Addendum 1

UCaaS CISCO POWERED SOLUTIONS PORTFOLIO CONNECTIVITY DESCRIPTION: Global VPN Service

This Addendum is part of the Service Schedule for the UCaaS Cisco Powered Solutions Portfolio and describes the parameters of the Global VPN Service Option available to Customer when configuring the Solution.

GLOBAL VPN SERVICE OPTION

A) Service Description. Supplier shall provide connectivity between Customer and the Solution on the Supplier Network through global virtual private network connectivity which provides users at distributed locations with secure, reliable remote access via broadband and wireless and subject to the Service Terms.

1. **Trunking over VPN:** In this option the interconnection trunking is provided over MPLS network (COS 1), with the exception of the multimodal functionality, which is provided over MPLS network (COS 2). This option allocates dedicated bandwidth for voice traffic (COS 1) and video traffic (COS 2) with stringent quality of service delivery by prioritizing the real-time voice application over other data traffic on the converged MPLS-based IP VPN.

1.1 **Global Outbound Off-Net Voice service, Global Inbound Off-Net Voice service, and Domestic Voice Service:** The Trunking over VPN solution connects Customer's premise-based voice systems – PBX/Diallers (TDM & IP), IP phones and soft phones – with Supplier's core voice infrastructure by utilizing the MPLS-based IP VPN.

1.2 **Multimodal functionality:** The Trunking over VPN solution connects Customer's video end points-based systems and its associated CPE, soft-client or hard-client PBX/call control with the core video infrastructure of Supplier utilizing MPLS based IP VPN.

The features of trunking over VPN may include the following capabilities:

i. Closed user group calls (excluding the multimodal functionality).

ii. Global Outbound Off-Net Voice Service, Global Inbound Off-Net Voice Service and Domestic Voice Service (COS 1).

iii. Multiple access speeds.

iv. Multimodal functionality (COS 2). For the multimodal functionality, Supplier shall endeavour to meet the following quality benchmarks in relation to the Supplier Network used in connection with the Service, provided, however, that these service levels shall not form part of Supplier's committed service levels:

   a. Packet Loss: <5%

   b. Latency: <150 msec one-way, on Supplier Network

v. PBX trunking capabilities over multiple protocols.

vi. Centralized dial plan management.

vii. Feature transparency – transit of signalling information end to end without interference.

viii. Performance reports for Global Outbound Off-Net Voice Service, Global Inbound Off-Net Voice Service and Domestic Voice Service with web-based reporting through Supplier provided performance management system (based on interconnect locations only).

ix. Customer portal for traffic and CDR viewing based on service subscribed by Customer.

x. MPLS-based security and priority class of service.

Note: Closed user group calls refers to voice calls from any Customer location to any other Customer location using a private numbering plan whereby the calls are configured to remain on Supplier Network between those locations.

B) Use Restrictions. Use of the VPN Option may require Customer to be licensed in India. In India Supplier provides this option as IP telephone, which allows only outbound calling under the Global Outbound Off-net Voice Service. Supplier will not commission the Services if Customer does not have the requisite regulatory approvals. Further, if proof of regulatory approval for Customer's use of the Service, where such approvals are required, is not submitted to Supplier within 60 days from the date of execution of the Order Form, then the Order Form shall be deemed terminated for cause by Supplier, without refund to Customer of any advance payments.

[End of Addendum 1]

Addendum 2

UCaaS CISCO POWERED SOLUTIONS PORTFOLIO CONNECTIVITY DESCRIPTION: Global SIP Connect Service

This Addendum is part of the Service Schedule for the UCaaS Cisco Powered Solutions Portfolio and describes the parameters of the Global SIP Connect Option available to Customer when configuring the Solution.

PART I. GLOBAL SIP CONNECT SERVICE OPTION

This Part I describes the Services that are available to Customer as part of the Solution. If a constituent Service described below is not selected by Customer in an Order Form, then the corresponding terms are not applicable to the Solution as described in that Order Form.

1. Global Outbound Off-net Voice Service.

1.1 Service Description: Supplier shall provide Customer with termination of international telecommunications traffic (IDDD type) which Customer has originated from the Webex Calling platform and which Cisco delivers to Supplier for termination to those international destinations. If a new route is created after the completion of the Order Form, Supplier may notify Customer of new routes via email or by posting on the Portal. Customer shall be responsible for monitoring the Portal for information on new Global Outbound Off-Net Voice Service routes.

1.2 Use Restrictions: Customer shall not send domestic national calling (also referred to as intra-country, interstate, and/or intrastate traffic) to Supplier under the Global Outbound Off-net Voice Services. If Customer fails to comply with this Section, Supplier may reroute the call(s) back to Customer for completion on the PSTN network of Customer's local carrier.

2. Domestic Voice Service.

2.1 Service Description: The Domestic Voice Service includes two separate and distinct services: (1) the IP outbound off-net voice service ("**Outbound Voice Service**") and; (2) the IP inbound off-net voice service ("**Inbound (DID) Voice Service**"). Customer may order one or both Services individually on the Order Form. The addition of Domestic Voice Services in new countries shall require the execution of a new Order Form.

2.1.1 Outbound Voice Service: Supplier transmits outbound voice calls placed by Customer to locations in the same local calling area or in the same national calling area.

2.1.2 Inbound (DID) Voice Service: Supplier transmits Inbound **DID** voice via the Session Initiated Protocol ("**SIP**") connection between Supplier and Customer. Supplier shall use commercially reasonable efforts to obtain required local Domestic Voice numbers as soon as practicable, and to work with the underlying carrier on switched translations and testing.

2.2 Domestic Voice Services are available in the countries which are identified in Addendum 5 (Domestic Voice Countries)**,** which is available here **https://www.tatacommunications.com/legal/terms-conditions/** and is incorporated herein by reference.. Customer must submit a new Order Form to receive Domestic Voice Services in any new countries added by Supplier from time to time. Additional terms and conditions also may apply to new countries and these terms will be added to the Order Form.

