Part I: Rates and Charges
Part III: Service Description and Requirements
Part IV: Service Level Agreement

Part I: Rates and Charges. Verizon offers Distributed Denial of Service (“DDoS”) mitigation services to help protect the availability of Customer’s Internet-connected business operations. This service attachment describes the terms and conditions for the DDoS Shield (“DDoS Shield”) mitigation service.

1. Service Commitment and Activation Date. A Service Commitment applies for each order of DDoS Shield 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 earlier of (a) the date of Verizon’s Verification Notice in accordance with Part II, Section 2.1.1 or (b) 30 days following the date of execution of this Service Attachment. The term of the Service Commitment and the billing of monthly recurring charges (“MRC”) will commence on the Service Activation Date.

2. DDoS Shield. Customer will pay the applicable MRC and NRC for the Service Tier ordered, as shown in the Contract. The term “Service Tier” refers to the Customer’s ingress bandwidth usage and number of IP subnet(s) announced to the Internet.

2.1 Installation and Upgrade Options. Customers can elect any of the following options:

   2.1.1 Standard Installation. With standard installation Verizon will install DDoS Shield within 14 Business Days from Configuration Receipt (as defined in Part II, Section 1.2 below).

   2.1.2 Emergency Installation. With expedited installation, upon Verizon’s approval, Customer will pay the additional non-recurring charge (“NRC”) shown in the Contract and Verizon will install DDoS Shield as soon as reasonably technically and commercially possible after Configuration Receipt.

3. Termination. Either party may terminate DDoS Shield, with or without Cause, effective sixty (60) days after written notice of termination is given to the other party. Customer accepts and agrees that, in the event (a) Customer terminates any order for convenience or (b) Verizon terminates any order for Cause prior to the end of the Service Commitment, Customer will pay Verizon all unpaid fees payable under this Service Attachment and the applicable order for the remainder of such Service Commitment. Customer will pay Verizon’s invoice in accordance with the terms of the applicable Contract.

Part II: Service Description and Requirements.

1. DDoS Shield Service Description. DDoS Shield is a managed, cloud-based, on-demand service designed to intercept and remove significant amounts of malicious DDoS traffic inbound to a Customer’s Internet-connected network. When mitigation is initiated, DDoS Shield announces Customer’s IP addresses (listed in the Customer IP (“CIP”) Schedule attached hereto as Exhibit A) to redirect all traffic inbound to those CIPs to Verizon’s cloud-based mitigation facilities, where Verizon filters the traffic prior to returning it to Customer via a dedicated Generic Routing Encapsulation (“GRE”) tunnel. Once provisioned, when not actively mitigating a DDoS attack, DDoS Shield is not intended to continually redirect Customer’s traffic (“always-on” configuration).

2. General. Before Verizon provisions DDoS Shield, Customer must provide the appropriate technical configuration information and authorized contact (“Authorized Contact”) details to the Verizon configuration engineer. Verizon will configure DDoS Shield in accordance with its policies as reasonably practicable to correspond to Customer’s configuration information.

2.1 Configuration and Testing.

   2.1.1 Upon receipt by Verizon of complete and accurate Customer configuration information, Verizon will configure DDoS Shield to help protect Customer’s environment when under a DDoS attack (“Configuration Receipt”) and perform validation testing to verify DDoS Shield is operational. Subsequent to such testing, Verizon will inform Customer that DDoS Shield is properly configured (“Verification Notice”) as provided in Section 2.1.2 below.

   2.2 Self-Service Portal. Verizon will make available daily mitigation traffic reports through the Verizon self-service web-based portal (the “Self-Service Portal”). Customer may request changes to its DDoS Shield configuration by opening a support ticket via the Self-Service Portal.

