TATA COMMUNICATIONS

Addendum 1

ADDITIONAL TERMS AND CONDITIONS

This Addendum is part of the Service Schedule for the DDoS-D&M Solution and describes certain additional applicable terms and conditions.

1. Disclaimers.

1.1 Items for Which Supplier is Not Liable. SUPPLIER WILL USE COMMERCIALLY REASONABLE EFFORTS TO PROVIDE THE SERVICES; HOWEVER, SUPPLIER DOES NOT GUARANTEE THE SECURITY OF CUSTOMER'S NETWORK AND/OR DATA AND SHALL HAVE NO LIABILITY IN CONTRACT, TORT OR OTHERWISE FOR ANY CLAIM ARISING FROM OR BASED ON UNAUTHORIZED ACCESS TO, OR ALTERATION, THEFT OR DESTRUCTION OF CUSTOMER'S FACILITIES, EQUIPMENT OR DATA FILES.

1.2 Upgrades notifications. Supplier is not obliged to, but may from time to time, provide notifications to Customer that upgrades and/or software patches have been made generally available by the vendor(s). The decision of whether to implement and install any such upgrades and/or patches is Customer's final decision. Supplier is not liable for any damage or harm caused by such actions or inaction.

1.3 Supplier shall not be liable for any service failures or delays (including without limitation, delays in provisioning and implementation) resulting from inaccurate or incomplete data or information provided by Customer.

2. Third Party Products.

Use of third party product(s) supplied as part of Solution is subject to the manufacturer's terms and conditions which will be provided to Customer upon delivery. Supplier will pass any third party product warranties through to Customer, to the extent Supplier is authorized to do so. Customer agrees to indemnify Supplier against any claims made by third parties with respect to Customer's misuse of such third party product(s) supplied hereunder.

3. Audit.

Once per calendar year and at Customer's expense, and on not less than 30 days' written notice, Customer or its authorized representatives ("Audit Team") may audit Supplier's Facilities, records and documents pertaining to the Supplier's provisioning of the Solution to Customer during the Term ("Audit"). For duly authorized written audit requests from a government authority, Supplier will endeavor to meet other reasonable timelines. The Audit Team shall agree in writing to: i) reasonable non-disclosure and confidentiality terms, ii) an Audit scope, and iii) an Audit schedule. Supplier shall provide the Audit Team with a copy of ISO, ISAE or other relevant reports or certifications as necessary. The Audit Team shall conduct the Audit during normal business hours and in accordance with generally accepted auditing standards. Supplier will Charge Customer Remote Hands Charges at hourly rates for all Audits except for the first 4 hours of Audit conducted in a calendar year. "Remote Hands Charges" shall mean a minimum rate of INR 15,000/hr (for India locations) and US$ 250/hr (for outside India locations) if not agreed in the audit Schedule. The Remote Hands Charges will cover Supplier costs for providing Customer access to Supplier Facilities and personnel during the Audit. The Customer will conduct Audits employing industry standard level of skill and technical knowledge. Customer represents and warrants that it will perform, or will cause to be performed, appropriate background screening of the Audit Team to ensure that the personnel are of a good repute. Supplier shall not permit members of the Audit Team that have been blacklisted or that are not properly screened to enter its Facilities. Customer will take all necessary care to avoid loss or damage to Supplier property and to prevent unnecessary and excessive consumption of Supplier personnel time. Customer will indemnify Supplier for any damage to Supplier's property and additional costs incurred by Supplier in facilitating the Audit. Access to premises or web links provided to Customer as reasonably required to perform the audit shall be subject to Customer's strict adherence to Supplier's Safety, Security, and Privacy policies and procedures. Upon completion of the audit, Customer shall share the Audit report within 30 days from the completion of the Audit otherwise the audit shall be deemed to have resulted in no findings.

4. Service Credit Claim Process and Award Rules.

4.1 If a Service Level Agreement does not expressly provide Service Credits for a Service, then no service level commitments apply for that Service.

4.2 Customer must provide Supplier with a written request for any Service Credit(s) for which it is eligible under an applicable Service Level Agreement within 30 days of the applicable event giving rise to the credit. Failure to do so will void Customer's eligibility for any Service Credit for such event(s). All claims are subject to review and verification by Supplier.

