface
TS-04-16.3.5	SONET @ OC-768c—CDNS	C.2.5.4.3	D	IP/PPP over SONET works with OC-768c Interface
TS-04-16.4	DSL @ 1.5 to 6 Mbps Up and 384 Kbps to 50 Mbps Down—CDNS	C.2.5.4.3	D	P-to-P Protocol, IPv4/v6 over DSL with uplink and downlink IAW TO
TS-04-16.5	Cable High Speed Access @ 320 Kbps up to 150 Mbps—CDNS	C.2.5.4.3	D	P-to-P Protocol, IPv4/v6 over Cable with speed IAW TO
TS-04-16.6.1	Wi-Fi Wireless Access—CDNS	C.2.5.4.3	D	P-to-P Protocol, IPv4/v6 works over WiFi Interface

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-04-16.6.2	LTE Wireless Access—CDNS	C.2.5.4.3	D	P-to-P Protocol, IPv4/v6 works over LTE Interface
TS-04-16.6.3	Satellite Wireless Access—CDNS	C.2.5.4.3	D	P-to-P Protocol, IPv4/v6 works over Satellite Interface
TS-04-19.1	IP phones -UCS	C.2.8.3.3	D	Establish connectivity
TS-04-19.2	Mobile phones—UCS	C.2.8.3.3	D	Establish connectivity
TS-04-19.3	Web browsers—UCS	C.2.8.3.3	D	Establish connectivity
TS-04-19.4	E-mail clients—UCS	C.2.8.3.3	D	Establish connectivity
TS-04-19.5	Desktop clients—UCS	C.2.8.3.3	D	Establish connectivity
TS-04-19.6	PCs—UCS	C.2.8.3.3	D	Establish connectivity
TS-04-19.7	Tablets—UCS	C.2.8.3.3	D	Establish connectivity
TS-04-20.1	(SONET OC-3, 148.608 Mbps, Transparent)—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using SONET OC-3 @148.608 Mbps (Ref: C.2.9.1.4)
TS-04-20.2	(SONET OC-3c, 148.608 Mbps, Transparent)—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using SONET OC-3c @148.608 Mbps (Ref: C.2.9.1.4)
TS-04-20.3	(SONET OC-12, 594.432 Mbps, Transparent)—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using SONET OC-12 @594.432 Mbps (Ref: C.2.9.1.4)
TS-04-20.4	(SONET OC-12c, 594.432 Mbps, Transparent)—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using SONET OC-12c @594.432 Mbps (Ref: C.2.9.1.4)
TS-04-20.5	(SONET OC-48, 2.377728 Gbps, Transparent)—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using SONET OC-48 @2.377728 Gbps (Ref: C.2.9.1.4)
TS-04-20.6	(SONET OC-48c, 2.377728 Gbps, Transparent)—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using SONET OC-48c @2.377728 Gbps (Ref: C.2.9.1.4)
TS-04-20.7	(SONET OC-192, 9.510912 Gbps, Transparent)—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using SONET OC-192 @9.510912 Gbps (Ref: C.2.9.1.4)
TS-04-20.8	(SONET OC-192c, 9.510912 Gbps, Transparent)—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using SONET OC-192 @9.510912 Gbps(Ref: C.2.9.1.4)
TS-04-20.9	(Optional) (SONET OC-768, 38.486016 Gbps, Transparent)—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using SONET OC-768 @38.486016 Gbps (Ref: C.2.9.1.4)
TS-04-20.10	(Optional) (SONET OC-768c, 38.486016 Gbps, Transparent)—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using SONET OC-768c @38.486016 Gbps (Ref: C.2.9.1.4)

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-04-20.11	Ethernet 1 Mbps to 10 Mbps at 1 Mbps increments—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using ETS 1 Mbps—10 Mbps w/1 Mbps increments (Ref: C.2.9.1.4)
TS-04-20.12	Ethernet 10 Mbps to 100 Mbps at 10 Mbps increments—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using ETS 10 Mbps—100 Mbps w/10 Mbps increments (Ref: C.2.9.1.4)
TS-04-20.13	Ethernet 100 Mbps to 1000 Mbps at 100 Mbps increments—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using ETS 100 Mbps—1000 Mbps w/100 Mbps increments (Ref: C.2.9.1.4)
TS-04-20.14	Ethernet 1 Gbps to 10 Gbps at 1 Gbps increments—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using ETS 1 Gbps—10 Gbps w/1 Gbps increments (Ref: C.2.9.1.4)
TS-04-20.15	Ethernet (Optional) 10 Gbps to 100 Gbps at 10 Gbps increments—MTIPS TC&D	C.2.8.4.3	D	MTIPS TC&D using ETS (Optional) 10 Gbps—100 Gbps w/10 Gbps increments (Ref: C.2.9.1.4)
TS-04-21	MSS shall support. VPNS as specified in Section C.2.1.1.1	C.2.1.1.1	D	Demonstration that required service KPIs are met.
TS-04-22	MSS shall support. ETS as specified Section C.2.1.2	C.2.1.1.1	D	Demonstration that required service KPIs are met.
TS-04-23	MSS shall support. IPS as specified in Section C.2.1.7	C.2.1.1.1	D	Demonstration that required service KPIs are met.
TS-04-25	IPSS shall support “Ethernet Access as specified in Section C.2.1.2”	C.2.1.2	D	Demonstration that required service KPIs are met.

7.5 TS-05 Test Cases

The test cases for test scenario 5 (TS-05, Technical Capabilities) are contained in ***Table 7.5.***