2.3 Domestic Voice Countries: The countries where Domestic Voice Services are available and the applicable use restrictions are set forth in the Global SIP Connect Addendum 5 (Domestic Voice Countries)**,** which is available here **https://www.tatacommunications.com/legal/terms-conditions/** and is incorporated herein by reference.

2.4 Customer Responsibilities:

2.4.1 Customer is responsible for the Webex Calling configuration and any required infrastructure including connectivity to connect their users to the Webex Calling services and blocking of premium rate or other high-cost numbers.

2.4.2 For the Domestic Voice Service, Customer shall deliver valid CLI of all outbound calls to Supplier at all times. The CLI must be associated with a telephone number that has been ported or provisioned for the Domestic Voice Service. If a valid CLI is not delivered to Supplier traffic, including emergency service traffic, may not complete. In addition, non-emergency Domestic Voice Service traffic delivered without a valid CLI may be terminated as Global Outbound Off-net Voice Service, subject to the terms, conditions, and rates associated with that service. Supplier will deliver any CLI presentation restrictions indicated by Customer to third party operators.

2.4.3 If Supplier provides or ports DID numbers to Customer as part of the Domestic Voice Services, despite anything to the contrary in the Agreement, the Service shall be deemed accepted when the DID numbers are delivered and/or ported to Customer in working order and Service Commencement Date shall be the date of such delivery/porting.

2.5 Telephone Books and Directory Assistance / Enquiries: Where required by applicable law, Supplier will put Customer's name, address and the Number(s) for the Domestic Voice Services in the telephone book published by the local provider for the respective area and make Customer's Number available to the directory assistance/enquiries database, as soon as practicable. However, subject to applicable law, Supplier will not do so if Customer instructs Supplier in writing not to do so. If Customer requires a special entry in the telephone book, Customer will be required to pay an extra charge and sign a separate agreement for that special entry. It is Customer's responsibility to verify that all directory entries are and remain correct. Supplier accepts no liability for any errors nor is Supplier liable for any costs or disputes that may arise from any omission or inaccuracy in the entry.

2.6 Australia-Specific Terms: The availability of Domestic Voice Services in Australia is subject to Customer executing the "Customer Service Guarantee Waiver". For Domestic Voice Services in Australia, the Domestic Voice Services are not available (i) to customers with less than AUD 3 million global revenue or (ii) if Customer's annual spend on the Domestic Voice Services in Australia is AUD 20,000 or less, or (iii) if Customer does not have a 'genuine and reasonable opportunity to negotiate the terms of the contract' with Supplier.

3. Emergency Calling.

3.1 General: Customer agrees that Supplier is not providing termination services to emergency numbers such as 120, 911 and 999 under this Service Schedule, except where Customer orders Domestic Voice Service from Supplier.

3.2 Release: Customer agrees that Supplier, its affiliates, directors, officers, employees, agents, underlying local provider(s) or other third party providers will not be liable for any injury, death, or damage to persons or property, arising directly or indirectly out of, or relating in any way to the Emergency Services, including without limitation any inability on the part of Customer or an End User to access the Emergency Service, unless such claims or causes of action arise from Supplier's gross negligence, recklessness, or wilful misconduct. Notwithstanding anything to the contrary contained in this Service Schedule, Customer shall indemnify and hold harmless Supplier, its affiliates and their respective directors, officers, employees, agents, underlying local provider(s) or other third party providers from any liabilities, claims, damages, losses and expenses (including reasonable legal fees and expenses) which Supplier, its affiliates or any of their respective directors, officers, employees, agents, underlying local provider(s) or other third party providers may incur, arising directly or indirectly out of or relating to the Emergency Services.

3.3 Domestic Voice Service: Supplier will provide Outbound Voice Service to local emergency numbers (such as 112, 911, or 999 short-codes) in the country for **which** Customer has purchased service ("**Emergency Services**"). Customer acknowledges and agrees that differences exist between traditional telephone service and IP-based voice services (such as the Outbound Voice Service) and that the emergency calls may be handled differently than emergency calls placed with traditional telephone service. Customer expressly consents to the limitations of the Emergency Services as set forth in more detail in the Global SIP Connect Addendum 3 (Emergency Services)**,** which is available here **https://www.tatacommunications.com/legal/terms-conditions/** and is incorporated into and forms part of the Agreement. Customer may consider alternate means for accessing traditional Emergency Services.

4. Global Inbound Off-net Voice Service: ITFS, NTFS, UIFN, LNS.

4.1 Service Description: Global Inbound Off-net Voice Service: Comprises International Toll Free Service ("**ITFS**"), National Toll Free Service ("**NTFS**"), and Universal International Freephone Number ("**UIFN**") Services (also referred to as "**Toll Free Services**") and Local Number Service ("**LNS**") which are described as follows:

4.2 Toll Free Services:

4.2.1 ITFS Service Description: Subject to the local PTT or other public or private agency assigning Customer an international toll-free number, Supplier routes domestic and international telecommunications traffic (Domestic Direct Distance Dialling/International Direct Distance Dialling (DDDD\IDDD) type) and provides service from various domestic and international origination points as specified in the Order Form. The ITFS Service is a direct dial toll-free service. Supplier shall use commercially reasonable efforts to obtain required international toll-free numbers as soon as practicable, and to work with the underlying third-party supplier on switched translations and testing.

4.2.1A NTFS Service Description: In countries that require a different numbering format for domestic inbound telecommunications traffic, and subject to the local PTT or other public or private agency assigning Customer a national toll-free number, Supplier routes domestic telecommunications traffic (Domestic Direct Distance Dialling (DDDD) type) and provides service from various domestic origination points as specified in the Order Form. The NTFS Service is a direct dial toll-free service. Supplier shall use commercially reasonable efforts to obtain required domestic toll-free numbers as soon as practicable, and to work with the underlying third-party supplier on switched translations and testing.

4.2.2 UIFN Service Description: UIFN is an option of ITFS that enables Customer to be allocated a unique toll-free number that may be accessed from multiple countries. The same number may be used from countries providing UIFN and from those countries with which Supplier has an express agreement for UIFN.