3. Mitigation Activation. When mitigation is initiated, both legitimate traffic and DDoS attack traffic will be redirected to pre-deployed mitigation facilities either by: (a) Customer’s redirection, if mutually agreed by the parties, or (b) Verizon
upon receipt of Customer’s notification. In order to receive DDoS Shield, Customer must have a public Internet circuit and publicly reroutable IP address space via Border Gateway Protocol (“BGP”), of at least a Classless Inter-Domain Routing (“CIDR”) /24 for IPv4 or larger. All equipment associated with DDoS Shield is housed within Verizon facilities and remains the property of Verizon.

3.1 Service Configuration. Customer is responsible for configuring the network edge router(s) it intends to utilize with DDoS Shield for purposes of accepting a GRE tunnel. Verizon will provide Customer with examples of GRE tunnel routing upon Customer’s request.

4 Administration.
4.1 Verizon will reroute Customer’s network traffic to a Verizon mitigation center when Verizon has received an authorized and valid Customer request to initiate DDoS Shield. Verizon has the sole discretion to determine whether a request is an appropriate request.

4.2 Customer may make administrative changes to DDoS Shield service (e.g., IP alterations, Authorized Contact changes, etc.) by opening a support ticket via the Self-Service Portal. Customer may perform periodic DDoS Shield initiation, availability, and alerting tests and review parameters on the Self-Service Portal. Notwithstanding the foregoing, Customer will not perform any mitigation testing of DDoS Shield without Verizon’s prior written consent and coordination with Verizon.

4.3 Mitigation may not be used on a continual basis or as a precautionary measure. Verizon reserves the right to stop mitigations 48 hours after Verizon has determined, in its sole discretion, that a DDoS attack has not occurred or has ceased.

4.4 Overutilization. Verizon will measure and monitor the volume of total traffic in the DDoS Shield Service Tier purchased by Customer. Usage in excess of such Service Tier (“Overutilization”) will be provided at Verizon’s sole discretion and at no additional charge to Customer. Customer acknowledges that, if Customer’s Overutilization averages 4 or more hours during any given active mitigation period, Verizon may deem such Overutilization as Customer’s authorization to increase Customer’s Service Commitment to the next level Service Tier as shown in Customer’s Contract, retroactive to and inclusive of the three-month period prior to the first date of such Overutilization.

5 Customer Obligations. In the event of a DDoS attack, Customer is solely responsible for initiating the DDoS Shield services it has ordered, either by contacting the Verizon DDoS Security Operations Center (“SOC”) and then upon approval rerouting traffic to DDoS Shield facilities itself or contacting the Verizon SOC and requesting Verizon to perform such rerouting function. Customer is also responsible for coordinating with the SOC the discontinuance of rerouting of traffic at the conclusion of a DDoS attack.

Part III: Terms and Conditions.

1 Customer Data.
1.1 Customer acknowledges that Verizon, Verizon Affiliates and their respective agents may, by virtue of the provision of the Services, come into possession of Customer Data, including personal and/or private information, voice and data transmissions and the originating and destination numbers and IP addresses, date, time, duration, and other data necessary for the establishment, billing or maintenance of such transmissions.

1.2 Verizon will implement appropriate technical and organizational measures to protect “Regulated Customer Data” against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access and against other unlawful forms of processing.

1.3 Verizon and its respective affiliates and agents may use, process, transfer and/or store Customer Data (including intra-group transfers and transfers to entities in countries that do not provide statutory protections for personal information): (a) in connection with provisioning of DDoS services; (b) to incorporate Customer Data into databases controlled by Verizon or its affiliates or agents for the purpose of providing DDoS services; administration; provisioning; billing and reconciliation; verification of Customer identity, solvency and creditworthiness; maintenance, support and product development; fraud detection and prevention; sales, revenue and customer analysis and reporting; market and customer use analysis; and (c) to communicate to Customer regarding the DDoS services.

1.4 Customer may withdraw consent for such use, processing or transfer of Customer Data as set out above, except as it is required to (a) provision, manage, account or bill for DDoS services; (b) carry out fraud detection; or (c) comply with any statutory or regulatory requirement or the order of a court or other public authority, by sending written notice to Verizon in the prescribed form, available from Verizon on request.