Table 7.5. TS-05 Test Cases

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-01.1	Meet applicable routing requirements in RFP Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.2	Provide multiple tunneling standards, as required by an agency.	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.3	Provide various encryption levels, as required by an agency.	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.4	Provide authentication services as required by an agency.	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.5	Support IPv4 as both the encapsulating and encapsulated protocol	C.2.1.1.1.4	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-01.6	Support IPv6 as both the encapsulating and encapsulated protocol	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.7	Support QoS modes for a) Best effort; b) "hose level"; c) "pipe level"; e) Diffserv marked;	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.8	Support QoS across a) 802.1p Prioritized ETS b) MPLS-based access; c) Multilink Multiclass PPP; d*) QoS-enabled wireless <Reserved – Not Bid>*	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.9	Support one or more of the QoS objectives: a) Intserv model for selected individual flows; b) Diffserv model for aggregated flows	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.10	Provide isolation of traffic and routing service for exchange per the requirements in RFP Section C.2.1.1.1.4 (10).	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.11	Support multiple VPNs by allowing both permanent and temporary access to 1 or more VPNs for authenticated users across a broad range of access technologies	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.12	Provide secure routing services to provide full routing capability on the VPN platform with a secure policy across the VPN.	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.13	Support the inclusion of encryption, decryption, and key management profiles as part of the security management system.	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.14	Support an agency in deploying and refining its own internal security mechanisms in addition to those deployed by the contractor.	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-01.15	Allow an agency to choose from Contractor-provided, Third party, and Agency-provided alternatives for authentication of temporary access users.	C.2.1.1.1.4	D	Demonstration that required Capability is met.
TS-05-02.1	Meet applicable routing requirements in RFP Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.2	Provide Intra-City ETS and Inter-City ETS geographical coverage	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.3	Support Ethernet UNI to support Layer 2 and Layer 3 clients.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.4	Support Ethernet Virtual Connections EVC.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.5	Support ETS delivery at the agency's SDP via a UNI.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.6	If required, Support circuit emulation services for TDM services.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.7	Support point-to-point, multi-point-to-point, and point-to multipoint EVCs.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.8	EVC multiplexing shall be supported.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.9	Support rate-limited throughput access links.	C.2.1.2.1.4	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-02.10	Support rate-limiting at the agency's SDP and the individual VLAN ingress & egress.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.11	Support privacy and security per IEEE 802.3, as defined in the TO.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.12	Physical interfaces shall be supported per RFP Section C.2.1.2.3	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.13	Support CIR, CBS, PIR and MBS traffic profiles.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.14	Performance parameters shall be supported per RFP Section C.2.1.2.7.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.15	Service Frame Delivery options supported shall include Unicast, Multicast and Broadcast Frame Delivery.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.16	Support VLAN tag preservation, tag translation, tag stacking, and aggregation (optional) across a common physical connection.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.17	Support service multiplexing w/multiple EVCs connected via a single UNI.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.18	Support bundling to enable two or more VLAN IDs to be mapped into a single EVC at a UNI.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.19	Security Filters shall be supported as specified in the TO.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.20	(Optional) Provide proactive Performance Monitoring per RFP Section C.2.1.2.1.4 (20).	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.21	Support the following maintenance functions per RFP Section C.2.1.2.1.4 (21).	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.22	Support Point-to-point, Point-to-Multi-point, Multi-point-to-Multi-point and Ring network topologies:	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.23	Support geographical diversity to provide added reliability.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.24	Support bridging in compliance with IEEE 802.1X-REV.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.25.1	Support Point-to-point ETS (up to 40 Gbps) Virtual Connection sizes.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.25.2	Support Multi-point-to-multi-point connections (up to 40 Gbps) Virtual Connection sizes.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.26	Quality of Service (QoS)—Support traffic prioritization that enables higher priority traffic to be transmitted first	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-02.27	Support traffic reconfiguration to allow modification of a specific service connection subsequent to the establishment of the connection.	C.2.1.2.1.4	D	Demonstration that required Capability is met.
TS-05-03.1	Support the following non-domestic (optional), CONUS and Metro Wavelength Services connections defined in RFP Section C.2.1.3.1.4.	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-03.2.1	As defined in RFP Section C.2.1.3.1.4 (1), provide Transmission Rates. Wavelengths	C.2.1.3.1.4	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
	shall be supported at 1 Gbps, 2.5 Gbps, and 10 Gbps			
TS-05-03.2.2	As defined in RFP Section C.2.1.3.1.4 (2), provide Clock Transparency.	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-03.2.3	As defined in RFP Section C.2.1.3.1.4 (3), provide Protocol Transparency—Metro	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-03.2.4	As defined in RFP Section C.2.1.3.1.4 (4), provide Protocol Transparency – CONUS and Non-Domestic (optional)	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-03.2.5	As defined in RFP Section C.2.1.3.1.4 (5), provide Byte Transparency.	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-03.2.6	As defined in RFP Section C.2.1.3.1.4 (6), provide Concatenation	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-03.2.7	As defined in RFP Section C.2.1.3.1.4 (7), provide (Optional) Channelization	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-03.2.8	As defined in RFP Section C.2.1.3.1.4 (8), provide Wavelength Delivery.	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-03.2.9	As defined in RFP Section C.2.1.3.1.4 (9), provide Access Methods to the ordered wavelength service for an end-to-end offering.	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-03.2.10	As defined in RFP Section C.2.1.3.1.4 (10), provide multi-vendor interoperability support to the GFP/SRE.	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-03.2.11	As defined in RFP Section C.2.1.3.1.4 (11), provide Efficient Transport.	C.2.1.3.1.4	D	Demonstration that required Capability is met.
TS-05-04.1	Meet applicable routing requirements in RFP Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.	C.2.1.4.1.4	D	Demonstration that required Capability is met.
TS-05-04.2	Provide transparency to any protocol used GFP.	C.2.1.4.1.4	D	Demonstration that required Capability is met.
TS-05-04.3	Provide PLS data transparency treatment of all bit sequences transmitted by GFP through the SDP.	C.2.1.4.1.4	D	Demonstration that required Capability is met.
TS-05-04.4	Support the 15 categories of PLS service as defined in RFP Section C.2.1.4.1.4 (2).	C.2.1.4.1.4	D	Demonstration that required Capability is met.
TS-05-07.1	Meet applicable routing requirements in Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.	C.2.1.7.1.4	D	Demonstration that required Capability is met.
TS-05-07.2	Provide IPS ports at the peak data rates specified by the customer.	C.2.1.7.1.4	D	Demonstration that required Capability is met.
TS-05-07.3	Support appropriate access services … to connect customer SDPs to CenturyLink's IPS.	C.2.1.7.1.4	D	Demonstration that required Capability is met.
TS-05-07.4	Provide the 4 arrangements, IP/domain name support as defined in RFP Section C.2.1.7.1.4 (4).	C.2.1.7.1.4	D	Demonstration that required Capability is met.
TS-05-07.5	Provide support for the Border Gateway Protocol (BGP) for EIS customers with registered Autonomous System (AS) numbers.	C.2.1.7.1.4	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-07.6	Validate routing protocol information using authenticated protocols.	C.2.1.7.1.4	D	Demonstration that required Capability is met.
TS-05-08.1	Provide unlimited on-net to on-net and on-net to CONUS off-net calling.	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.2	Provide off-net calling to CONUS, OCONUS, and Non-Domestic locations.	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.3	Provide capabilities that enable IPVS users to establish and receive telephone calls between both on-net locations and the PSTN.	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.4	Provide a remote access capability per RFP Section C.2.2.1.1.4 (4).	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.5.1	Provide capability for Real time transport of voice, facsimile, and TTY communications	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.5.2	Provide capability for Real time delivery of Automatic Number Identification (ANI) information (when provided from the originating party)	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.5.3	Provide capability to Interoperate with public network dial plans (e.g., North American Numbering Plan and ITU-E.164).	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.5.4	Provide capability to Interoperate with private network dial plans and support direct station to station dialing	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.5.5	Provide capability to (Optional) Interoperate with non-commercial, agency-specific 700 numbers	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.5.6	Provide access to public directory and operator assistance services	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.5.7	Provide unique directory numbers for all on-net government locations, including support for existing government numbers.	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.5.8	Provide the capability to initiate automatic callback	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.5.9	Provide capability to Support 3-way calling	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.6	Provide Subscriber and PSTN gateways … between CenturyLink's IP-based network and the PSTN, or with agency UNIs.	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.7	Provide the capability to support station mobility.	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.8	The IPVS shall ... traverse and successfully interoperate with agency firewalls and security layers per RFP Section C.2.2.1.1.4.	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.9	Ensure that security practices and safeguards per RFP Section C.2.2.1.1.4.	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.10	Provide security safeguards for DoS, Intrusion and Invasion of Privacy.	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08.11	Fully comply with emergency service requirements, including 911 and E911 services per	C.2.2.1.1.4	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