(a) Operational Requirements: The UIFN format is as follows: + 800 xxxxxxxx, where "+" is the international access code, "800" is the three digit country code for a global service application and "x" is the eight digit global subscriber number. Calls generated through the Toll-Free Services may be transmitted to Customer designated termination numbers via PSTN connections. Since 800 as the country code is an integral part of the number, all calls must be dialled as international calls. The ordering and implementation procedures are defined in the ITU-T Recommendations E.169, a copy of which can be obtained from Supplier upon request. Supplier will begin testing after confirmations from the ITU that the UIFN are assigned to Customer. Customer acknowledges that each UIFN must be implemented within 90 days of the date of the ITU assignment.

4.2.3 Rates: Additional ITFS, NTFS and UIFN Fees: Customer shall pay to Supplier:

(a) an implementation fee for each ITFS number ordered;

(b) an implementation fee for each NTFS number ordered;

(c) an implementation fee per origin country implemented; and

(d) the fee that Supplier is required to pay to the ITU Council pursuant to ITU Decision 464, 1996 Session for each UIFN requested (excluding alternative UIFNs), regardless of whether a UIFN is assigned and/or implemented.

4.3 Local Number Service ("LNS"):

4.3.1 Service Description: The Local Number Service includes Local Origination from direct inward dial ("**DID**") numbers. Supplier routes the traffic and provides the service from various local origination points around the world as specified in the Order Form. The LNS is a direct dial service. Calls generated through the LNS may be transmitted to Customer designated termination numbers via PSTN connections.

4.3.2 Operational Requirements: For LNS, Supplier processes Customer's calls delivered from the origination to the Point of Demarcation. To do so, Supplier translates the local number(s) into routing number(s) (or "**DNIS**") as assigned and approved by Customer. One routing number will be assigned for each local number. Customer hereby appoints Supplier as its agent for the purposes of establishing related services with domestic and international underlying third-party suppliers as may be required in connection with the LNS. In connection therewith, Customer shall execute any certifications, Letters of Agency/Authorization, or other similar documents required to facilitate Supplier obtaining local numbers(s) from the third-parties that supply them. Supplier will use commercially reasonable efforts to obtain the required local numbers(s) as soon as practicable, and to work with the underlying third-party supplier on switched translations and testing.

4.3.3 Use Restrictions: Customer agrees that the LNS is not intended to be used, and shall not be used, for making toll free calls in the United States or its territories that are converted into a DID number with an SMS database. In addition, the LNS is subject to use restrictions imposed by third party suppliers. Accordingly, Customer shall comply with the restrictions provided by Supplier prior to the provisioning any DID number and/or Services. Supplier reserves the right to revise such restrictions from time to time. Customer shall indemnify and hold Supplier harmless from any third party claims, actions or liabilities arising from Customer's violation of this Section and Supplier may cancel and/or temporarily suspend any or all of the Services if Customer engages in activities that violate this Section.

5. (a) Audio Conferencing Service – India.

(i) **Service Description:** Supplier offers the Audio Conferencing Service in India, which involves arranging the necessary domestic toll free ("**DTF**") numbers in India for Customer to access an India conference bridge. Supplier shall use commercially reasonable efforts to obtain the DTF numbers requested by Customer or its ordering Affiliate as soon as practicable.

(ii) **Use Restrictions for Users in India:** For a Solution that includes the Audio Conferencing Service, the Solution may involve multiple bridges located in different locations around the world that together establish a single conference session. In such situations, one of these bridges located outside India acts as the master bridge ("**Master Bridge**") and the other bridges act as secondary bridges ("**Secondary Bridges**"). Accordingly, in this circumstance the call flow for the Service is as follows: i) a user in India dials a local number and gets connected to a conference involving multiple bridges via a Secondary Bridge located outside of India; ii) the Master Bridge outside of India co-ordinates the conference by authenticating the identity of the participants dialling into the different Secondary Bridges allowing them to access the Master Bridge. Where an India caller is accessing a conferencing bridge that is located outside India Customer shall not permit any portion of the conference call session to loop back within the geographical boundaries of India.

(b) Audio Conferencing Service – Indonesia

(i) **Service Description:** Supplier offers the Audio Conferencing Service in Indonesia, which involves arranging the necessary domestic toll free ("DTF") numbers in Indonesia for Customer to access an Indonesia conference bridge. Supplier shall use commercially reasonable efforts to obtain the DTF numbers requested by Customer or its ordering Affiliate as soon as practicable.

(ii) **Use Restrictions for Users in Indonesia:** For a Solution that includes the Audio Conferencing Service, the Solution may involve multiple bridges located in different locations around the world that together establish a single conference session. In such situations, one of these bridges located outside Indonesia acts as the master bridge ("**Master Bridge**") and the other bridges act as secondary bridges ("Secondary Bridges"). Accordingly, in this circumstance the call flow for the Service is as follows: i) a user in Indonesia dials a local number and gets connected to a conference involving multiple bridges via a Secondary Bridge located outside of Indonesia; ii) the Master Bridge outside of Indonesia co-ordinates the conference by authenticating the identity of the participants dialling into the different Secondary Bridges allowing them to access the Master Bridge. Where an Indonesia caller is accessing a conferencing bridge that is located outside Indonesia Customer shall not permit any portion of the conference call session to loop back within the geographical boundaries of Indonesia.

6. Customer Responsibilities: Customer shall be responsible for the following:

(a) Customer PBX/dialler/call controller routing reconfiguration and any required inside wiring to connect Services to PBX/dialler/call controller.

(b) Configuring Customer PBX/dialler for non-international routing and Emergency Service calls (e.g. E911 in the US) per applicable regulations.

(c) For the Global Outbound Off-Net Voice Service over dedicated/public IP network, for maintaining and having the relevant regulatory operating licenses for international and in-country off-net calls.

(d) For the Global Outbound Off-net Voice Service, for delivering valid CLI of all outbound calls to Supplier at all times. If a valid CLI is not delivered to Supplier traffic may not complete. Supplier will deliver any CLI presentation restrictions indicated by Customer to third party operators.

