COMCAST ENTERPRISE SERVICES
PRODUCT-SPECIFIC ATTACHMENT
DDoS MITIGATION SERVICE

ATTACHMENT IDENTIFIER: DDoS Mitigation Service, Version 1.4

The following additional terms and conditions are applicable to Sales Orders for Comcast's DDoS Mitigation Service:

DEFINITIONS

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the General Terms and Conditions.

"**Estimated Availability Date**" means the target date for delivery of Service.

"**On-Net**" means a Comcast-provided internet circuit that carries internet service to a Service Location and which uses an internet backbone provided by Comcast.

"**Service(s)**" means the Comcast DDoS Mitigation Services as described in **Schedule A-1**.

ARTICLE 1. SERVICES

This attachment shall apply to the Services. A further description of the Services is set forth in Schedule A-1 hereto which is incorporated herein by reference.

ARTICLE 2. PROVIDER

Service shall be provided by Comcast Business Communications, LLC.

ARTICLE 3. SERVICE COMMENCEMENT DATE

Comcast shall inform Customer when the Service is available and performing in accordance with the "Technical Specifications" set forth in Schedule A-1 hereto ("**Availability Notification**"). Charges for Services shall begin to accrue as of the Service Commencement Date. The Service Commencement Date shall be earliest of: (A) the date on which Customer confirms receipt of and concurrence with the Availability Notification; (B) five (5) business days following the date of the Availability Notification, if Customer fails to notify Comcast that the Service does not comply materially with the Technical Specifications (defined in Article 6); or (C) the date on which Customer first uses the Service. In the event that a Service Term has not been expressly set forth in a Sales Order, the Service Term for such Sales Order shall be twelve (12) months.

ARTICLE 4. SERVICE REQUIREMENTS

4.1 Notwithstanding anything to the contrary contained herein (including, but not limited to, Articles 5.3 and 5.4), in order to provide the Service at a Service Location: (i) the Service Location must have Comcast Ethernet Dedicated Internet Service provided on a "Type I" or "Type II" basis ("**Underlay EDI Service**"), which must be ordered from Comcast and may be pre-existing or ordered in conjunction with the Service; and (ii) the applicable Underlay EDI Service (i.e., the applicable EDI circuit) must have bandwidth capacity to support the Services as determined by Comcast (the "**Bandwidth Requirement**").

4.2 The Service is provided on a per circuit basis. For the purposes of an example only, if Customer has two EDI circuits (whether at a single Service Location or at two separate Service Locations) and desires to have the Service with respect to both circuits, it will be required to order the Service with respect to each circuit and each ordered Service will constitute a separate Service for the purposes of the Agreement.

4.3 Customer acknowledges and agrees that charges may begin to accrue with respect to Underlay EDI Service and the Service at different times. For the avoidance of doubt, charges will begin to accrue with respect to the Underlay EDI Service in accordance with the PSA applicable thereto.

ARTICLE 5. TERMINATION CHARGES; PORTABILITY; UPGRADES

5.1 The charges set forth or referenced in each Sales Order have been extended to Customer in reliance on the Service Term.

5.2 Termination Charges.

A. Subject to Articles 5.2(C) and (D), in the event that Service is terminated following Comcast's acceptance of the applicable Sales Order, but prior to the Service Commencement Date, Customer shall pay Termination Charges equal to one hundred and twenty percent (120%) of the costs and expenses incurred by Comcast in installing or preparing to install the Service.

B. Subject to Articles 5.2(C) and (D), in the event that Service is terminated on or following the Service Commencement Date but prior to the end of the applicable Service Term, Customer shall pay Termination Charges

equal to a percentage of the monthly recurring charges remaining for the unexpired portion of the then-current Service Term, calculated as follows:

- **i.** 100% of the monthly recurring charges with respect to months 1-12 of the Service Term; plus
- **ii.** 80% of the monthly recurring charges with respect to months 13-24 of the Service Term; plus
- **iii.** 65% of the monthly recurring charges with respect to months 25 through the end of the Service Term; plus
- **iv.** 100% of any remaining, unpaid non-recurring charges.