	RFP Section C.2.2.1.1.4.			
TS-05-08.12	The contractor's IPVS shall comply with the Federal Communications Commission (FCC) Local Number Portability (LNP) requirements.	C.2.2.1.1.4	D	Demonstration that required Capability is met.
TS-05-08M.1	1. Provide all hardware and licensing necessary per RFP Section C.2.2.1.5 (1).	C.2.2.1.5	I	Provide required information.
TS-05-08M.2	2. The Managed LAN Service solution shall interoperate with the ordering agency's provided VoIP ready infrastructure per RFP Section C.2.2.1.5 (2).	C.2.2.1.5	D	Demonstration that required Capability is met.
TS-05-08M.3	3. Be responsible for the ongoing maintenance and upgrades of CenturyLink-owned equipment used to provide the Managed LAN Service.	C.2.2.1.5	D	Demonstration that required Capability is met.
TS-05-08M.4	4. Propose installation time intervals for additional user devices at sites already using the IPTel and Managed LAN Service.	C.2.2.1.5	I	Provide required information.
TS-05-08M.5	5. The Managed LAN Service shall not include any wireless devices or components on the LAN (i.e., wired solution only) unless requested and approved by the ordering contract officer (OCO).	C.2.2.1.5	D	Demonstration that required Capability is met.
TS-05-08M.6	6. The Managed LAN Service shall not support other services (i.e., data, video etc.) unless requested and approved by the government.	C.2.2.1.5	D	Demonstration that required Capability is met.
TS-05-08M.7	7. Ensure that only authorized devices (as determined by the ordering agency) are able to operate on the Managed LAN Service.	C.2.2.1.5	D	Demonstration that required Capability is met.
TS-05-08M.8	8. Monitor, manage and restore the Managed LAN Service on a 24x7 basis.	C.2.2.1.5	D	Demonstration that required Capability is met.
TS-05-08M.9	9. Specify the LAN management activities provided as well as identify those activities which are considered customer responsibilities as defined in RFP Section C.2.2.1.5 (9.	C.2.2.1.5	I	Provide required information.
TS-05-08M.10	10. Provide proactive notification of major and minor alarms to the Managed LAN Service per RFP Section C.2.2.1.5 (10).	C.2.2.1.5	D	Demonstration that required Capability is met.
TS-05-08M.11	11. Define the escalation path for trouble tickets for...network and hardware issues.	C.2.2.1.5	I	Provide required information.
TS-05-08S.1	Session Initiation Protocol (SIP) Trunk Service shall be fully integrated with IPVS per RFP Section C.2.2.1.6.	C.2.2.1.6	D	Demonstration that required Capability is met.
TS-05-08S.2	Provide capabilities that enable SIP users to successfully establish and receive telephone calls between both on-net locations and the PSTN.	C.2.2.1.6.1	D	Demonstration that required Capability is met.
TS-05-12.1.1	As required, assuming responsibility for all damage or injury to persons or property as per the requirements in C.2.4.4 (1) (a).	C.2.4.4	I	Provide required information.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-12.1.2	As required, completing any necessary pre-delivery preparations for the delivery site, site security, or storage facilities as per the requirements in C.2.4.4 (1) (b).	C.2.4.4	D	Demonstration that required Capability is met.
TS-05-12.1.3	As required, relocating GFP from initial receiving points or temporary storage facilities to the final contractor facility and installation site.	C.2.4.4	D	Demonstration that required Capability is met.
TS-05-12.1.4	As Required, preparing the final installation site including the provisioning of necessary physical space, environmental systems, and network connectivity…	C.2.4.4	D	Demonstration that required Capability is met.
TS-05-12.1.5	As required, facilitating GFP setup, including assembling, loading, configuring, testing, and (at end of life) crating and packing GFP for return.	C.2.4.4	D	Demonstration that required Capability is met.
TS-05-12.1.6	As required, providing contractor personnel with all required national citizenship, security clearances, training, and technical certifications per RFP Section C.2.4.4 (1) (f).	C.2.4.4	I	Provide required information.
TS-05-12.2	Authorized government personnel and third-parties shall have access to GFP as per RFP Section C.2.4.4 (2).	C.2.4.4	I	Provide required information.
TS-05-12.3	Provide a service management capability such that user can remotely monitor facility and equipment status in real-time.	C.2.4.4	D	Demonstration that required Capability is met.
TS-05-12.4	The service management capability shall present alarms to the user in real-time for facility and communication failures.	C.2.4.4	D	Demonstration that required Capability is met.
TS-05-12.5	The service management capability shall continuously update and present to the user the status of power per RFP Section C.2.4.4 (5)	C.2.4.4	D	Demonstration that required Capability is met.
TS-05-13.1	Provide access to agency data in data centers that complies with National Policy as defined in RFP Section C.1.8.8.	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.2	Provide Cloud Data Center Security per RFP Section C.2.5.1.1.4.1 (2).	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.3	Provide Agency Cloud Service Security per RFP Section C.2.5.1.1.4.1 (3).	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.4	Provide a Virtualized elastic computing infrastructure:	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.5	Provide Virtual Machines (VMs)	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.6	Provide Network Storage	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.7	Provide Server Hosting for Private-facing Internal Web Hosting & Public-facing External Web Hosting.	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.8	Provide Backup and Restore of agency data	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-13.9	Provide On-demand self-service service for IaaS per C.2.5.1.1.4.1 (9).	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.10	Visibility into usage of measured/metered (usage-based) service.	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.11	Allow users to have VMs with their own private IP address-blocks.	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.12	Support bulk import and export of VM per ISO 17203.	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.13	Allow users access to log events such as resource provisioning and de-provisioning, VM start and stop, and account changes, for at least 60 days.	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.14	(Optional) Allow users to place metadata tags on provisioned resources and to run reports based on them…	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.15	Support cost control measures such as quotas and leases.	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.16	Support with 24x7 customer service, via phone, email and chat.	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.17	Provide tools so the client agency can fully retrieve its data in the original or ...agreed-upon format.	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.18	Ensure Cloud resources, particularly the data at rest, are be located within the U.S. or the jurisdiction identified in the TO per RFP Section C.2.5.1.1.4.1 (18).	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.19	Provide Disaster Recovery (DR) and Continuity of Operations (COOP) per agency-specific requirements in the TO.	C.2.5.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-13.20	For Data Center Augmentation with Common ITSM, ability to manage both cloud and the agency Data Center's virtual resources per RFP Section C.2.5.1.1.4.2 (1).	C.2.5.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-13.21	For Data Center Augmentation with Common ITSM, the management platform shall include a visual indicator distinguishing cloud and premises resources.	C.2.5.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-13.22	(Optional) for Data Center Augmentation with Common ITSM, ability to integrate with agency's data center management platform.	C.2.5.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-14.1	Access to agency data in data centers shall comply with National Policy as defined in RFP Section C.1.8.8 including agency sites and remote locations.	C.2.5.2.1.4	D	Demonstration that required Capability is met.
TS-05-14.2	Provide Developer Tools per RFP Section C.2.5.1.1.4.2 (2).	C.2.5.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-14.3	Provide Database Management Systems (DBMS)/Relational DBMS (RDBMS)	C.2.5.2.1.4	D	Demonstrated Database Systems (DBMS/RDMS)
TS-05-14.4	Provide Big Data Solution Platform.	C.2.5.2.1.4	D	Demonstrated Big Data Solution Platform.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-14.5	Provide Directory per RFP Section C.2.5.1.1.4.2 (6).	C.2.5.2.1.4	D	Demonstrated Directory per C.2.5.1.1.4.2 (6).
TS-05-14.6	Provide Application, Web and Workflow Test Tools	C.2.5.2.1.4	D	Demonstration that required Capability is met.
TS-05-14.7	Provide tools to allow the client agency to fully access PaaS-related data from the cloud in a usable format as needed.	C.2.5.2.1.4	D	Demonstration that required Capability is met.
TS-05-15.1	Provide Access to agency data in data centers shall comply with National Policy as defined in RFP Section C.1.8.8 including agency sites and remote locations.	C.2.5.3.1.4	D	Demonstration that required Capability is met.
TS-05-15.2	Provide Customer Relationship Management (CRM) tools	C.2.5.3.1.4	D	Demonstration that required Capability is met.
TS-05-15.3	Provide Enterprise Resource Planning (ERP) tools	C.2.5.3.1.4	D	Demonstration that required Capability is met.
TS-05-15.4	Provide Human Capital Management (HCM) tools	C.2.5.3.1.4	D	Demonstration that required Capability is met.
TS-05-15.5	Provide Desktop applications	C.2.5.3.1.4	D	Demonstration that required Capability is met.
TS-05-15.6	Provide Office Automation tools	C.2.5.3.1.4	D	Demonstration that required Capability is met.
TS-05-15.7	Provide Security tools	C.2.5.3.1.4	D	Demonstration that required Capability is met.
TS-05-15.8	Provide Other tools as defined in the TO	C.2.5.3.1.4	D	Demonstration that required Capability is met.
TS-05-15.9	Provide tools to allow the client agency to fully access SaaS related data from the cloud in usable format as needed.	C.2.5.3.1.4	D	Demonstration that required Capability is met.
TS-05-16.1	Provide Static Content Download Service including text, video, and music.	C.2.5.4.1.4	D	Demonstration that required Capability is met.
TS-05-16.2	Provide Real Time Streaming (Webcasting) per RFP Section C.2.5.4.1.4 (1) (b).	C.2.5.4.1.4	D	Demonstration that required Capability is met.
TS-05-16.3	Content Distribution: c) On Demand Streaming per RFP Section C.2.5.4.1.4 (1) (c).	C.2.5.4.1.4	D	Demonstration that required Capability is met.
TS-05-16.4	Site Monitoring/Origin Server Performance Measurements a) Perform continuous monitoring to ensure performance and quality of service using measurements listed in RFP Section C.2.5.4.1.4 (2)(a).	C.2.5.4.1.4	D	Demonstration that required Capability is met.
