verizon

DOS DEFENSE +

1. ~~**Part I:**~~ **RATES AND CHARGES.** This service attachment describes the terms and conditions for the DOS Defense Detection service ("DOS Defense Detection") or DOS Defense Mitigation service ("DOS Defense Mitigation"). DOS Defense Detection and DOS Defense Mitigation are collectively referred to herein as "DOS Defense." As of June 1, 2016, DOS Defense Mitigation services are no longer available to new customers. Existing DOS Defense Mitigation customers may move, change, and disconnect their DOS Defense Mitigation services with the understanding that renewals of such services will not be permitted. As of June 1, 2016, "DOS Defense" means DOS Defense Detection only.

1.1 **Service Commitment and Activation Date.** A Service Commitment applies for each order of DOS Defense Detection or DOS Defense Mitigation as shown in Customer's Contract. If no Service Commitment is shown, a one-year Service Commitment will automatically be applied. The Service Activation Date is the date DOS Defense has been accepted (or deemed accepted) by Customer. The billing of monthly recurring charges ("MRC") will commence on such date.

1.2 **DOS Defense Detection.** Customer will pay the applicable MRC and the applicable non-recurring charge ("NRC") based on the IP Bandwidth ordered, as shown in a Contract, and at the following URL~~:~~: www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm.
~~–~~The term "IP Bandwidth" refers to Customer's Internet service port type/speed. Any increase or decrease in Customer's Internet IP Bandwidth may result in a price adjustment ~~in accordance with the table below~~.

1.3 **DOS Defense Mitigation.** Customer will pay the applicable MRC and the applicable NRC for the Capacity ordered, as shown in a Contract, and at the following URL~~:~~: www.verizonenterprise.com/external/service_guide/reg/applicable_charges_toc.htm.
~~–~~The NRC will vary by installation option as described below and shown in a Contract. The term "Capacity" refers to the volume of total traffic that DOS Defense Mitigation will process at any given time (separating the distributed denial of service ("DDoS") attack traffic from legitimate traffic). The term "Zone" refers to

the maximum number of Customer circuits, and such circuits' associated DOS Defense Mitigation return path, which can be protected by the Capacity ordered by Customer. Verizon will use the same parameters to define which traffic is allowed or blocked for each circuit in a Zone when mitigation is activated.

1.3.1 **DOS Defense Mitigation Installation and Upgrade Options.** Customers can elect any of the following options:

1.3.1.1 **Standard Installation.** With standard installation Verizon will install DOS Defense Mitigation within 14 Business Days from Configuration Receipt as provided in the Acceptance Testing clause below.

1.3.1.2 **Emergency Upgrade.** Verizon will increase Customer's DOS Defense Mitigation Capacity with 24 hours' notice.

1.3.1.3 **Emergency Installation.** With emergency installation, Customer will pay the additional NRC shown in a Contract and Verizon will install DOS Defense Mitigation within 3 Business Days from Configuration Receipt.

1.3.1.4 **Expedited Installation.** With expedited installation, upon Verizon's approval, Customer will pay the additional NRC shown in a Contract and Verizon will install DOS Defense Mitigation as soon as commercially possible from Configuration Receipt.

~~1.2~~1.4 **Termination.** If Customer terminates DOS Defense ordered under this Service Attachment, or any portion thereof, during a Service Commitment, except for termination for Cause, such termination shall not be effective until 60 days after Verizon receives written notice of termination.

2. ~~**Part II:**~~ **SERVICE DESCRIPTION AND REQUIREMENTS~~.~~

2.1 **General.** Before activation, Customer must provide the appropriate technical configuration information and Customer Technical Point of Contact (~~"~~TPOC~~"~~) detail for the Verizon configuration engineer. Verizon will configure DOS Defense in accordance with Customer's configuration information. Customer is responsible for confirming that DOS Defense is configured in accordance with Customer's preferences prior to and after activation.

2.1.1 **Monitoring.** DOS Defense includes proactive monitoring of DOS Defense related equipment on Verizon's network for operation, capacity, utilization, and version updates of applicable software.

2.1.2 **Acceptance Testing.**

~~2.1.1.1~~2.1.2.1 Upon receipt by Verizon of complete and accurate Customer configuration information, Verizon will configure Customer's site(s) and related IP addresses and perform validation testing to verify the operation of DOS Defense (~~"~~Configuration Receipt~~"~~). Subsequent to such testing, Verizon will inform the Customer that DOS Defense is properly configured and activated (~~the "~~Verification Notice~~"~~). Additional testing prior to the issuance of the Verification Notice for DOS Defense Mitigation is described below.

2.1.2.2 Customer has five business days testing after the Verification Notice to conduct and complete acceptance testing. If the Customer fails to accept or reject DOS Defense during such five business day period, or begins utilizing DOS Defense for purposes other than testing, the DOS Defense configuration will be deemed accepted and Verizon will commence billing. If Verizon receives notice that DOS Defense is rejected, Verizon will correct the failure identified by Customer in the notice and DOS Defense will be deemed accepted within five business days of the correction unless Customer again provides notice of rejection. This notice and correction process will be repeated until DOS Defense is accepted, or until Verizon, at its discretion, elects to terminate DOS Defense.

2.1.22.1.3 **Self-Service Portal and Reports.** Verizon will make available daily traffic reports through the Verizon self-service web-based portal (the "Self-Service Portal"). Customer may make administrative changes to DOS Defense Detection by opening an administrative ticket via the Self-Service Portal.