Termination Charges shall be immediately due and payable upon cancellation or termination and shall be in addition to any and all accrued and unpaid charges for the Service rendered by Comcast through the date of cancellation or termination.

C. **Exclusions.** Termination Charges shall not apply to Service terminated by Customer in accordance with the General Terms and Conditions and as a result of Comcast's material and uncured breach.

D. Customer acknowledges and agrees that termination of the Underlay EDI Service shall constitute a termination of the Service and Customer shall pay Termination Charges with respect to the Service as provided herein; provided, that, if Customer terminated the Underlay EDI Service as a result of Comcast's material and uncured breach in accordance with the General Terms and Conditions, then Customer will not be obligated to pay Termination Charges with respect to the Service.

5.3 Portability. Customer may terminate an existing Service (an "**Existing Service**") and turn up a replacement Service (*i.e.*, activate Service with termination points on Comcast's network that are different than those of the Existing Service) (a "**Replacement Service**") without incurring Termination Charges with respect to the Existing Service, provided that: (a) the Replacement Service has bandwidth equal to or greater than the bandwidth of the Existing Service; and (b) Customer submits a Sales Order to Comcast for the Replacement Service within ninety (90) days after termination of the Existing Service and that Sales Order is accepted by Comcast.

5.4 Bandwidth Upgrades. Customer may upgrade bandwidth of an Existing Service without incurring Termination Charges, provided that: (a) the upgraded Service (the "**Upgraded Service**") must assume the remaining Service Term of the Existing Service, but in no event less than twelve (12) months; (b) the Upgraded Service is provided to the same Service Location as the Existing Service; (c) Customer submits a Sales Order to Comcast for the Upgraded Service and that Sales Order is accepted by Comcast; and (d) Customer agrees to pay the applicable monthly recurring charges for the Upgraded Service commencing with the upgrade.

ARTICLE 6. TECHNICAL SPECIFICATIONS; SERVICE LEVEL AGREEMENT

The technical specifications applicable to the Service are set forth in Schedule A-1 hereto ("**Technical Specifications**"). The service level agreement applicable to the Service is set forth in a Schedule A-2 hereto and incorporated herein by reference.

ARTICLE 7. CUSTOMER PORTAL

Comcast provides the Customer with a password-protected web portal ("**Portal**"), which Customer will be required to access to operate and view information regarding the Service. Customer may have the option to use the Portal to enter changes to the Customer's Service settings and configurations, subject to the availability of self-service settings and configurations, as determined by Comcast in its sole discretion.

COMCAST ENTERPRISE SERVICES
PRODUCT-SPECIFIC ATTACHMENT
DDoS MITIGATION SERVICES

SCHEDULE A-1
SERVICE DESCRIPTIONS AND TECHNICAL SPECIFICATIONS

The Services will be provided in accordance with the service descriptions and technical specifications set forth below.

I. Service Descriptions

The Service is a managed security service that includes threat mitigation functionality to respond to certain types of distributed denial of service ("**DDoS**") attacks, including volumetric and flood attacks. The Service is available to Customer on an unlimited subscription basis or an emergency basis, and is available to Legacy Customers (as defined in Section (I)(4)(A) below) as an incident-based subscription, all as described in more detail below. All versions of the Service require Customer to have Comcast provided EDI Underlay Service at the applicable Service Location which meets the Bandwidth Requirement. The Unlimited Subscription Service (as defined below) is also available to Customers on an Off-Net (as defined in Section 2 below) basis subject to the conditions herein, including those set forth in Section 2.