TS-05-16.5	Capability = Site Monitoring/Server Performance Measurements b) Provide statistics via a performance dashboard – a secure, Web-based portal accessible 24x7 by agency clients.	C.2.5.4.1.4	D	Demonstration that required Capability is met.
TS-05-17D.1	As a DES, Identify hardware and firmware...related software, and SRL required by the agency to deliver EIS services.	C.2.8.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-17D.2	As a DES, identify network components and determine protocols, redundancy, traffic filtering, and traffic prioritization requirements. Recommend the appropriate performance	C.2.8.1.1.4.1	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
	levels and network capacities, as required.			
TS-05-17D.3	As a DES, Provide complete project management per RFP Section C.2.8.8.8.4.1 (3).	C.2.8.1.1.4.1	D	Demonstration that required Capability is met.
TS-05-17I.1	For implementation, management, and maintenance (IMM), develop, implement, and manage comprehensive solutions per RFP Section C.2.8.1.1.4.2 (1) using the EIS services to meet agency-specific requirements.	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.2	For IMM, Supply and manage the hardware, firmware and related software required by the agency.	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.3	For IMM, Provide tools to monitor performance and provide visibility per RFP Section C.2.8.1.1.4.2 (3).	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.4	For IMM, Manage the network per RFP Section C.2.8.1.1.4.2 (4).	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.5	For IMM, Permit SNMP read-access data feeds that provide the agency with managed equipment information, as applicable.	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.6	For IMM, Manage network configuration and perform the 9 Activities listed in C.2.8.1.1.4.2(6)	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.7	For IMM, Provide IP Address Management as applicable per RFP Section C.2.8.1.1.4.2 (7).	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.8	For IMM, Monitor and control access to equipment per RFP Section C.2.8.1.1.4.2 (8).	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.9	For IMM, regularly perform off-site equipment configuration backups per RFP Section C.2.8.1.1.4.2 (9),	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.10	For IMM, Perform necessary hardware and software maintenance per RFP Section C.2.8.1.1.4.2 (10).	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.11	For IMM, Provide preventative and corrective maintenance on agency-specific devices.	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.12	For IMM, Proactively detect problems, respond to alerts and promptly report situations per RFP Section C.2.8.1.1.4.2 (12).	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.13	For IMM, Provide the agency with real or near-time access per RFP Section C.2.8.1.1.4.2 (13).	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-17I.14	For IMM, Provide inventory tracking tool(s) to maintain and track all agency circuit, transport service and equipment inventory information.	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-17I.15	For IMM, Provide agency with secure access to current and historical information per RFP Section C.2.8.1.1.4.2 (15).	C.2.8.1.1.4.2	D	Demonstration that required Capability is met.
TS-05-19.1	Support enabling UC capabilities via many devices, including desktop phones and mobile devices (smart phones, tablets, etc.), wireline and IP phones, soft clients, and video conferencing devices.	C.2.8.3.1.4	D	Demonstration that required Capability is met.
TS-05-19.2	Provide Unified Messaging (UM) with the 4 functions as defined in RFP Section C.2.8.3.1.4 (2).	C.2.8.3.1.4	D	Demonstration that required Capability is met.
TS-05-19.3	Support Mobile Integration per RFP Section C.2.8.3.1.4 (3).	C.2.8.3.1.4	D	Demonstration that required Capability is met.
TS-05-19.4	Provide a Unified User Interface with the functions defined in RFP Section C.2.8.3.1.4 (4).	C.2.8.3.1.4	D	Demonstration that required Capability is met.
TS-05-19.5	Provide the… capabilities to support QoS per RFP Section C.2.8.3.1.4 (5).	C.2.8.3.1.4	D	Demonstration that required Capability is met.
TS-05-19.6	Provide a premises-based WAN optimizer per RFP Section C.2.8.3.1.4 (6).	C.2.8.3.1.4	D	Demonstration that required Capability is met.
TS-05-19.7	Support both IPv4 and IPv6 and be able to communicate over IPv4-only, IPv6-only and/or dual-stack networks.	C.2.8.3.1.4	D	Demonstration that required Capability is met.
TS-05-19.8	Meet a minimum voice quality level that is equivalent to or better than a Mean Opinion Score (MOS) of 4.0 as specified in ITU-T specification P.800 series.	C.2.8.3.1.4	D	Demonstration that required Capability is met.
TS-05-19.9	Ensure that security practices and safeguards are provided per RFP Section C.2.8.3.1.4 (9).	C.2.8.3.1.4	D	Demonstration that required Capability is met.
TS-05-20.1	Provide TIC Portal Access to External Networks including the Internet per RFP Section C.2.8.4.1.4.1 (1).	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.
TS-05-20.2	EINSTEIN Protection –At each TIC Portal, Meet applicable routing requirements in RFP Section C.1.8.8 ensuring any encrypted tunnels are applied and proxied to allow inspection.	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.
TS-05-20.3	Provide a TIC Portal SOC per RFP Section C.2.8.4.1.4.1 (3).	C.2.8.4.1.4.1	I	Provide required element for inspection.
TS-05-20.4	Provide a ICD 705 Sensitive Compartmented Information Facility (SCIF) per RFP Section C.2.8.4.1.4.1 (4).	C.2.8.4.1.4.1	I	Provide required element for inspection.
TS-05-20.5	Content Filtering/Inspection of Encrypted Traffic with documented procedures.	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.
TS-05-20.6	Process traffic with Asymmetric Routing per RFP Section C.2.8.4.1.4.1 (6).	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.
TS-05-20.7	Provide Federal Video Relay Service (FedVRS) Support per RFP Section C.2.8.4.1.4.1	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
	(7).			
TS-05-20.8	E-Mail Forgery Protection – Domain-level sender forgery analysis equivalent to Domain Keys Identified Mail or Sender Policy Framework standards.	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.
TS-05-20.9	Optionally support signing procedures for outgoing email messages per C.2.8.4.1.4.1 (9).	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.
TS-05-20.10	Support Domain Name System (DNS) and DNS Security Extensions (DNSSEC) requirements per RFP Section C.2.8.4.1.4.1 (10).	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.
TS-05-20.11	The MTIPS portals shall be equipped for uninterrupted operations for at least 24 hours in the event of a power outage	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.
TS-05-20.12	Support Internet Protocol Version 6 (IPv6) for all TIC systems per RFP Section C.2.8.4.1.4.1 (12).	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.
TS-05-20.13	Data Loss/Leak Prevention – Support Data Loss (Leak) Prevention (DLP) program.	C.2.8.4.1.4.1	D	Demonstration that required Capability is met.
TS-05-20.14	Allow the agency's Internet bound traffic to reach the Internet via one of the two TIC Portals.	C.2.8.4.1.4.2	D	Demonstration that required Capability is met.
TS-05-20.15	An agency Trusted Domain (DMZ) shall be created by CenturyLink as defined in RFP Section C.2.8.4.1.4.2 (2).	C.2.8.4.1.4.2	D	Demonstration that required Capability is met.
TS-05-20.16	Inter-agency traffic shall be routed through and inspected by the TIC Portal if the connection is classified as an external connection.	C.2.8.4.1.4.2	D	Demonstration that required Capability is met.
TS-05-21M.1	Provide design and implementation services.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.2	Provide software and hardware components, including log servers, as applicable.	C.2.8.5.1.4.1	I	Provide proof of required element for inspection.
TS-05-21M.3	Implement hardware or software load balancing capabilities and redundancy necessary to meet KPI and agency requirements.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.4	Provide installation support to include testing of equipment, testing of software, and loading of any agency-relevant data, as required by the agency.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.5	Maintain the latest configuration information for restoration purposes, reporting, and forensics analysis.	C.2.8.5.1.4.1	I	Provide proof of required element for inspection.
TS-05-21M.6	Maintain the managed service capabilities, performing hardware/software upgrades and replacements, and content updates.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-21M.7	Ensure that MPS systems and components comply with NIST SP 800-53 identification and authentication controls for high impact systems (FIPS 199). Administrative access devices requires multi-factor authentication (OMB M-11-11).	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.8	Notify the agency about patches and bug fixes as soon as they become available.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.9	Test and deploy the latest patches and bug fixes as soon as they become available and are approved by the agency.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.10	Perform and document configuration and management as applicable to ensure that security, access, and information-flow policies are enforced as requested by the agency.	C.2.8.5.1.4.1	I	Provide proof of required element for inspection.
TS-05-21M.11	Proactively monitor the health and status of MPS hardware/software components on a 24x7 basis for indications of compromise such as intrusions, anomalies, malicious activities, and network misuse.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.12	Monitor the overall performance of the service, including the adequacy of the hardware/software components as the network expands.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.14	Ensure the service allows only necessary functionality, network protocols, ports or services with documented customer approval.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.15	Perform and document periodic validation activities (e.g., via scans) to ensure service configurations are not vulnerable and are enforcing agency policies.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.16	Notify the agency of MPS-failure events via email, fax, or telephone, as directed by the agency.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.17	Receive, handle, and use sensitive but unclassified cybersecurity indicators provided by the agency or the Department of Homeland Security (DHS).	C.2.8.5.1.4.1	I	Provide proof of required element for inspection.
TS-05-21M.18	Ensure that service statistics, events messages, logs, and suspected attack information are sent via secure means to the agency-specified operation center.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.19	Ensure that event messages associated with DHS-provided indicators are sent via secure means to DHS.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.20	Ensure that event messages have necessary and consistent timestamps and content to establish context per RFP Section C.2.8.5.1.4.1 (19).	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21M.21	Be able to identify and retrieve each customer agency's data for the agency, without divulging any other agency's data.	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-21M.22	Provide agency with secure web access to logs and service information per RFP Section C.2.8.5.1.4.1 (21).	C.2.8.5.1.4.1	D	Demonstration that required Capability is met.