4.3 If Customer is eligible to receive Service Credits for an event under more than one service level, Customer will be entitled to receive only the Service Credit with the highest value.

4.4 In no event shall the total amount of Service Credits issued to Customer per month for any Service exceed 50% of the Services Fees invoiced to Customer for the affected Service, as applicable, for that month.

4.5 Service Credits are calculated after deduction of all discounts and other special pricing arrangements, and may not be applied against governmental fees, taxes, surcharges, local access charges or any other charges other than monthly recurring Service charges.

4.6 Service Credits will generally be reflected on the second invoice following the billing month in which the Service-affecting event occurs. The credits provided in the relevant Service Level Agreement are Customer's sole and exclusive remedies for all matters related to the Service affecting incidents giving rise to the Service Credit.

4.7 Termination of an Order Form or the Agreement due to Customer's non-payment or other breach will immediately void all accrued, but unused Service Credits.

5. **Service Activation.**

5.1 Supplier commits that the Service will be provided to the Customer on the committed ready for Service date ("CRFS Date"). The CRFS Date may be a different date to the Requested Ready for Service Date (Requested RFS Date) specified in the Order Form. The CRFS Date will be either (i) the standard service lead time of 14 Business Days commencing upon Supplier's acceptance of an Order Form in accordance with the MSA / General Terms and Conditions for Delivery of Services; or (ii) as per written notice provided by Supplier during the course of provisioning the Service. Once the Service is ready for use, Supplier will notify the Customer by email that the Service is ready for use for a Qualifying Site (Service Activation).

5.2 If the provisioning of the Service is prevented or delayed beyond the standard service lead time as a result of inaccurate or incomplete data or information provided by Customer, or failure by the Customer to take any necessary actions as advised by the Supplier for the provisioning of the Service, the Customer shall be deemed to have accepted the Service 30 days after Supplier's acceptance of an Order Form, and the Supplier may commence billing for the Service.

5.3 The Service is provided to Customer on a Qualifying Site by Qualifying Site basis.

6. **Obligation of Customer.** Customer shall assure that its and Users' use of the DDoS D&M Solution complies with written and electronic instructions for use of the Customer Portal.

7. **Proprietary Rights over DDoS-D&M Reports.** All DDoS D&M reports are Supplier proprietary information and subject to the terms specified in the Agreement.

7. **Service Limitation.** The Services are not warranted to operate uninterrupted or error free. New security threats are constantly evolving and no product or Service designed to provide protection from such threats will be able to insulate network resources from all security threats and vulnerabilities, and are no guarantee against unsolicited e-mails and undesirable internet content. The Solution is not fault tolerant and is not designed or intended for use in hazardous environments requiring fail-safe operation, including without limitation aircraft navigation, air traffic control systems, weapon systems, life-support systems, nuclear facilities, or any other applications in which product or Service failure could lead to death, personal injury, or property damage. Customer acknowledges that products or Services meant for testing, assessing, scanning or monitoring the security of network resources, including implementation and deployment, may disclose or create problems in the operation of such resources; therefore, Customer and its employees and agents represent and warrant that (i) they are fully authorized by the Customer and the owners of the network resources to enter into this Agreement and each Order Form, and (ii) they and the owners of such network resources understand and accept the risks involved which in some circumstances could include without limitation, down time, loss of connectivity or data, system crashes or performance degradation.

ADDITIONAL TERMS AND CONDITIONS (FOR DDoS–CPE, when provided as part of Solution):

Where DDoS-CPE is provided as part of the Solution, the following terms and conditions will apply:

1. With respect to software, Supplier or its Affiliate or licensor retains exclusive ownership of all software which is provided to Customer on a subscription basis as part of the DDoS-CPE provided as part of Solution and Supplier or its Affiliate or licensor, as the case may be, shall be responsible for any and all duties, charges, and applicable import taxes, including GST, VAT and/or withholding taxes, with respect to the software.