1.5 Customer warrants that it has obtained or will obtain all legally required consents and permissions from relevant parties (including data subjects) for the use, processing and transfer of Customer Data as described in this Section 1.
1.6 As part of providing DDoS services, Verizon may transfer, store and process Customer Data in the United States or any other country in which Verizon or its agents maintain facilities. By using DDoS mitigation services, Customer consents to this transfer, processing and storage of Customer Data.

2. Warranties.

2.1 Verizon Warranties. Verizon warrants to Customer that it will perform its obligations in a good and workmanlike manner. Verizon's entire liability and Customer's sole and exclusive remedies regarding DDoS (including, without limitation, relating to installation and performance) are set forth in the SLA for DDoS which is set forth at DDoS Shield Service Level Agreement. When utilizing DDoS during a DDoS attack, Verizon does not guarantee that only DDoS attack traffic will be dropped or that only legitimate traffic will be allowed to reach Customer. Verizon does not warrant that DDoS will detect and prevent all possible threats and vulnerabilities or that such services will render Customer's network and systems invulnerable to all security breaches and vulnerabilities. Customer acknowledges and agrees that (a) DDoS mitigation services constitutes only one component of Customer's overall security program and is not a comprehensive security solution; and (b) there is no guarantee that DDoS mitigation services will be uninterrupted or error-free, or that DDoS mitigation services will meet Customer's requirements.

2.2 Third Party Warranties. For any third party products and/or services incorporated as part of DDoS mitigation services, Customer shall receive only the warranties offered by such third party to the extent Verizon may pass through such warranties to Customer.

2.3 Customer Warranties. Customer represents and warrants that Customer (a) has been assigned the IP addresses listed in the CIP Schedule (and is the exclusive user of such IP addresses) by the appropriate Internet Assigned Numbers Authority (IANA) regional Internet numbers registry, (b) consents to Verizon's performance of DDoS mitigation services with respect to such IP addresses, (c) has and will continue to have all rights, power, permissions and authority necessary to, have Verizon perform DDoS mitigation services with respect to such IP addresses along with the rerouting of such IP addresses for purposes of DDoS services including, without limitation, consent of all authorized network users, (d) the deliverables, documentation, and other information provided by Verizon in connection with DDoS mitigation services will be used solely for purposes of protecting Customer from abusive, fraudulent, or unlawful use or access to its information, systems and applications including Verizon's public Internet service, and (e) will comply with all applicable laws and regulations and the provisions of Section 4 below. Customer is responsible for maintaining an up-to-date list of CIP by providing a revised CIP schedule to Verizon from time to time as required. Customer further represents and warrants that the CIP and domains provided to Verizon for purposes of receiving DDoS mitigation services are accurate and hereby assumes the sole responsibility for the accuracy of such CIP and domains. Customer will be liable for all costs and expenses from any third party claims of loss, damage (including reasonable attorneys’ fees) and liability of any kind that may be incurred as a result of Customer's breach of the foregoing warranty.

3. Third Party Products or Services. The parties agree that Verizon shall not be liable for any damages caused by hardware, software, or other products or services furnished by parties other than Verizon, its agents, subcontractors, or any damages caused by the products and/or services delivered by or on behalf of Verizon which have been modified, serviced, or otherwise attended to by parties other than Verizon or without Verizon's prior written and express consent. Customer acknowledges that Verizon shall not be liable for any damages resulting, directly or indirectly, from any act or failure to act by Customer or any third party (including, without limitation, the non-performance, defaults, omissions or negligence of any third party that provides telecommunications services in the country or countries in which Customer's premises or systems are situated and other countries from, across, to or in respect which DDoS services are provided by or on behalf of Verizon).