TS-05-21V.1	Provide external Vulnerability Scanning which tests Internet connected nodes in the network, including web environments.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.2	Provide internal Vulnerability Scanning which looks for local/host flaws and internal threats, usually inside the firewall.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.3	The service shall Periodically probe networks, including operating systems and application software, for potential openings, security holes, and improper configuration.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.4	Provide a VSS that probes agency systems for vulnerabilities in at least the 48 areas listed on RFP Section C.2.8.5.1.4.2.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.5	Proactively identify network vulnerabilities and propose appropriate countermeasures, fixes, patches, and workarounds.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.6	Notify the agency of vulnerabilities discovered via email, fax, or telephone, as directed by the agency.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.7	Provide the agency with secure Web access to vulnerability information, scan summaries, device/host reports, and trend analyses.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.8	Review vulnerabilities discovered with the agency, as required.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.9	Provide scan scheduling flexibility to the agency in order to minimize any interruptions in normal business activities.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.10	Provide the agency with non-destructive and non-intrusive vulnerability scans that will not crash the systems being analyzed or disrupt agency operations. The scans shall not provoke a denial of service condition on the agency system being probed.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.11	Use other analytical means to ascertain the vulnerability of agency systems if a particular scan is potentially destructive or intrusive.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.12	Ensure that the scanning engine is regularly updated with new vulnerabilities information in order to maintain effectiveness of the service.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21V.14	Support networks of varying size and complexity.	C.2.8.5.1.4.2	D	Demonstration that required Capability is met.
TS-05-21I.1	Review the agency's security infrastructure and develop appropriate strategic plans in collaboration with the agency.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-21I.2	Provide the agency with effective incident response support on a 24x7 basis.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.3	Maintain a problem detection system for the diagnosis of alerts and violations.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.4	Analyze suspicious security alerts to determine the significance and scope of an event and immediately notify the agency when the event is deemed high priority.	C.2.8.5.1.4.3	A	Provide required analysis.
TS-05-21I.5	Provide the agency with immediate access to vulnerability and severe alert information which contains but is not be limited to the following: Description, Target, Origin, Potential Incident Impacts, Remedies, and Prevention Measures.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.6	Coordinate with the agency to handle potential security incidents according to the appropriate response procedures.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.7	Provide countermeasures to contain the security incident, limit its spread, and protect internal systems.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.8	Recommend the fixes necessary to eliminate identified vulnerabilities, and appropriate procedures to guard against future attacks.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.9	Provide the agency with secure web access to incident analysis findings and recommendations.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.10	Assist the agency in containing the damage and restoring affected systems to their normal operational state.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.11	Assist the agency in testing restored systems in order to Ensure that identified vulnerabilities have been corrected.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.12	Provide dedicated support until resolution of the problem.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.13	Provide post-incident investigative and forensics services.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.14	Provide telephone support to the agency, as required.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.15	Deploy cybersecurity personnel to agency sites to handle security incidents, as necessary.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-21I.16	Provide security awareness training to agency personnel as required.	C.2.8.5.1.4.3	D	Demonstration that required Capability is met.
TS-05-25.1	Establish and support a process that allows DHS to provide cyber threat indicators and define desired effects in the protection of covered network traffic.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.2	Demonstrate to DHS that IPSS operates as intended when traffic is present that matches	C.2.8.9.1.4	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
	malicious indicators prior to the activation of new or modified indicators and their associated actions.			
TS-05-25.3	Support a process that allows DHS to direct actions on network traffic to gather additional information on cyber threats, stop cyber attacks, and/or respond to cyber incidents.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.4	Provide for the ability to receive, accept, utilize, and secure government furnished information (GFI) up to the Top Secret/Sensitive Compartmented Information (TS/SCI) level, including PII, such as cyber threat indicators signatures, and associated actions in accordance with DHS-approved security guidelines.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.5	Provide an automated means for DHS to share GFI and utilize the GFI provided within the DHS IPSS in as near real-time as possible.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.6	Establish or leverage additional commercially available cyber threat information and/or DHS IPSS functional capabilities to provide additional protections for Federal Systems.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.7	Ensure only those indicators and associated actions that are approved and further specified by DHS are applied to Participating Agencies.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.8	Provide the ability to apply different sets of mitigation capabilities to a Participating Agency's traffic that does not affect which mitigations are applied to a separate Participating Agency's traffic.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.9	Ensure that GFI is not disclosed or shared with any third party or used for any purpose that DHS has not specifically authorized.	C.2.8.9.1.4	I	Provide proof of required element for inspection.
TS-05-25.10	Gain access to approved Participating Agency's Federal System network traffic that uses CenturyLink as its Internet service provider.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.11	Establish the ability to detect malicious network traffic to support the DHS IPSS and to provide additional contextual information associated with alerts to support post-incident analysis.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.12	Support signature-based, heuristic-based and/or other emerging detection methods.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.13	Provide solutions that allow for the detection of malicious activity within encrypted traffic.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.14	Support a wide-range of unclassified and/or classified protection measures.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.15	Include the ability to redirect to a safe server.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.16	Allow for the capturing and storing of analytically relevant data associated with potential	C.2.8.9.1.4	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
	harmful network traffic specific to some indicators but and not necessarily applied to all indicators.			
TS-05-25.17	Ensure that the DHS IPSS technology does not retain traffic other than traffic associated with suspected malicious activity or as otherwise required by DHS.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.18	Apply DHS-directed prevention services, as defined and approved by the United States Computer Emergency Readiness Team (US-CERT).	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.19	Apply DHS-directed prevention services through an approved traffic segregation solution to only designated, Federal System network traffic.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.20	Operate as an in-line service (i.e., a service within the ISP network boundary per RFP Section C.2.8.9.1.4 (20).	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.21	Define and apply the full range of existing and future DHS IPSS functional capabilities (typically defined in a technology roadmap) at cyber-relevant speed to counter cyber threats and attacks.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.22	Provide quarantined malware to Participating Agency and to DHS via the US-CERT malware lab or other specified DHS entity.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.23	Prior to utilization of cyber threat indicators, signatures, and/or countermeasures, demonstrate to the government that cyber threat indicators, signatures, and/or countermeasures provided operate as intended.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.24	Provide DHS and Participating Agencies with detection alerts and associated contextual information around suspicious traffic sufficient to identify the facts of a particular incident or attempted incident for protected traffic in accordance with DHS specifications or guidance.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.25	Provide DHS and Participating Agencies with data to support network traffic pattern assessments to detect and address anomalous patterns that may be indicators of malicious activity in accordance with DHS specifications or guidance.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.26	Provide DHS and Participating Agencies with information related to indicators, signatures, associated actions, and/or alerts over a given time period.	C.2.8.9.1.4	D	Demonstration that required Capability is met.
TS-05-25.27	Ensure that agency network traffic and other information are not disclosed to any party other than DHS and the agency per RFP Section C.2.8.9.1.4 (27)	C.2.8.9.1.4	D	Demonstration that required Capability is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-05-25.28	Provide test results and support a process that allows for government participation and observation in tests.	C.2.8.9.1.4	I	Provide proof of required element for inspection.
TS-05-25.29	Within 15 minutes of discovery, notify DHS of any unauthorized access, use, disclosure, or retention of Participating Agency data, and of any breach of any security or information handling requirements or additional instructions provided by DHS regarding the handling of Participating Agency network traffic, and provide relevant information to allow DHS to assess the scope of any such breach.	C.2.8.9.1.4	D	Demonstration that required Capability is met.