2. With respect to hardware, Supplier may sell the hardware or provide the hardware as part of the Service, as provided in the applicable Order Form, and pursuant to the terms provided below:

(a) Sale of Hardware Outright. If Customer purchases the hardware, title and risk of loss transfer to Customer at FOB Point of Origination. Customer shall be required to obtain all necessary import/export licenses to enable the hardware to clear customs and enter the country where the hardware will be maintained. Customer shall be responsible for any and all duties, charges and applicable import taxes, including GST, VAT and/or withholding taxes, with respect to the hardware. Supplier shall cooperate and reasonably assist Customer in procuring all necessary licenses and permits as appropriate.

(b) Hardware provided as Part of the Service. If Supplier provides to Customer the hardware as part of the Service, title and ownership will remain with Supplier or a Supplier Affiliate or licensor. As the owner of record, Supplier or Supplier Affiliate or licensor (as the case may be) shall (i) be the licensor of record and (ii) obtain all necessary import/export licenses related to the hardware. Supplier or a Supplier Affiliate or licensor shall be responsible for any and all duties, charges and applicable import taxes, including GST, VAT and/or withholding taxes, with respect to the hardware. Risk in the hardware transfers to the Customer from the time it is delivered to the relevant Customer Premises and Customer shall be required to pay compensation for any damage to the hardware or the cost of replacing the damaged hardware. Customer must immediately inform Supplier if the hardware is damaged in any way on or after delivery. Customer shall procure and maintain all risk applicable or appropriate insurance against loss or damage to the hardware for not less than the full replacement value of the hardware. Within 5 business days of termination of the Order Form, Customer shall return the hardware to Supplier or Supplier's Affiliate or licensor, as determined in Supplier's sole discretion.

Upon expiration or other termination of Services in relation to DDoS-CPE, Customer shall permanently delete all Supplier provided software associated with such DDoS-CPE Services and destroy any related software disks (or other media) and documentation, and certify to Supplier in writing that the foregoing has been completed.

3. Maintenance for DDoS-CPE. In some cases, DDoS-CPE will include applicable and necessary maintenance fees, at levels designated by Supplier, for any hardware and software products which Supplier is managing for Customer in its provision of the Services. In cases where the Services do not include the maintenance fees, the Customer shall be responsible for maintaining in effect all necessary maintenance services and support contracts for the applicable hardware and/or software. The Service Level Agreements will not apply for any period during which such maintenance services and support contracts are not current or are unavailable for the applicable hardware and/or software.

[End of Addendum]

Addendum 2

This Addendum is part of the Service Schedule for Managed DDoS-D&M Service Solution and describes some of the defined terms used in that document. In the event of a conflict between any terms in this Addendum and definition in the MSA/General Terms and Conditions governing the Agreement, the definitions in this Addendum shall govern.

1. DEFINITIONS.

"**Administrative Changes**" means changes to Customer's Security Contact(s) or changes to procedures for the delivery of the Managed DDoS D&M Solution.

"**Alerts**" means notification via email or pager (as specified by Customer in advance) of IP Traffic Anomalies or IP Threats that, in the opinion of Supplier, require immediate action by the Customer, to mitigate or to monitor for possible defensive action.

"**Attack Mitigation Capability**" means the level of scrubbing capacity (in Gigabits or other unit of measurement) purchased by Customer from Supplier that will be available to scrub the traffic if a Distributed Denial of Service Attack occurs.

"**Attack Notification**" means notification of an identified DDoS Attack.

"**Business Day**" means a day (other than a Saturday, Sunday or public holiday) on which commercial banks are generally open for business in the jurisdiction where Services are rendered.

"**Customer**" means Customer entity that executed the relevant Order Form to receive the Services**.**

"**Customer Portal**" means the website(s) where Customer and Users access the Service(s).

"**Cloud (On-net)**" means the Service provided to the Customer over Supplier's IP backbone to protect Customer provided IP addresses from DDoS Attack.

"**Cloud Extension (Off-net)**" means the Service provided to the Customer on IP backbone other that Supplier IP backbone, to protect Customer owned public IP addresses from DDoS Attack.

"**DDoS**" means distributed denial of service.