(e) For Services provided in India, for partitioning platform (i.e. PBX) configuration and keeping call flows routed towards Global SIP Connect Service separate from other call routing flows. Customer agrees not to provide conferencing for calls from Supplier Network net to domestic off-net destinations in India.

(f) For Global Outbound Off-Net Voice Service or Global Inbound Off-Net Voice Services over MPLS network provided in India, for obtaining another Service Provider ("OSP") licence from the Department of Telecommunications, Government of India.

[End of Addendum 2]

Addendum 3

EMERGENCY SERVICES

This Addendum is part of the Service Schedule for the UCaaS Cisco Powered Solutions Portfolio and describes the limitations to any Emergency Services provided as part of the Outbound Voice Service. These limitations apply to Customer and its End Users.

Customer expressly consents to the limitations of the Emergency Services as set forth in more detail in Global SIP Connect Addendum 3**,** which is available here **https://www.tatacommunications.com/legal/terms-conditions/** and is incorporated herein by reference. Customer may consider alternate means for accessing traditional Emergency Services.

Addendum 4

UCaaS CISCO POWERED SOLUTIONS PORTFOLIO CONNECTIVITY DESCRIPTION: SDWAN

This Addendum is part of the Service Schedule for the UCaaS Cisco Powered Solutions Portfolio and describes the parameters of the Software Defined Wide Area Network ("**SDWAN**") Service Option available to Customer when configuring the Solution.

A) SDWAN SERVICE OPTION

Supplier shall provide connectivity between Customer and the Solution on the Supplier Network through SDWAN as described in more detail below.

1. Service Description.

IZO SDWAN Service is a managed tunnel overlay network service that may be delivered in connection with a Supplier-provided physical network connectivity ("**Underlay Network**") or a customer-provided Underlay Network ("**Bring Your Own Network**" or "**BYON**"). BYON allows Customer to connect a third-party network that it has procured separately from the Solution to the Supplier-provided and managed Solution components, such that the BYON is integrated with the Supplier-provided and managed Solution. IZO SDWAN Service is available in two variants: i) IZO SDWAN Select Service; and ii) IZO SDWAN Prime Service.

2. Service Options Descriptions.

2.1 IZO SDWAN Select:

2.1.1 IZO SDWAN Select Description: IZO SDWAN Select Service is a managed network service using Supplier provided and managed software and hardware, Supplier cloud gateway equipment options, and a shared orchestrator to provide a secure overlay network across Customer's underlay networks and internal local area network ("**LAN**"). IZO SDWAN Select provides advanced application visibility and application aware routing to control application traffic that flows between SDWAN Service Access Points ("**SAP**"). "**Service Access Point**" or "**SAP**" means the logical or physical element that acts as the demarcation point between Customer's or CSP's domain and Supplier's domain, representing the point at which Service is available and specific Service level targets may be committed and measured. IZO SDWAN Select is available for use with the UCaaS Cisco Powered Solution with the Premium Service package; and with the add-on security Advanced package. Details on the packages are set forth below.

2.1.2 IZO SDWAN Select Service Components: IZO SDWAN Select consists of an IZO SDWAN Select service package and an "**SDWAN Edge**" at each customer site. SDWAN Edge is the virtual or physical "machine" that terminates the Supplier side of the SAP connection between the Customer and the Service Provider on one side, and one or more Customer WAN connections on the other side. The SDWAN SAP is the boundary between Customer and Supplier responsibilities. Each IZO SDWAN Select service package includes a management, monitoring, and notification feature based on Customer requirements and outlined in a Solution Design Document ("**SDD**") attached to the Order Form. Supplier will activate, monitor, and manage the Customer SDWAN overlay network as specified in the SDD. Supplier will monitor the hardware, Supplier cloud gateway equipment and underlay network circuit(s) status between SAPs and proactively notify Customer of service failures by sending an email notification to Customer. The specific SLAs for the Solution is set forth in the UCaas Cisco Powered Solutions Portfolio Service Schedule.

2.1.3 IZO SDWAN Select Service Packages: IZO SDWAN Select is available with the Premium service package. IZO SDWAN Select Premium supports the following features:

IZO SDWAN Select Premium Features
Basic Routing
Zero-Touch CPE provisioning
Basic Reporting (Packet Loss, Jitter, Latency)
Full Encryption
Any to Any Topology
Self-Service Portal
Route Based Traffic Steering
Advance Analytics & Application Visibility (DPI based)
VPN Segmentation

App Aware Traffic Steering & Load Balancing
App QoS and Adaptive Traffic Shaping
Service chain with WAN Optimization, Security elements
Path Conditioning, Packet level Forward Error Correction

2.1.4 SDWAN Select Software Defined Security Service ("SD-Security") Options: In the Order Form, Customer may select Supplier's "Advanced" security package for inclusion with the SDWAN Select component of the UCaaS Cisco Powered Solution. The Advanced package is comprised of the following features:

Features Add-On SD Security
Stateful Firewall
DOS
Application Control
IP Reputation & Filtering
URL Reputation & Filtering
SSL Inspection/Decryption

2.1.5 IZO SDWAN Select Edge Option: In the Order Form, Customer may select from virtual and physical termination "machine" options for the Supplier-side of the SAP connection between the Customer and one or more "WAN" connections on the other side. In cases where Supplier provides the IZO SDWAN Service on a physical device, a universal customer premises equipment ("uCPE") will serve as the SDWAN Edge at Customer site.

2.1.6 Proactive Notification Scope: Where the SDWAN Select Service includes Supplier-provided network link(s) Supplier will log a "branch down" ticket and troubleshoot the relevant components until the problem has been verified as fixed. Where the Solution includes a Proactive Notification option on a network that i) includes the SDWAN Edge option; and ii) is connected to the SDWAN Edge by BYON connectivity, then where Customer receives a "branch down" alert from Supplier, Customer is responsible forl troubleshooting the outage with its BYON provider. Supplier will use reasonable business efforts to assist in such troubleshooting.