1. Unlimited Subscription DDoS Mitigation Service ("Unlimited Subscription Service")

A. The Unlimited Subscription Service is a subscription-based Service offering that provides Customer with proactive network detection of DDoS attack traffic, alert notifications, mitigation of attacks, and online reporting. Upon receipt of complete and accurate Customer contact and network information, Comcast will configure Customer's site(s), related IP addresses, and countermeasure options. Following Comcast's completion of such configuration, Comcast shall make three (3) attempts to schedule a call during which Customer will conduct an acceptance test to confirm that the Unlimited Subscription Service is configured in accordance with Customer's preferences after activation and to verify the operation of the Unlimited Subscription Service ("**Customer Confirmation of Unlimited Subscription Service**"). If Comcast's attempts to schedule a call are unsuccessful, Comcast shall automatically activate the Unlimited Subscription Service unless and until Customer contacts Comcast and requests that Comcast deactivate the Unlimited Subscription Service. Customer acknowledges and agrees that without Customer Confirmation of Unlimited Subscription Service, Comcast may (i) be unable to prevent DDoS attack traffic from reaching the Service Location and (ii) block legitimate traffic from reaching the Service Location.

B. Comcast monitors the Customer network traffic and will automatically detect DDoS attack traffic at the closest Comcast network edge router using filtering rules. If Comcast detects high severity DDoS attack traffic, as defined by Comcast, (a "**High Severity Attack**") after applying such filtering rules, Comcast will send an alert to Customer notifying them that the Service detected a DDoS attack.

C. During DDoS attack mitigation, Comcast will leverage Border Gateway Protocol (BGP) to route any traffic that is not filtered at the network edge router to a Comcast scrubbing center that filters malicious traffic and routes legitimate traffic back to Customer's network. After mitigation terminates, Comcast delivers all traffic to Customer's network via normal routes.

D. Customer has a choice of "On-Demand" or "Automatic" mitigation options, which are described below, under the Unlimited Subscription Service. Automatic mitigation is the default option and will apply unless Customer selects the On-Demand option. Such mitigation options are selected and applied on a per circuit basis.

i. On-Demand. Customer must authorize Comcast to initiate mitigation through the Portal or by contacting the Comcast Security Assurance Team at 877-215-5529. Once Customer authorizes Comcast to initiate mitigation for a particular circuit, such circuit converts to an Automatic circuit only during the Mitigation Incident (as defined herein) such that High Severity Attacks are mitigated automatically without Customer intervention. Upon expiration of the Mitigation Incident, the circuit reverts to On-Demand. Time to mitigate (the "**Mitigation Interval**") is the elapsed time from when the Customer authorizes Comcast to enable mitigation until Comcast initiates mitigation of any attack traffic. Mitigation of a particular attack

ceases when Comcast no longer detects such attack traffic. With respect to On-Demand, a "**Mitigation Incident**" is defined as one (1) twelve-hour (12) hour window in which Comcast provides Customer with DDoS mitigation assistance as set forth above regardless of whether Comcast provides such assistance for the full twelve (12) hours or less than twelve (12) hours. Customer acknowledges and agrees that Comcast will discontinue mitigation efforts upon the expiration of each Mitigation Incident unless instructed by Customer to continue mitigation efforts, which Customers may do through the Portal or by contacting the Comcast Security Assurance Team at 877-215-5529.

ii. Automatic. The Automatic mitigation option mitigates High Severity Attacks automatically without Customer intervention following the detection of attack traffic that exceeds pre-set thresholds. The Mitigation Interval is the elapsed time from when Comcast detects a High Severity attack to when Comcast initiates mitigation of attack traffic. Mitigation ceases when attack traffic is no longer detected.

2. Off-Net DDoS Mitigation Service ("Off-Net Service")

A. The Off-Net Service is a subscription-based service that provides Customer with proactive network detection of DDoS attack traffic, alert notifications, mitigation of attacks, and online reporting for non-Comcast circuits. For purposes of this Agreement, "**Off-Net**" means one or more multihomed internet circuits that carry internet service to the same Service Location as the Unlimited Subscription Service, and which use an internet back bone provided by a third-party service provider that is not Comcast. Upon receipt of complete and accurate Customer contact and network information, Comcast will configure Customer's site(s), related IP addresses, and countermeasure options. Following Comcast's completion of such configuration, Comcast shall make three (3) attempts to schedule a call during which Customer will conduct an acceptance test to confirm that the Off-Net Service is configured in accordance with Customer's preferences after activation and to verify the operation of the Off-Net Service ("**Customer Confirmation of Off-Net Service**"). If Comcast's attempts to schedule a call are unsuccessful, Comcast shall automatically activate the Off-Net Service unless Customer contacts Comcast and requests that Comcast deactivate the Off-Net Service. Customer acknowledges and agrees that without Customer Confirmation of Off-Net Service, Comcast may (i) be unable to prevent DDoS attack traffic from reaching the Service Location and (ii) block legitimate traffic from reaching the Service Location.