4. Confidential Information. Customer acknowledges that the following information constitutes “Confidential Information” hereunder: (a) the methods, systems, data and materials used or provided by Verizon in connection with the provision of DDoS services; and (b) all reports issued by Verizon in connection with such results including, without limitation, security analyses and insight (“Net Intel Information”). Customer will disclose Net Intel Information only to Customer employees with a “need to know” for the purposes set forth in this Service Attachment and who are bound to confidentiality obligations at least as restrictive as those set forth in the Agreement and this Service Attachment. In no event may Customer use lesser efforts to protect Net Intel Information from use or disclosure not permitted under the Agreement than it uses to protect its own highly-sensitive confidential information, or less than reasonable efforts. The term “Confidential Information” shall not include information that is comprised of statistical information, or other aggregated information regarding security vulnerabilities, security configurations and the like insofar as such information does not identify Customer or Customer’s computer network or computer systems.

Customer will indemnify, defend or settle and hold Verizon Indemnitees harmless from and against all losses, damages, costs and expenses (including allocable costs of in-house counsel and other legal fees) associated with any claims, suits, judgments, settlements, investigations, fines, consent decrees, requests for information, or other
dispute resolution, enforcement, regulatory or legal proceedings or actions of any kind, suffered or incurred directly or indirectly by Verizon Indemnities from or arising out of Customer's breach of any of the representations and warranties above or based on, arising out of or relating to Customer's use or interpretation of Net Intel Information provided by Verizon.

5. Customer acknowledges and agrees that DDoS mitigation services are offered and provided by Verizon to multiple customers doing business in various industries. Absent terms to the contrary in the Agreement, DDoS mitigation services are implemented without specific controls that may generally be required or customary for customers in any particular industry and is not designed to satisfy any specific legal obligations. Customer shall be solely responsible for determining that DDoS mitigation services satisfy Customer's obligations under law or contract. Customer agrees to use DDoS mitigation services in accordance with all applicable laws and not to use DDoS mitigation services in any manner that imposes obligations on Verizon under any laws other than those laws with which Verizon agrees to comply as specifically set forth in the Contract. Without limiting the generality of the foregoing, Customer agrees not to cause, or otherwise request that Verizon create, receive, maintain or transmit protected health information (as defined at 45 C.F.R. § 160.103) for or on behalf of Customer in connection with DDoS mitigation services or in any manner that would make Verizon a business associate (as defined at 45 C.F.R. § 160.103) to Customer. In the event Customer acts or uses DDoS mitigation services in a manner not permitted under this Section 5, Customer shall (a) be in material breach of the Contract, including this Service Attachment; (b) indemnify, defend and hold harmless Verizon for any losses, expenses, costs, liabilities, damages, penalties, investigations or enforcement proceedings (including attorneys’ fees) arising from or relating to Customer’s breach of this Section 5; (c) take, at Customer's expense, prompt action to correct and/or mitigate the effects of Customer’s breach of this Section 5; and (d) provide Verizon with reasonable cooperation and support in connection with Verizon's response to Customer's breach of this Section 5. Customer shall assume and be solely responsible for any reporting requirements under law or contract arising from Customer's breach of this Section 5.

6. **Export Compliance.** Customer agrees to comply with all applicable export, import and economic sanctions laws and regulations. Customer represents and warrants that Customer (a) will not provide Verizon access to export-controlled information without providing advance written notification to Verizon; and (b) is not subject to any government order suspending, revoking or denying privileges necessary for the performance of Customer’s or Verizon’s obligations under the Contract.

7. **Country Specific Terms.**

   7.1 **Customer Indemnification.** Customer will indemnify Verizon and Verizon affiliates, and Verizon’s associates, officers, directors, employees, agents and partners (“Verizon Indemnites”) from and against all losses, damages, costs and expenses (including allocable costs of in-house counsel and other legal fees) associated with any claims, suits, judgments, settlements, investigations, fines, consent decrees, requests for information, or other dispute resolution, enforcement, regulatory or legal proceedings or actions of any kind, suffered or incurred directly or indirectly by Verizon Indemnites or any third party from or arising out of Customer’s or Verizon’s breach of any non-U.S. laws or regulations applicable to protection of data or data privacy including, without limitation, personal data or personally identifiable information.