2.1.7 IZO SDWAN Select SLAs: Supplier support and service SLAs are detailed in Annex A and/or Annex B of the UCaas Powered Solutions Portfolio Service Schedule and in Addendum 5. Unless otherwise stated in the Solution Agreement, Supplier is not responsible for any SLA failures, outages, or issues arising from Customer's BYON and all Supplier SLAs exclude any such trouble incidents.

2.2 IZO SDWAN Prime:

2.2.1 IZO SDWAN Prime Description: IZO SDWAN Prime is a Supplier-proprietary routing and end-to-end congestion management system for WANS based on Cisco router. IZO SDWAN Prime includes advanced application viability, centralized management, end-to-end management, and application aware routing to control application traffic that flows between SDWAN SAPs. IZO SDWAN Prime also includes a reporting platform to provide the Customer with visibility on the distribution of applications and traffic across Customer networks.

2.2.2 IZO SDWAN Prime Service Packages: The IZO SDWAN Prime component of the UCaaS Cisco Powered Solution comes with the Enhanced service package which includes Dynamic Congestion Management. The package also includes a periodic assessment ("**Periodic Assessment**") once every 6 months by an engineer who will review the Customer IZO SDWAN Prime Service against predefined criteria established by Supplier. The Periodic Assessment will result in a report to Customer that summarizes Customer network application traffic, identification of applications that could benefit from inclusion in the IZO SDWAN Service set up, and when appropriate, recommendations on CPE upgrades, network bandwidth upgrades, QoS, application routing and traffic steering rules. A summary of the components of the Advanced package is in the table below:

Advanced Package Features
Dynamic Congestion Management
Zero-Touch CPE provisioning
Basic Reporting (Packet Loss, Jitter, Latency)
Full Encryption

Any to Any topology
Self-Service Portal
Route Based Traffic Steering
Advance Analytics & Application Visibility (DPI based)
VPN Segmentation
App Aware Traffic Steering & Load Balancing
App QoS and Adaptive Traffic Shaping
Service Chain with WAN Optimization, Security elements
Path Conditioning, Packet Level Forward Error Correction

2.2.3 Dynamic Congestion Management: This Option is available with IZO SDWAN Prime Enhanced package that protects CoS-1 voice traffic on EAS and IZO Internet WAN circuits with a conforming ETP against IP network congestion. This helps reduce Packet Drops, Jitter and Round-Trip Delay for CoS-1 voice traffic for EAS and IZO Internet WAN. Supplier commits to higher service level targets for Packet Delivery, Jitter and Round-Trip delay for circuits with a conforming ETP and Dynamic Congestion Management enabled.

2.2.4 Dynamic Path Selection: This option is available with the IZO SDWAN Prime Enhanced package. Supplier has developed a unique and robust solution called Dynamic Path Selection (DPS). The service intelligently maximizes the uses of both circuits at a remote site, ensuring that the off-loading of the less critical applications is achieved in an inbound and outbound manner (symmetrical) and that the service is congestion aware to protect business critical services.

2.2.5 IZO SDWAN Prime SLAs: Supplier support and service SLAs are detailed in Annex A and/ or B of the UCaaS Cisco Powered Solution Service Schedule and in Addendum 5; otherwise stated in the Solution Agreement, Supplier is not responsible for any SLA failures, outages, or issues arising from Customer's BYON and all Supplier SLAs exclude any such trouble incidents.

B) SDWAN ADDITIONAL SERVICE LEVEL AGREEMENTS

In addition to the support and service SLAs detailed in Annex A and/or B of the UCaaS Cisco Powered Solution Schedule, the service SLAs described below also apply to SDWAN. When Supplier fails to meet a target commitment under a given SLA defined below (excluding Service Credit Exclusions) and a trouble ticket is opened, Customer will be eligible for the Service Credits set forth below.

1. Packet Delivery Ratio ("PDR") SLA.

1.1 PDR Definition: PDR is the ratio of packets that are successfully delivered, to the total packets that are sent, over the Supplier Network in a billing month, excluding packets that are not delivered due to factors unrelated to Supplier Network. Supplier commits that the PDR for relevant Solution components, as selected by Customer in the Order Form, shall comply with the PDR targets set forth in the table below.

1.2 Measurement and Calculation: PDR is measured by electronic tools native on Supplier's network, which test the PDR by sending 20 Cisco style ICMP pings of 64 Byte at a regular interval of five (5) minutes from SAP and then automatically calculates the PDR. The Service Credit is determined on a per site bases by comparing the test results against the PDR service level targets for the relevant network configuration selected by Customer.

1.3 PDR Targets and Credits: If Supplier fails to meet its PDR SLA in any given calendar month, Supplier shall provide Customer Credits, based on the Monthly Recurring Charges per affected site, as set out in the tables below.

SDWAN Prime- Dynamic Congestion Management Enabled			
Tier	**Target**	**% Packets Delivered**	**Service Credits (% of SDWAN Prime MRC)**
1, 2 & 3	**99.7%**	**100% to 99.7%**	**No credits**
		99.7% to 99	**5%**
		99% to 98%	**10%**
		98% to 95%	**15%**
		Less than 95%	**20%**

1.4 Rules:

1.4.1 Supplier provides a PDR service level target commitment for the same number of paths as number of Site(s). If, for example, a Customer has seven Site(s) Supplier will offer commitment on not more than 7 paths.

1.4.2 The PDR service level targets exclude any packets that are dropped due to congestion at Customer exit interface (Egress Hybrid WAN Port) due to inadequate availability of Customer-procured bandwidth.

1.4.3 The PDR SLA is not offered for connectivity options that include SDSL / EFM access.

2. Round Trip Delay ("RTD") SLA.

2.1 RTD Definition: Round Trip Delay is the length of time it takes for a packet to travel between two SAPs on Supplier's Network plus the length of time it takes for an acknowledgement of that packet to be received at the originating SAP. Supplier commits that the RTD between relevant Solution SAPs, as selected by Customer in the Order Form, shall comply with the RTD targets set forth in the table below.