B. Customers subscribing to the Off-Net Service must also have an Unlimited Subscription Service at the same Service Location. The Off-Net Service requires a Comcast EDI Underlay Service at the same Service Location that meets the Bandwidth Requirement.

C. The Off-Net Service requires a router at the Service Location configured to Comcast specifications.

D. The Off-Net Service will be configured based on the Automatic mitigation option described in Section 1(D) above. The On-Demand mitigation option is not available for the Off-Net Service.

E. Customer acknowledges and agrees that credit allowances as described in Schedule A-2 shall not be applicable to the Off-Net Service.

3. Emergency DDoS Mitigation Service ("Emergency Service")

A. The Emergency Service is available only on an On-Net basis and is available for Service Locations for which Customer does not have an Unlimited Subscription Service.

B. Upon notification of suspicious traffic from Customer, Comcast will analyze traffic for anomaly detection and patterns to determine whether the business is under a DDoS attack. In performing this analysis, Comcast will gather the appropriate network information (*e.g.*, routable IP addresses). When authorized by Customer via the execution of a Sales Order, which will include relevant fees, Comcast will monitor Customer's incoming Internet traffic to detect and filter malicious traffic matching specific DDoS attack vectors and route legitimate traffic to Customer's network.

C. For Customers receiving the Emergency Service, applicable charges shall apply with respect to each Mitigation Incident. With respect to Emergency Services, a "**Mitigation Incident**" is defined as one (1) seventy-two (72) hour

window in which Comcast provides Customer with DDoS mitigation assistance as set forth above regardless of whether Comcast provides such assistance for the full seventy-two (72) hours or less than seventy-two (72) hours. Customer acknowledges and agrees that Comcast will discontinue mitigation efforts upon the expiration of each Mitigation Incident unless instructed by Customer to continue mitigation efforts, which Customers may do through the Portal or by contacting the Comcast Security Assurance Team at 877-215-5529. Each seventy-two (72) hour period in which Comcast provides mitigation assistance shall constitute a separate Mitigation Incident subject to additional charges; provided, however, that if Customer purchases an Unlimited Subscription Service for the applicable Service Location prior to the expiration of the Mitigation Incident, then Customer will not be charged for additional Mitigation Incidents. For illustrative purposes only, if Comcast provides mitigation assistance (i) for seventy-two (72) or fewer hours, there will have been one (1) Mitigation Incident, (ii) for one hundred (100) hours, there will have been two (2) Mitigation Incidents and (iii) for one hundred fifty (150) hours, there will have been three (3) Mitigation Incidents.

4. Incident-Based Subscription DDoS Mitigation Service ("Incident-Based Subscription Service")

A. Incident-Based Subscription Services are available only to Customers that currently have an active subscription to the Incident-Based Subscription Service (each such Customer, a "**Legacy Customer**"). The following terms will apply only to Legacy Customers.

B. The Incident-Based Subscription Service is a subscription-based Service offering that provides Legacy Customers with proactive network detection of DDoS attack traffic, alert notifications, and mitigation of attacks. Upon receipt of complete and accurate Legacy Customer contact and network information, Comcast will configure Legacy Customer's site(s), related IP addresses, and countermeasure options. Following Comcast's completion of such configuration, the parties will conduct an on-boarding call during which Legacy Customer will conduct an acceptance test to confirm that the Incident-Based Subscription Service is configured in accordance with Legacy Customer's preferences after activation and to verify the operation of Incident-Based Service.