"**Distributed Denial of Service Attacks**" or "**DDoS Attack**" means volumetric traffic based attacks directed toward Customer's IP addresses which, if not scrubbed, are likely to materially disrupt Internet access.

"**DDoS Profile**" mean the detection boundary created by the Supplier in its infrastructure for generating the DDoS alerts for the protected IP addresses.

"**GRE Tunnel**" means the generic routing encapsulation (GRE) method used by the Supplier for sending the DDoS Attack mitigated clean traffic back to the Customer's Qualifying Site. GRE Tunnel is terminated on Customer's router.

"**IAS**" means Internet Access Service formerly known as Internet Leased Line.

"**Internet Emergency**" means an incident has affected a significant portion of Supplier's protected Customer networks, or the public internet. Such emergencies are declared through Supplier's security services operations center (S-SOC).

"**IP subnets**" is the logical subdivision of IP network provided by the Customer for provisioning the DDoS D&M Services.

"**IP Threat**" means data traffic across the Supplier IP Backbone such as viruses, buffer overloads, DDoS Attacks or other traffic, that may potentially disable, interrupt or degrade single or multiple connection(s) to the Supplier IP Backbone.

"**IP Traffic Anomaly**" means data traffic across the Supplier IP Backbone that has a pattern or characteristic recognized by Supplier as warranting investigation.

"**Monthly Recurring Charge**" or "**MRC**" means the charge payable by Customer to Supplier for each relevant Service every month during the Term.

"**Netflow Traffic Data**" means a sample of Customer's data traffic on the Supplier IP Backbone used to identify and mitigate DDoS Attack(s).

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

"**Qualifying Site**" means the internet port(s) identified by Customer to Supplier to be monitored for Distributed Denial of Service Attacks.

"**Scrubbing Device**" means equipment used by Supplier to isolate and mitigate a DDoS Attack.

"**Service**" or "**DDos D&M Service**" means, collectively, the DDoS D&M Service(s) as described in this Service Schedule.

"**Service Activation**" means when the Service becomes available for Customer's use in accordance with Addendum 1.

"**Service Credits**" shall mean the credits provided by Supplier to Customer for Service Unavailability or failure to meet other Service level targets as set out in relevant service level agreement.

"**Service Level Agreement**" means the document so entitled applicable to relevant constituents of DDoS D&M Solution.

"**Service Schedule**" means the service schedule for Managed DDoS-D&M Service Solution.

"**Supplementation**" means an amendment to the Customer Order Form which may include addition of (i) new Qualifying Site (ii) upgradation of mitigation capacity, addition / removal of: (i) IP subnets, (ii) GRE tunnel (iii) DDoS Profiles (iv) DDoS-CPE**.**

"**Supplier**" means the Tata Communications entity that has executed the relevant Order Form to provide the Services**.**

"**Supplier IP Backbone**" means the Supplier-owned and operated Internet Protocol ("IP") infrastructure.

"**Term**" means Service Term as defined in the Master Services Agreement.

"**Time to Mitigate**" means the time that Supplier takes to initiate mitigation strategies in connection with a DDoS Attack after attack detection or notification. "Time to Mitigate" does not include (a) inability to mitigate a Distributed Denial of Service Attack of a type not listed in the above definition of Distributed Denial of Service Attacks; and (b) inability to mitigate Distributed Denial of Service Attacks exceeding the Attack Mitigation Capability.

"**Traffic Anomaly Detection**" means Supplier's identification of traffic anomalies directed at a defined set of Customer IP addresses on the Supplier IP Backbone.

"**Users**" means the persons authorized by the Customer to use the Service.

2. <u>ADDITIONAL DEFINITIONS</u>:

In case the Customer has ordered DDoS-CPE, as part of Solution, following additional definitions will apply:

"**Customer Premises Equipment**" or "**CPE**" means, certain hardware and/or software provided by Supplier and installed at Supplier or Customer Premises to facilitate Supplier delivery of Managed DDoS D&M Solution.

"**DDoS-CPE**" mean the CPE for the provision of DDoS D&M Service.

"**Policy Change Request**" means any authorized request by Customer for profile changes.

[End of Addendum]