7.6 TS-06 TEST CASES

The test cases for test scenario 6 (TS-06, Features) are contained in ***Table 7.6.***

Table 7.6. TS-06 Test Cases

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-06-01.1	Provide Load sharing, Fail-over protection, or Diverse access points to service provider's POP(s) high availability options for CPE.	C.2.1.1.2	D	Demonstration that required Feature is met.
TS-06-01.2	(optional) Provide interworking services for an agency's VPN to transparently access agency locations that use CenturyLink's Ethernet Transport Service.	C.2.1.1.2	D	Demonstration that required Feature is met.
TS-06-02.1	Meet the 4 Bandwidth on Demand (BoD) requirements in RFP Section C.2.1.2.2 (1).	C.2.1.2.2	D	Demonstration that required Feature is met.
TS-06-02.2	Provide Reserved Protection Bandwidth per RFP Section C.2.1.2.2 (2).	C.2.1.2.2	D	Demonstration that required Feature is met.
TS-06-02.3	Provide Shared Protected Bandwidth per RFP Section C.2.1.2.2 (3).	C.2.1.2.2	D	Demonstration that required Feature is met.
TS-06-03.1	Customer Network Management (CNM)—Level 1 (Optional)	C.2.1.3.2	D	Demonstration that required Feature is met.
TS-06-03.2	Customer Network Management (CNM)—Level 2 (Optional)	C.2.1.3.2	D	Demonstration that required Feature is met.
TS-06-03.3	Equipment Protection 1:1 – GFP/SRE. Provide protection to the client interfaces at the SDP, where the protection channel is bridged to the failed working channel.	C.2.1.3.2	D	Demonstration that required Feature is met.
TS-06-03.4	Equipment Protection 1+1 – GFP/SRE. Provide protection switching per C.2.1.3.2 (4).	C.2.1.3.2	D	Demonstration that required Feature is met.
TS-06-03.5	Equipment protection – Network Side. Support two channels facing the network for full redundancy and equipment protection at the SDPs.	C.2.1.3.2	D	Demonstration that required Feature is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-06-03.6	Support geographically diverse wavelengths per RFP Section C.2.1.3.2 (6).	C.2.1.3.2	D	Demonstration that required Feature is met.
TS-06-03.7	(Optional) Support protected Non-Domestic and OCONUS Wavelengths per RFP Section C.2.1.3.2 (7).	C.2.1.3.2	D	Demonstration that required Feature is met.
TS-06-03.8	Protected CONUS Wavelength shall be less than 300 ms for a single failure. This feature is limited to 2,500 kilometers.	C.2.1.3.2	D	Demonstration that required Feature is met.
TS-06-03.9	Protected Metro Wavelength. Provide protection on a per-wavelength basis when delivering services in the metro areas per RFP Section C.2.1.3.2 (9).	C.2.1.3.2	D	Demonstration that required Feature is met.
TS-06-04.1	Multipoint Connection—Allow interconnection of three or more subscriber premises as defined in RFP Section C.2.4.2 (1).	C.2.1.4.2	D	Demonstration that required Feature is met.
TS-06-04.2	Special Routing—Provide different routes for PLS circuits based on the arrangements as defined in RFP Section C.2.4.2 (2).	C.2.1.4.2	D	Demonstration that required Feature is met.
TS-06-07.1	Class of Service (CoS)—Accommodate and optimize an agency's applications per RFP Section C.2.1.7.2 (1).	C.2.1.7.2	D	Demonstration that required Feature is met.
TS-06-08.1	Offer voice mail capability per RFP Section C.2.2.1.2 (1).	C.2.2.1.2	D	Demonstration that required Feature is met.
TS-06-08.2	Provide auto attendant capabilities	C.2.2.1.2	D	Demonstration that required Feature is met.
TS-06-08.3	Provide Augmented 911/E911 Service.	C.2.2.1.2	D	Demonstration that required Feature is met.
TS-06-08.4	Provide the 23 standard features for basic service listed in RFP Section C.2.2.1.2.	C.2.2.1.2	D	Demonstration that required Feature is met.
TS-06-08S.1	Sip Trunk Service will have Automatic call routing	C.2.2.1.6.2	D	Demonstration that required Feature is met.
TS-06-08S.2	Sip Trunk Service will have Bandwidth QoS management	C.2.2.1.6.2	D	Demonstration that required Feature is met.
TS-06-08S.3	Sip Trunk Service will have Trunk bursting	C.2.2.1.6.2	D	Demonstration that required Feature is met.
TS-06-08S.4	Sip Trunk Service will have Telephone number blocks (DID)	C.2.2.1.6.2	D	Demonstration that required Feature is met.
TS-06-12.1	The contractor may be required to provide CHS in an Intelligence Community Directive (ICD) 705 SCIF with size and other characteristics provided in the TO.	C.2.4.5	D	Demonstration that required Feature is met.
TS-06-13.1	(Optional) Ability to have "bare metal" physical servers on a dynamic basis with provisioning times of two hours or less.	C.2.5.1.2	D	Demonstration that required Feature is met.
TS-06-13.2	Provide Data management and analytics per the requirements in RFP Section C.2.5.1.2 (2).	C.2.5.1.2	D	Demonstration that required Feature is met.
TS-06-14.1	NONE	C.2.5.2.2		
TS-06-15.1	NONE	C.2.5.3.2		