2.2 **DOS Defense Detection Service Description.** DOS Defense Detection is a managed network-based traffic analysis service providing anomaly detection and proactive alerts when Customer's traffic deviates from normal traffic patterns. Customer must have Verizon provided dedicated Internet access of at least an E1 or T1, as applicable, to utilize the DOS Defense Detection service. All equipment associated with DOS Defense Detection resides on the Verizon network and remains the property of Verizon.

2.3 **DOS Defense Mitigation Service Description.** DOS Defense Mitigation is a managed network-based service that acts to intercept the malicious traffic utilized in a DDoS attack. DOS Defense Mitigation provides redirection of legitimate traffic and DDoS attack traffic to pre-deployed mitigation centers either by; (a) Customer's network-based redirection, or (b) Customer's notification to Verizon and Verizon's redirection. Customer must have Verizon-provided dedicated Internet access of at least an E1 or T1, as applicable, to utilize the DOS Defense Mitigation service. All equipment associated with DOS Defense Mitigation resides on the Verizon network and remains the property of Verizon.

2.3.1 **Service Configuration.** If needed, the Customer will configure the router it intends to utilize with DOS Defense Mitigation to accept a GRE tunnel. Verizon will provide Customer with examples of GRE tunnel routing upon Customer's request.

2.3.2 **Mitigation Acceptance Testing.** Verizon will make a Border Gateway Protocol ("BGP") routing announcement into Verizon's BGP routing tables, with the assistance of Customer, to test for proper configuration of DOS Defense Mitigation after receipt of the Customer configuration information. This routing update redirects designated Customer network traffic to Verizon's mitigation centers. Once Verizon has verified that the redirection is functioning and configured consistent with the Customer configuration information, DOS Defense Mitigation shall be deemed properly configured and activated and Customer will be sent the Verification Notice.

2.3.22.3.3 **Administration.**

2.3.3.1 Verizon will reroute the Customer's network traffic to a Verizon mitigation center when Verizon has received an authorized and appropriate Customer request. Verizon has the sole discretion to determine an appropriate request.

2.3.3.2 Customer may make administrative changes to DOS Defense Mitigation service (e.g., IP alterations, TPOC changes, etc.) by opening an administrative ticket via the Self-Service Portal. Customers may perform periodic DOS Defense Mitigation activation, availability, and alerting tests and review perimeters on the Self-Service Portal. The Self-Service Portal may not be used as a Customer network monitoring tool. In such case, Verizon may request Customer to stop such network monitoring overutilization or suspend Self-Service Portal access.

2.3.2.12.3.3.3 Mitigation may not be used on a continual basis or as a precautionary measure. Verizon reserves the right to stop mitigations 96 hours after Verizon has determined, in its sole discretion, that a DDoS attack has not occurred or has ceased.

3. **Part III: TERMS AND CONDITIONS.**

3.1 **Customer Obligations.** In the event of a DDoS attack, Customer is solely responsible for activating the DOS Defense Mitigation it has ordered, either by rerouting traffic to a pre-deployed mitigation center or contacting Verizon in order for Verizon to perform such rerouting function. Customer is also responsible for discontinuing the rerouting of traffic at the conclusion of a DDoS attack or requesting that Verizon discontinue such rerouting of traffic, as applicable. Customer is responsible to provide all information

reasonably requested by Verizon and that all information provided is complete, accurate, and kept current. Customer information will only be accepted from and discussed with the registered TPOC. Customer is responsible to ensure that Verizon is informed of changes to the TPOC.

3.2 **Service Testing.** At no time shall the Customer perform volumetric or capacity testing of DOS Defense Mitigation.

3.3 **Overutilization.** For DOS Defense Mitigation, Verizon will measure and monitor the volume of total traffic for the Capacity in the related Zone purchased by Customer. Any mitigation provided above the purchased Capacity will be provided at Verizon's sole discretion and at no additional charge to Customer. Verizon may use reasonable means to maintain DOS Defense Mitigation service generally to all customers, or protect its network, including stopping mitigation above the purchased Capacity and deleting Customer's traffic. If mitigation above the purchased Capacity occurs more than three times in any 90 day period, Verizon may increase Customer's Capacity, and related MRCs, for the remainder of the Service Commitment to a level it determines to be appropriate to mitigate such overuse.

3.4 **Disclaimer.** Verizon's entire liability and Customer's sole and exclusive remedies regarding DOS Defense (including without limitation relating to installation and performance) are set forth in the SLA for DOS Defense which is set forth at www.verizonenterprise.com/terms. When utilizing DOS Defense Mitigation during a DDoS attack, Verizon does not guarantee that only DDoS attack traffic will be dropped nor that only legitimate traffic will be allowed to reach Customer. Customer acknowledges and agrees that (a) DOS Defense constitutes only one component of Customer's overall security program and is not a comprehensive security solution; and (b) there is no guarantee that DOS Defense will be uninterrupted or error-free or that DOS Defense will meet Customer's requirements.

~~3.5 **Export Compliance.** Customer acknowledges that the Export Restrictions set forth in the Guide apply.~~

4. ~~**Part IV:**~~ **DEFINITIONS.** In addition to the definitions identified in the Master Terms, the following administrative charge definitions apply to DOS Defense~~:~~ :
www.verizonenterprise.com/external/service_guide/reg/definitions_toc_2017DEC01.htm~~.~~