2.2 Measurement and Calculation: RTD is measured by electronic tools native to Supplier's network, which test the RTD between SAP pairs as an aggregated monthly average of sample measurements. Each sample is measured by sending 20 Cisco style ICMP pings of 64 Byte at a regular interval of 5 minutes. The measurements are recorded, and the results are averaged monthly, per region.

2.3 RTD Targets and Credits: Provisional service level Targets between different Sites (in milliseconds) on Supplier's Network are set forth in table 1 below. Actual RTD will be based on actual PoP as per Solution. Final Numbers will be available only after successfully commissioning of the service and monitoring for period of five (5) days. If Supplier fails to meet its RTD SLA between any two SPAs in any given calendar month, Supplier shall provide Customer with a Credit as set forth in table 2 below:

Table 1- (RTD) Service Level Targets in milliseconds ("ms")

City	Chicago	Frankfurt	Hong Kong	London	Miami	Mumbai	New York	Paris	San Jose	Singapore	Sydney	Tokyo
Chicago	NA											
Frankfurt	125	NA										
Hong Kong	225	230	NA									
London	110	20	230	NA								
Miami	67	130	237	125	NA							
Mumbai	231	124	110	131	236	NA						
New York	24	100	251	90	44	220	NA					
Paris	115	16	220	14	135	125	83	NA				
San Jose	70	180	177	158	90	292	95	178	NA			
Singapore	250	195	41	195	265	75	275	185	198	NA		
Sydney	255	360	175	355	264	289	272	360	200	222	NA	
Tokyo	180	290	66	280	190	150	202	290	118	80	149	NA

Table 2- Credits

Credits	Credit - 5% MRC	Credit - 10% MRC	Credit - 15% MRC	Credit - 20% MRC	Credit - 30% MRC
RTD exceeding target value by:	up to10 ms	up to15 ms	up to 25 ms	up to 35 ms	> 35 ms

2.4 Rules:

2.4.1 Customer will be given an RTD service level target commitment for the same number of paths as number of Sites up to a maximum of 10 sites unless agreed in the Order Form.

2.4.2 RTD SLA applies to Site to Site Hybrid traffic and not for the local Internet breakout traffic.

3. Jitter SLA.

3.1 Jitter Definition: Jitter is the time variation between packet arrivals between two points on Supplier's Network.

3.2 Jitter Measurement and Calculation: Jitter is measured for real time class of service (CoS1) between SAP-SAP pairs as an aggregated monthly average of sample measurements. Each sample is measured by sending 20 Cisco style ICMP pings of CoS1 queue of 64 Bye at a regular interval of 5 minutes from SAP and then automatically calculates the Jitter.

3.3 Jitter Targets and Credits: Jitter service level target and credits are as set forth in the table below:

SDWAN Prime- Dynamic Congestion Management Enabled			
Tier	**Target**	**% Packets Delivered**	**Service Credits (% of SDWAN Prime MRC)**
1, 2 & 3	**30 ms**	**Up to 30 ms**	**No credits**
		31 ms to 40 ms	**5%**
		41 ms to 50 ms	**10%**
		More than 50 ms	**15%**

3.4 Rules:

3.4.1 Customer is offered a Jitter SLA for the same number of paths as number of Site(s) up to maximum of ten Sites unless otherwise agreed on the Customer Order Form, so that if for example a Customer has 7 site(s) Supplier will offer commitment on not more than 7 paths.

4. Additional Rules for RTD, PDR, and Jitter.

4.1 Customer shall only raise a trouble ticket and shall only be entitled to Service Credits and when the average link utilization at a SAP is less than or equal to 70% and when the problem persists consistently for at least 10 minutes.

4.2 If any Site has the Resilient or Redundant Service Availability option using dual Local Loops, the Service Credits will only apply if the backup link bandwidth is equal to the primary link bandwidth at the Site. In the event that the primary link is down and the back-up link is provided through IZO or EAS, then Site-to-Site Performance Functions are not available and any associated service targets will not apply for the period during which the primary link is down, except that for IZO the IZO RTD and PDR Performance Functions and Service Level Targets apply.

4.3 Service Level Targets shall not apply if the average packet size carried on the Service exceeds 64bytes for packets marked CoS1, or Customer presents more than 2000 Prefixes per VPN.

4.4 Where access is provided using DSL technology(s) (e.g. for EAS), the Site Availability commitments do not apply for failure or degradation due to different factors (such as noise) on the copper lines between the Managed CPE and the DSLAM.

4.5 Because many factors influence data transmission over DSL, 3G/4G/5G or VSAT access, the public Internet and the Service Gateways, Supplier does not commit to any availability of bandwidth for the Extended Access Service between the Site and the Service Gateway, nor to any Packet Delivery Ratio, Round Trip Delay, or Jitter Service Level Target. Further not right to terminate the affected Service accrues to Customer in such circumstances.

4.6 For the IZO SDWAN Select Service option, RTD, PDR, and Jitter are measured between PoPs, rather than end-to-end.

5. SDWAN Select Reporting Portal SLA.

IZO SDWAN Select includes an analytics portal that provides Customer with data on network utilization, including a list of applications and related performance metrics obtained by collecting and analyzing data flow across Customer's SDWAN network. This data is collected from the SDWAN CPEs, the reports are available in near real-time, and are accessible through the Analytics portal. Reports provided by analytics portal are mainly used for Customer self-diagnosis and analysis. Customer shall not use those reports for Supplier's service SLA and credits Calculation. Below are the key reports available:

- SDWAN Site MAP
- Traffic utilization per path
- SLA Metrics reports per path and per Class of Service (COS) - Delay, Fwd delay var, Rev delay var, Fwd loss ratio, rev loss ratio, PDU loss ratio
- CPE CPU/Disk/Mem utilization
- Application utilization and activity reports
- Max bandwidth utilization by site and access circuit
- Heatmap and site availability report
- Application usage reports
- QoS utilization reports

Supplier uses standard Y.1731 based probes encapsulated within SDWAN overlay tunnels per access circuit 'Network Control' queue to measure the path SLAs. 1 probe packet is sent every '1s' and measurements are aggregated over 5 mins and exported to Analytics using IPFIX. Measurements are initiated as soon as traffic flow happens between a pair of sites and automatically stops when there are no more flows between the sites. The granularity of the data stored in the reporting portal is defined as data aggregation period. The reporting portal has the following aggregation period i.e. the duration for which data sent by the CPE devices at the Customer Site sent to the reporting application is stored in the reporting server and its level of granularity are:

Data storage sizing parameters	
Configured data export granularity on CPE [minute]	**5**
Data retention period without any aggregation [days]	**5**
Data retention period with every 15-minute aggregation [days]	**7**
Data retention period with 24-hour aggregation [days]	**365**

5.1 SDWAN Reporting Portal SLA Target: Supplier endeavors to ensure that the IZO SDWAN Select Reporting Portal is consistently available for Customer's use at least 99.9% of the time in a calendar month.