C. Comcast monitors the Legacy Customer network traffic and will automatically drop or rate limit Layer 3 and Layer 4 traffic at the closest network edge router using filtering rules. If Comcast detects High Severity Attack traffic after applying such filtering rules, an alert will be sent to the Legacy Customer notifying Legacy Customer that mitigation is required. Legacy Customer must authorize Comcast by phone or as otherwise determined by Comcast to initiate mitigation (i.e., On-Demand) and the Mitigation Interval shall be the elapsed time from when the Legacy Customer authorizes Comcast to enable mitigation until Comcast initiates mitigation of any attack traffic. Comcast will continue its mitigation efforts with respect to a particular attack until the earlier of the time such attack traffic is no longer detected or Comcast is instructed by Customer to terminate mitigation. During the mitigation, Comcast will leverage BGP to route any traffic that is not filtered to Comcast scrubbing centers where malicious traffic will be filtered and legitimate traffic will be routed back to Legacy Customer's network. After mitigation ends, Comcast will deliver all traffic to Legacy Customer's network via normal routes.

D. For those Legacy Customers receiving the Incident-Based Subscription Service, additional charges (in addition to the monthly recurring charges (MRC)) shall apply with respect to each Mitigation Incident. With respect to the Incident-Based Subscription Service, a "**Mitigation Incident**" is defined as one (1) twelve-hour (12) hour window in which Comcast provides Legacy Customer with DDoS mitigation assistance as set forth above regardless of whether Comcast provides such assistance for the full twelve (12) hours or less than twelve (12) hours. Legacy Customer acknowledges and agrees that Comcast will discontinue mitigation efforts upon the expiration of each Mitigation Incident unless instructed by Legacy Customer to continue mitigation efforts, which Legacy Customers may do by contacting the Comcast Security Assurance Team at 877-215-5529 or as otherwise instructed by Comcast. Each twelve (12) hour period in which Comcast provides mitigation assistance shall constitute a separate Mitigation Incident subject to additional charges. For illustrative purposes only, if Comcast provides mitigation assistance (i) for twelve (12) or fewer hours, there will have been one (1) Mitigation Incident, (ii) for fifteen (15) hours, there will have been two (2) Mitigation Incidents and (iii) for twenty-five (25) hours, there will have been three (3) Mitigation Incidents.

II. Service Management. Certain settings and configurations are applied and managed on a per circuit basis, not at the Service Location level. Customer shall be responsible for setting up and maintaining an account within the Portal, including setting up a primary user and secondary users with appropriate privileges, such as administrator or read-only.

III. Disclaimer. Customer acknowledges the following additional terms for the Services:

A. When Customer Internet traffic is traversing Comcast mitigation platform, Comcast makes no guarantees that only DDoS attack traffic will be prevented from reaching the Service Location nor that only legitimate traffic will be allowed to reach Customer.

B. Comcast mitigation constitutes only one component of Customer's overall security program and is not a comprehensive security solution; instead, the DDoS Mitigation Service is intended to mitigate the impacts of certain types of DDoS attacks that are already underway.

C. Comcast makes no warranty, express or implied, that: (i) all DDoS attacks will be detected (for Customers receiving a Subscription Service (as defined in Schedule A-2)); (ii) the mitigation efforts implemented by Comcast in response to such DDoS attacks will be successful in mitigating the overall impact of the incident; or (iii) or that Comcast detection, alerting, and/or mitigation (a) will be uninterrupted or error-free or (b) will not inadvertently block non-malicious traffic. Customer also understands that there may be volumetric-based attacks that exceed the amount of traffic volume that Comcast can successfully divert.

D. Comcast's ability to provide the DDoS Mitigation Services is contingent on (i) Customer providing accurate and timely information to Comcast, including the provision of IP addresses and a list of trusted applications and sites (ii) Customer provided equipment and software (including Customer-Provided Equipment) being compatible with the Service as determined by Comcast in its sole discretion (*e.g.*, Comcast will not be able to provide a 3GB DDoS Mitigation Service if Customer has a 1GB Firewall).