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-06-16.1	Provide Failover Service per RFP Section C.2.5.4.2 (1).	C.2.5.4.2	D	Demonstration that required Feature is met.
TS-06-16.2	(Optional) Provide Redirection and Distribution Service (Global Load Balancing) per C.2.5.4.2 (2).	C.2.5.4.2	D	Demonstration that required Feature is met.
TS-06-17.1	GFP Maintenance: Maintain and repair SRE.	C.2.8.1.2	D	Demonstration that required Feature is met.
TS-06-17.2	Provide agency-specific NOC and SOC services per RFP Section C.2.8.1.2 (2).	C.2.8.1.2	D	Demonstration that required Feature is met.
TS-06-17.3	Support Network Testing per RFP Section C.2.8.1.2 (2).	C.2.8.1.2	D	Demonstration that required Feature is met.
TS-06-17.4	Provide Traffic Aggregation Service (DHS Only as defined in RFP Section C.2.8.1.2 (4).	C.2.8.1.2	D	Demonstration that required Feature is met.
TS-06-19.1	<NONE>	C.2.8.3.2		
TS-06-20.1	The TIC Portal shall support encrypted traffic as defined in RFP Section C.2.8.4.2 (1).	C.2.8.4.2	D	Demonstration that required Feature is met.
TS-06-20.2	Adhere to and enforce Agency Security Policies as defined in RFP Section C.2.8.4.2 (2).	C.2.8.4.2	D	Demonstration that required Feature is met.
TS-06-20.3	Support Forensic Analysis activities as defined in RFP Section C.2.8.4.2 (3).	C.2.8.4.2	D	Demonstration that required Feature is met.
TS-06-20.4	Provide reports as required by the ordering agency, including ad-hoc reports.	C.2.8.4.2	I	Demonstration that required Feature is met.
TS-06-20.5	Provide additional features and functions customized to agency's specifications not covered by the Web portal included in the basic service.	C.2.8.4.2	D	Provide proof of required element for inspection.
TS-06-20.6	Provide Custom Security Assessment and Authorization Support	C.2.8.4.2	D	Demonstration that required Feature is met.
TS-06-20.7	Enable External Network Connections as defined in RFP Section C.2.8.4.2 (7).	C.2.8.4.2	D	Demonstration that required Feature is met.
TS-06-20.8	Encrypted DMZ: Support encryption, FIPS 140-2 compliant, from the agency's SDP at the edge of the agency's WAN to the MTIPS Portal. CenturyLink shall provide encryption devices and manage the devices, as set forth in RFP Section C.2.8.4.2 (8).	C.2.8.4.2	D	Demonstration that required Feature is met.
TS-06-20.9	The MTIPS portal shall support remote access for teleworkers connecting from home or satellite offices and mobile, on-the-go workers as defined in RFP Section C.2.8.4.2 (9).	C.2.8.4.2	D	Demonstration that required Feature is met.
TS-06-20.10	The TIC portal shall Support extranet connections as defined in RFP Section C.2.8.4.2 (10).	C.2.8.4.2	D	Demonstration that required Feature is met.
TS-06-20.11	Provide an Inventory/Mapping Service as defined in RFP Section C.2.8.4.2 (11).	C.2.8.4.2	D	Demonstration that required Feature is met.
TS-06-21.1	a) Provide, operate and manage Firewalls per RFP Section C.2.8.5.2 (1) (a).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.2	b) Personal Firewalls – Provide personal firewalls or personal firewall appliances... to secure remote personal computers or small remote networks ... as required by the agency	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.3	c) Provide a Network Intrusion Prevention System per RFP Section C.2.8.5.2 (1) (c).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.4	d) Provide host based Endpoint Protection per RFP Section C.2.8.5.2 (1) (d).	C.2.8.5.2	D	Demonstration that required Feature is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-06-21.5	e) Provide a Secure Web Proxy per RFP Section C.2.8.5.2 (1) (e).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.6	f) Provide Inbound Web Filtering per RFP Section C.2.8.5.2 (1) (f).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.7	g) Provide an Application-Level Gateway per RFP Section C.2.8.5.2 (1) (g).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.8	h) Provide the capability for Network Behavior Analysis per RFP Section C.2.8.5.2 (1) (h).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.9	i) Provide capabilities that extract objects from network traffic and examine those objects using real-time binary and execution engine analysis.	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.10	j) Provide Email Forgery Protection and Filtering per RFP Section C.2.8.5.2 (1) (j).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.11	k) Provide Email Content Analysis and Sandboxing per RFP Section C.2.8.5.2 (1) (k).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.12	l) Support User Authentication Integration per RFP Section C.2.8.5.2 (1) (l).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.13	m) Provide DNS security capabilities described in NIST SP800-81-2 to Ensure data integrity and source authentication.	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.14	n) Provide capabilities to block or redirect network traffic based on manipulation of DNS query responses.	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.15	o) Provide capabilities to discover and identify sensitive data and to manage, monitor, and protect it from being deleted, destroyed or divulged.	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.16	p) Support Demilitarized Zones (DMZs) per RFP Section C.2.8.5.2 (1) (p).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.17	q) Support connections to extranets which can facilitate inter-agency interactions or enable the agency to interface with trusted stakeholders.	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.18	r) Support firewall-to-firewall VPNs which establishes secure tunnels between agency firewalls, and also between firewalls and CenturyLink's operation center.	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.19	s) Provide remote agency users with secure access to the network, employing VPN encryption technology.	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.20	t) EINSTEIN 2 – interact with DHS to obtain indicators, establish US-CERT event feeds, and provide EINSTEIN network flow and detection capabilities for agency-specified traffic.	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.21	u) Provide storage capacity to retain at least 24 hours of agency-specific data generated by the MPS. Traffic shall be selectively filtered and stored, and retained data shall be made securely available to the agency.	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.22	v) Provide storage capacity to retain a year of agency-specific data generated by the MPS.	C.2.8.5.2	D	Demonstration that required Feature is met.

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
TS-06-21.23	Traffic shall be selectively filtered and stored, and retained data shall be made securely available to the agency. w) Agency-specified policy enforcement.	C.2.8.5.2	I	Provide proof of required element for inspection.
TS-06-21.24	a) Provide the agency with the ability to integrate the service into its own tools and applications… as required by the agency.	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-21.25	a) Provide Advanced Analytics per RFP Section C.2.8.5.2 (3) (a).	C.2.8.5.2	D	Demonstration that required Feature is met.
TS-06-25.1	Provide capabilities that apply sensitive and classified (up to TS/SCI) indicators and countermeasures offered by DOD/DHS to email messages and with real-time secure exchange with DHS for global awareness.	C.2.8.9.2	D	Demonstration that required Feature is met.
TS-06-25.2	Provide capabilities that apply sensitive and classified (up to TS/SCI) indicators and countermeasures offered by DOD/DHS to DNS queries and responses and with real-time secure exchange with DHS for global awareness.	C.2.8.9.2	D	Demonstration that required Feature is met.
TS-06-25.3	Additional countermeasures as specified by DHS.	C.2.8.9.2	D	Demonstration that required Feature is met.
TS-06-27.1	Provide new “networking and security service-related equipment” “incidental to the installation, operation and maintenance of EIS services”	C.2.10	D	Demonstrate that the new equipment provided in response to each EIS TO performs to manufacturer’s specification, CenturyLink EIS design criteria and TO technical requirements.
TS-06-27.2	Warranty arrangements (to accompany provided equipment) in place and warranty process, terms and conditions are understood by the agency and GSA.	C.2.10.1	I	Successful re view and acceptance of warranty information and process with agency.
TS-06-29.1	Provide installation services	C.2.12	D	Demonstrate that CenturyLink installation services support the requirements of the TO, complies with each appropriate standard, and fully complies with all applicable codes, and accepted practices.
TS-06-29.2	Provide appropriate cabling and wiring…”in accordance with the TO and appropriate standards”	C.2.12	D	Demonstrate that CenturyLink installed cabling and wiring supports the requirements of the TO, complies with each appropriate standard, and fully complies with all applicable codes,