5.2 Measure and Calculation: Portal Availability is the duration in any calendar month that the portal is available for Customer to login and view the reports for the applicable sites detailed in the Order Form. Supplier shall calculate its monthly compliance with the Reporting Portal SLA as following:

Target Compliance % = ((TM- TMO) / TM) x 100

TM = total available Service minutes per Month = total minutes in a Month = 43,200
TMO=total minutes of outage

5.3 Target and Credit: Supplier's SLA target and the Customer's Credits in the event Supplier fails to meet its SLA Target are set forth in the table below:

Down time	Service Credits (% of SDWAN MRC)
>=1hour	**1%**
>=5hour	**2%**

5.4 Rules:

5.4.1 The Credit does not apply where a portal outage is due to a network related fault or the physical or software failure of a CPE. These incidents will be credited by their respective credit mechanisms.

5.5 Exclusions: No Credits are due under this SLA where the Portal is unavailable because of any of the following:

5.5.1 Causes under Customer's control such as i) CPE or local access facilities provided by Customer; ii) failure of power, circuits, services / systems that are not part of the Solution; iii) Customer's misconfiguration via self-service portal, iv) Customer supplying or Incorrect data or Site information;

5.5.2 Customer electing not to release the Service for testing, repair, or maintenance;

5.5.3 During implementation of a Customer Order or change request;

5.5.4 The underlay network bandwidth at any site that is not equivalent to the SDWAN port; or

5.5.5 Planned or scheduled maintenance on the Supplier Platform, and where a router is unavailable.

[End of Addendum 4]

Addendum 5

SERVICE COVERAGE, CITY TIER FOR CONNECTIVITY SERVICE OPTIONS

This Addendum is part of the Service Schedule for the UCaaS Cisco Powered Solutions Portfolio and describes county and/or city Tiers for the service level agreements ("**SLA**") applicable to the different connectivity Service options.

1. **Tiers.** Certain Service Level Targets ("**SLTs**") and Service Credits are dependent upon the geographic endpoints selected in the Order Form. These endpoints are grouped, by county and/or city, into "**Tiers**" (e.g. "**Tier 1**", "**Tier 2**", "**Tier 3", "Tier 4**"). Each Tier is assigned specific SLTs and Service Credits. Tiers are contained in the tables below.

1.1 Global Service Locations:

Global Tier-1	Australia	Austria	Belgium	Canada	Denmark	Finland	France
	Germany	Hong Kong	Ireland	Italy	Japan	Netherlands	Norway
	Singapore	South Korea	Spain	Sweden	Switzerland	United Kingdom	United States
Global Tier-2	Albania	Antigua & Barbuda	Barbados	Bermuda	Bosnia Herzegovina	British Virgin Islands	Bulgaria
	Cayman Islands	China	Croatia	Curacao	Czech Republic	Dominica	Dominican Republic
	Egypt	Faroe Island	French Guiana	Greece	Grenada	Guadeloupe	Haiti
	Hungary	Iceland	Indonesia	Israel	Jamaica	Kuwait	Lithuania
	Luxembourg	Macedonia	Malaysia	Martinique	Morocco	New Zealand	Pakistan
	Peru	Poland	Portugal	Qatar	Romania	Russia	Serbia
	Slovakia	St Lucia	St Vincent	Suriname	Taiwan	Trinidad & Tobago	Turkey
	Turks & Caicos Islands	United Arab Emirates	US Virgin Islands				
Global Tier-3	Argentina	Bahrain	Bangladesh	Bermuda	Bolivia	Brazil	Chile
	Colombia	Costa Rica	Ecuador	El Salvador	Estonia	Ghana	Guatemala
	Honduras	Kenya	Latvia	Mexico	Montenegro	Nicaragua	Nigeria
	Panama	Paraguay	Philippines	Puerto Rico	Saudi Arabia	Slovenia	South Africa
	Sri Lanka	Thailand	Tanzania	Ukraine	Uruguay	Venezuela	Vietnam
Global Tier-4	Algeria	Angola	Aruba	Botswana	DRC	Jordan	Kenya
	Mozambique	Namibia	Rwanda	Tanzania	Tunisia	Uganda	Zambia
	Zimbabwe						

1.2 EAS SLA Locations:

EAS SLA Tier 1	Australia, Austria, Belgium, Canada, Cyprus, Denmark, Finland, France, Germany, Hong Kong, Ireland, Japan, Luxembourg, Malta, Monaco, Netherlands, Norway, Poland, Portugal, Singapore, South Korea, Spain, Sweden, Switzerland, Taiwan, United Kingdom and the United States.
EAS SLA Tier 2	Bahrain, Bolivia, Brazil, Chile, Croatia, Czech Republic, Ecuador, Egypt, Estonia, Greece, Hungary, Israel, Italy, Latvia, Lithuania, Malaysia, Mexico, New Zealand, Peru, Russia (Moscow, St Petersburg), Slovakia, Slovenia, Saudi Arabia, South Africa, Turkey and United Arab Emirates
EAS SLA Tier 3	All other countries where available