   7.2 **Russia/Middle East/North Africa.** Due to restrictions under local laws, Verizon may not sell or deliver DDoS mitigation services into Russia or countries in the Middle East or North Africa.

**Part IV: DDoS Shield Service Level Agreement.** The service level agreement (“SLA”) for DDoS Shield may be found at the following URL:

[DDoS Shield Service Level Agreement](#)
1. **Description.** DDoS mitigation services, as described in the service attachment, require that Verizon perform services for Customer utilizing a list of Customer provided IP addresses (collectively, “CIP”) as provided by Customer.

<table>
<thead>
<tr>
<th>Location/Site</th>
<th>IP Addresses</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

2. **Customer Representations and Warranties related to DDoS and Customer IP Addresses provided.**
   2.1 Customer represents and warrants that Customer (a) has been assigned the IP addresses listed in the CIP Schedule (and is the exclusive user of such IP addresses) by the appropriate Internet Assigned Numbers Authority (IANA) regional Internet numbers registry, (b) consents to Verizon’s performance of DDoS mitigation services with respect to such IP addresses, (c) has and will continue to have all rights, power, permissions and authority necessary to, have Verizon perform DDoS mitigation services with respect to such IP addresses along with the rerouting of such IP addresses for purposes of DDoS mitigation services including, without limitation, consent of all authorized network users, (d) the deliverables, documentation, and other information provided by Verizon in connection with DDoS mitigation services will be used solely for purposes of protecting Customer from abusive, fraudulent, or unlawful use or access to its information, systems and applications including Verizon’s public Internet service, and (e) will comply with all applicable laws and regulations and the provisions of Section 6 below. Customer is responsible for maintaining an up-to-date list of CIP by providing a revised CIP schedule to Verizon from time to time as required. Customer further represents and warrants that the CIP and domains provided to Verizon for purposes of receiving DDoS mitigation services are accurate and hereby assumes the sole responsibility for the accuracy of such CIP and domains. Customer will be liable for all costs and expenses from any third party claims of loss, damage (including reasonable attorneys’ fees) and liability of any kind that may be incurred as a result of Customer’s breach of the foregoing warranty.

3. **Confidential Information.** Customer acknowledges that the following information constitutes “Confidential Information” hereunder: (a) the methods, systems, data and materials used or provided by Verizon in connection with the provision of DDoS mitigation services; and (b) all reports issued by Verizon in connection with such results including, without limitation, security analyses and insight (“Net Intel Information”). Customer will disclose Net Intel Information only to Customer employees with a “need to know” for the purposes set forth in this Service Attachment and who are bound to confidentiality obligations at least as restrictive as those set forth in the Agreement and this Service Attachment. In no event may Customer use lesser efforts to protect Net Intel Information from use or disclosure not permitted under the Agreement than it uses to protect its own highly-sensitive confidential information.
or less than reasonable efforts. The term “Confidential Information” shall not include information that is comprised of statistical information, or other aggregated information regarding security vulnerabilities, security configurations and the like insofar as such information does not identify Customer or Customer's computer network or computer systems.

Customer will indemnify, defend or settle and hold Verizon Indemnitees harmless from and against all losses, damages, costs and expenses (including allocable costs of in-house counsel and other legal fees) associated with any claims, suits, judgments, settlements, investigations, fines, consent decrees, requests for information, or other dispute resolution, enforcement, regulatory or legal proceedings or actions of any kind, suffered or incurred directly or indirectly by Verizon Indemnitees from or arising out of Customer's breach of any of the representations and warranties above or based on, arising out of or relating to Customer's use or interpretation of Net Intel Information provided by Verizon.