Test Case ID	Test Case Description	Requirement References	A, D. I or M	Expected Output(s)
				and accepted practices.
TS-06-29.3	Provide trenching…"in accordance with the TO and appropriate standards"	C.2.12	D	Demonstrate that any provided trenching supports the requirements of the TO, complies with each appropriate standard, and fully complies with all applicable codes, and accepted practices.
TS-06-29.4	Provide ducting…"in accordance with the TO and appropriate standards"	C.2.12	D	Demonstrate that any provided ducting supports the requirements of the TO, complies with each appropriate standard, and fully complies with all applicable codes, and accepted practices.
TS-06-29.5	Provide grounding…"in accordance with the TO and appropriate standards"	C.2.12	D	Demonstrate that any provided grounding supports the requirements of the TO, complies with each appropriate standard, and fully complies with all applicable codes, and accepted practices.
TS-06-29.6	Provide lighting protection systems…"in accordance with the TO and appropriate standards"	C.2.12	D	Demonstrate that any provided lightning protection system supports the requirements of the TO, complies with each appropriate standard, and fully complies with all applicable codes, and accepted practices.

7.7 TS-07 TEST CASES <RESERVED>

<RESERVED>

8.0 TEST EXECUTION (E.2.2.1, E.2.2.4)

Upon receipt of a TO, CenturyLink will develop the test case books as defined in Section 5.0. CenturyLink will use test data sets that reflect real-world service conditions and locations and address all relevant test cases. Once the test cases to be performed at each site (and between sites) are finalized, CenturyLink will ensure that all test equipment, data terminals, load boxes, test cables, and any other hardware and software required for testing are provided. To ensure that real world situations are met, the test data sets and conditions (such as load peaks) that may be used will be applied as appropriate for each test. At this point, test execution can begin. During this activity, government representative(s) may observe all or any part of the EIS services verification testing.

The sequence of test operations defined in Section 6.0 will be followed for each service tested. Once each milestone has been achieved, a checkpoint will be made of the tests conducted to that point and the conditions under which they were conducted. This will be done in a two phase arrangement, first at the group of service demonstration sites, and then adding the remaining agency sites ordered.

If, during any stage of this sequence of test operations a test fails, then a defect is opened and assigned to the appropriate CenturyLink resource that will assess the root cause of the defect and its priority/severity. Once the status has changed to “fixed”, then the test will fallback to the conditions that existed at the previous milestone and retesting will occur. When all applicable milestones have been reached, the test will be considered completed.

9.0 TEST RESULTS (E.2.2.5)

CenturyLink will complete verification and acceptance testing based on the acceptance criteria defined in the government accepted EIS Test Plan.

9.1 TEST ACCEPTANCE

With the exception of the standard provisioning intervals defined in RFP Section G.8.2.2.1, provisioning intervals and schedules (as applicable) are defined on a TO by TO basis. Scheduling for these tests will be done in accordance with the order of

operation as defined in this plan. Verification and acceptance testing as described in this plan will occur toward the end of the provisioning process and upon successful completion of these tests, a service order completion notice (SOCN) will be issued to define the effective billing date.

Upon SOCN notification that the service has been tested by CenturyLink and is ready for operation, the government may choose to complete acceptance testing based on the acceptance criteria defined in this plan with the right to perform additional tests to confirm proper operation of a delivered EIS service as defined by the TO. If problems are not detected by the government during this test period, the effective billing date will be the completion date stated in the SOCN. If the government rejects the services within three days of receipt of the SOCN or within a time period specifically defined within the TO, an effective billing date will only be defined if corrective actions are implemented, a new SOCN is issued and the government subsequently accepts the service. The service will be considered accepted if the government does not reject the service within the three day period.

On a case-by-case basis, the GSA CO or the OCO may:

1. Direct a repeat of the procedure

2. Withdraw the service from acceptance testing

3. Direct CenturyLink to facilitate the return of the services to their original provider (for services transitioned or migrated from another contractor's network);

4. Request a replacement of the service (in whole or in part); or

5. Cancel the service order without penalty.

If the government elects option 1, CenturyLink will initiate corrective actions to remedy the problem reported on the trouble ticket and keep the government informed of progress. If the government exercises any of these options, CenturyLink recognizes that it will be responsible for all related expenses incurred by the government. Waiver of the acceptance testing may be considered in those instances when CenturyLink has demonstrated that the problems encountered are not the fault of CenturyLink and the government has determined that CenturyLink has taken all reasonable actions to

correct all problems. In these cases, CenturyLink will notify government of the details surrounding the deficiencies and the steps taken to overcome the deficiencies. If a waiver is not granted, CenturyLink will continue to attempt correction of the deficiencies encountered in order to successfully accomplish the acceptance testing.

Due to the nature of the required communication and documentation, CenturyLink will use the structure shown in ***Table 9.1*** which tracks each test case step and its pass/fail status. If there is a rejection by the government, retesting will occur after the rejection is addressed and a new SOCN issued to start the three day clock again.

Once complete, a SOCN is issued and if there is no rejection by the government within three days of receipt, a test case form will be generated using all the elements listed in ***Table 9.1***. This form will have spaces for signatory acceptance of the test by authorized government personnel as well as the SOCN issue date so a de facto acceptance will occur three days after the SOCN is issued, if there is no rejection notification by the government and a government individual does not choose to exercise the right to a formal sign-off. The forms completed for each test will then be compiled to form the EIS testing report.

Table 9.1. Test Case Reporting Elements

Test Case Element	Description
Test case name	Literal name of the test case being conducted
Test case description	Description of what will be covered in the test case
Precondition	Any precondition that needs to be noted prior to the execution of the test case. Can also identify previous test cases that this test case may be predicated on.
Test case start date	Provides the date the test case begins
Test case end date	Provides the date the test case concludes with full passing
Test case status	Provides the current status of the test case
Test case number	ID for the specific test case
Scenario	Identifies, in the individual steps, which test scenario is being covered: 1=Cloud Services A&A 2=KPIs & SLAs 3=Dark Fiber 4=Access and Interfaces 5=Technical Capabilities 6=Features 7=TO-Specific
Step number	Identifies the step number being performed
Manual or system step	Identifies the step as a M=Manual or A=Automated step
Description	Provides a full description of what is being run in the test step. Identifies either the manual or

Test Case Element	Description
	system step being executed or required.
Test data set	Identifies the data set being used in the execution of the test case
Additional information	Identifies additional information required for the steps (pre-conditions, pre-loaded data, etc.)
Expected results	Describes the expected result of the test case step. Identifies the threshold for a pass on the step.
Actual results	Describes the actual results after executing the test step.
Test case pass/fail indicator	Flagged accordingly
Notes/comments	Text field used for useful commentary on the test step, execution, or results of the test step.
Acceptance: SOCN issue date plus 3	
Acceptance: Government Reviewer Name/Date	
Acceptance: Government Reviewer Signature	

9.2 DELIVERABLES (E.2.2.6)

As a living document, the EIS Services Verification Test Plan will be updated when services test requirements change or if new services are added to the contract and a revision history will be maintained as shown in the table following the table of contents.

The EIS testing report that was prepared as described in Section 9.1 will be provided to the government for its records within three days after completion of service installation and testing.