COMCAST ENTERPRISE SERVICES
PRODUCT-SPECIFIC ATTACHMENT
DDoS MITIGATION SERVICES

SCHEDULE A-2
SERVICE LEVEL AGREEMENT

Except for the Off-Net Service, the Services are backed by the following Service Level Agreement ("**SLA**"):

A. Definitions

Capitalized terms not otherwise defined herein shall have the meaning ascribed to them in the DDoS Mitigation Services PSA or the General Terms and Conditions.

"**Subscription Service**" means, as applicable, the Unlimited Subscription Service or Incident-Based Subscription Service.

B. DDoS Mitigation Services - Service Level Agreement

Service	Mitigation Option	Mitigation Interval	Remedy
Emergency Service	N/A	Less than or equal to 60 minutes	No Credit
		Greater than 60 minutes	Account Credit = one (1) day of Daily Mitigation fee
Unlimited Subscription Service	On-Demand	Less than or equal to 15 minutes from Customer authorization*	No Credit
		Greater than 15 minutes from Customer authorization*	Account Credit = 1/30 of MRC
	Automatic	Less than or equal to 5 minutes from discovery of attack traffic**	No Credit
		Greater than 5 minutes from discovery of attack traffic**	Account Credit = 1/30 of MRC
Incident-Based Subscription Service	On-Demand	Less than or equal to 15 minutes from Customer authorization*	No Credit
		Greater than 15 minutes from Customer authorization*	Account Credit = 1/30 of MRC

*Comcast will notify Customer of any High Severity DDoS Attacks targeting their protected IP addresses. To commence On-Demand mitigation, Customer must authorize incident mitigation through the Portal or by contacting the Comcast Security Assurance Team at 877-215-5529. Upon Customer's authorization for incident mitigation, the "**Mitigation Interval**" will commence.

**Upon Comcast's detection of a high severity Internet traffic incident, the Mitigation Interval will commence.

Customer shall be entitled to up to one credit per day and, for any billing month, Credits may not exceed fifty percent (50%) of the total monthly recurring charge ("**MRC**"), or in the case of Emergency Service total daily mitigation fees charged in the applicable month, of the applicable Subscription Service.

In order to receive a Credit for Comcast's failure to meet the SLA detailed above, Customer must open a trouble ticket with Comcast. Customer must request a credit within thirty (30) days following the completion of the Mitigation Interval.

C. Exceptions and Terms applicable to all SLAs

1. Emergency Blocking

The parties agree that if either party hereto, in its reasonable and sole discretion, determines that an emergency action is necessary to protect its own network, the Party may, after engaging in reasonable and good faith efforts to notify the other party of the need to block, block any transmission path over its network by the other party where transmissions do not meet

material standard industry requirements. The parties further agree that none of their respective obligations to one another under the Agreement will be affected by any such blockage except that the party affected by such blockage will be relieved of all obligations to make payments for charges relating to the circuit(s) which is so blocked and that no party will have any obligation to the other party for any claim, judgment or liability resulting from such blockage.

2. Remedy Processes

All claims and rights arising under this Service Level Agreement must be exercised by Customer in writing within thirty (30) days of the conclusion of the applicable Mitigation Interval. The Customer must submit the following information to the Customer's Comcast account representative with any and all claims for credit allowances: (a) Organization name; (b) Customer account number; and (c) basis of credit allowance claim (including date and time, if applicable). Comcast will acknowledge and review all claims promptly and will inform the Customer by electronic mail or other correspondence whether a credit allowance will be issued, or the claim rejected, with the reasons specified for the rejection.

3. Exceptions to Credit Allowances

Comcast failure to meet the service objectives or the Mitigation Intervals shall not qualify for the remedies set forth herein if such failures related to, associated with, or caused by: scheduled maintenance events; Customer actions or inactions; Customer-provided power or equipment (including Customer-Provided Equipment); any third party not contracted through Comcast, including, without limitation, Customer's users, third-party network providers, any power, equipment or services provided by third parties; or an event of force majeure as defined in the Agreement.

4. Other Limitations

The remedies set forth in this Service Level Agreement shall be Customer's sole and exclusive remedies for any service interruption, liability, outage, unavailability, delay, or other degradation, or any Comcast failure to meet the service objectives and Mitigation Intervals.