1.3 India SLA Tier Locations:

SLA Tier	PoP and SLA Tier
Tier 1	Ahmedabad, Bangalore. Chennai, New Delhi, Emakalim Hyderabad, Kolkata, Mumbai (other than those listed in Tier 2), and Pune
Tier 2	Bhopal, Bhubaneshwar, Coimbatore, Gurgao, Guwahati, Indore, Jaipur, Jalandhar, Jamshedpur, Karnal, Lucknow, Mohali, Mumbai-BKC, Mumbai – Nelco, Mumbai-Vashi, Mumbai-VSB, Nagpur, Noida, Panaji, Park Road (U.P), Patna, Surat, Trivanthapuram, Vadodara Shivasakti, Vijayawada, and Visakhapatnam (Vizag)
Tier 3	Adoni, Agra, Ahmed Nagar, Ajmer, Allahabad, Alleppy/ Alpuzha, Alwar, Ambala, Ambattur, Amritsar, Anand (Nadiad), Asansol, Aurangabad, Bareilly, Belgaum, Bharuch, Bhilai, Bhilwara, Chandigarh, Calicut / Kozhikode, Cannore, Cuttack, Dehradun, Durgapur, Erode, Gandhinagar, Ghaziabad, GIFT (Gujarat), Guntur, Gwalior, Hassan, Himatnagar, Hissar, Hossur, Hubli, Jabalpur, Jalgaon, Jammu, Jamnagar, Jodhpur, Kakinada, Kannur, Kanpur, Kolhapur, Kollam, Kota, Kottayam, Ludhiana, Madurai, Mangalore, Meerut, Mehsana, Mysore, Nasik, Nellore, New Delhi—GK-1,Patiala, Pondicherry, Pune Shivajinagar, Raipur, Rajahmundry, Rajkot, Ranchi, Rohtak, Roorkee, Rourkela, Salem, Sambalpur, Sangli, Satara, Shimla, Siliguri, Solapur, Sonepat, Surat (Udhana),Thirussur, Tiruchirappallli, Tirupati, Tiruppur, Tumkur, Udaipur, Vododara Jambuva, Valsad, Varanasi, Vellore Warangal

[End of Addendum 5]

Addendum 6

DEFINITIONS

This Addendum is part of the Service Schedule for the UCaaS Cisco Powered Solutions Portfolio and describes defined terms used in that document. In the event of a conflict between any terms in this Addendum and definition in the General Terms governing the Solution Agreement, the definitions in this Addendum shall govern.

"**Business Day**" means any day other than Saturday, Sunday or a day which is a public holiday in the country where the Service is provided.

"**Business Hour**" means any hour from 9am to 5pm on a Business Day.

"**Caller Line Identification**" or "**CLI**" means a service whereby the caller's number is transmitted and presented to the called party.

"**Class of Service**" or "**COS**" means the priority of the IP packets that can be set and sent to Supplier Network as part of the GVPN Service Class of Service package ordered by Customer as set out in the Customer Order Form. COS values can be a combination of COS 1, 2, 3, 4, 5 or 6.

"**Class of Service Package**" means predetermined packages of Classes of Service as detailed in the Appendix and which is a standard of service ordered by Customer as set out in the Customer Order Form.

"**Customer Premises Equipment**" or "**CPE**" means equipment provided by Customer or Supplier and used in conjunction with the Supplier Network in order to receive the Service.

"**GVPN Port**" means a VPN access point to which Customer is connected to the Supplier Network via a provider edge router, and which is the Service Access Point for the delivery of Unmanaged Service to Customer.

"**Mean Time to Restore**" or "**MTTR**" is the average time to restore service for a specific connection during Service Outage(s). The length of all Service Outages related to Customer is totalled at the end of the billing month and is divided by the total number of Trouble Tickets opened by Customer for that month.

"**Planned Maintenance**" means any preventative, routine or scheduled maintenance which is performed with regard to the GVPN Service, the Supplier Network or any component thereof, which Supplier or its agents reasonably believe is necessary in order to maintain the Service or prevent or remedy a defect which may affect Customer's use or access to the Services. Supplier shall endeavor to give Customer at least seven (7) day notice of any Planned Maintenance event.

"**Qualifying Incidents**" means the incidents for which Customer raises a Trouble Ticket and which are confirmed by Supplier as a fault or Service degradation or an incident where a Trouble Ticket is raised by Supplier.

"**Qualified Down Time**" means that portion of a Qualifying Incident that is not an Exclusion.

"**Scheduled Maintenance**" means any maintenance of the Supplier Network or to any Supplier Network element which is a part of Customer's service and for which Customer shall be sent a notice of Scheduled Maintenance a minimum of 24 hours in advance. Notice of Scheduled Maintenance will be provided to Customer's designated point of contact by a method elected by Supplier (telephone, email, fax, account manager).

"**Service Access Point**" or "**SAP**" means the logical or physical element which acts as the demarcation point between Customer's domain and Supplier's domain, representing the point at which Service is available and specific Service level targets are committed and measured.

"Service Commencement Date" means (i) the date Customer has accepted or is deemed to have accepted the Services in accordance with the provisions of the MSA or applicable Service Schedule; or (ii) the date Customer begins using the Services other than for testing purposes, whichever date is earlier.

"**Service Outage"** or "**Outage**" means an instance when Customer is unable to convey traffic to one (1) or more Sites via the Supplier Network (other than an Exclusions) which results in Service Unavailability.

"**Service Unavailability**" means the duration of any Qualified Down Time experienced at a Service Access Point.

"**Site**" or "**Managed Site**" means the site owned or controlled by Customer which is directly connected to Supplier's PoP and which hosts a physical element(s) which is managed by Supplier as set out in the Customer Order Form.

"**Supplier Network**" means the telecommunications network and network components owned, operated and maintained by Supplier and its Affiliates, including points of presence ("**PoP**"). The Supplier Network does not include Customer Premises Equipment ("**CPE**") such as modems, routers, etc., local data links between a POP and Customer's location or any networks or network equipment not owned or controlled by Supplier.

"**Trouble Ticket**" means the official method used by Customer to advice Supplier of a potential Service Outage.

"**VPN**" means virtual private network.

[End of Addendum 6]