1. **Services Description.** Sprint's Multiprotocol Label Switching Virtual Private Network ("MPLS VPN") solution is a network-based IP VPN available globally across Sprint's IP/MPLS backbone. This solution provides Subscribing Entities with a secure IP VPN solution with any-to-any intranet connectivity and a private means by which to connect their enterprise sites. In addition, Subscribing Entities can purchase Value Added Services ("VAS"), such as Secure Internet Access with Network-based Firewall, all on the same underlying network infrastructure.

2. **TSR Order Term.** The initial TSR Order Term for the Services will be stated on the TSR Order and will begin on the first day of the billing month following the date Services are installed and available to Subscribing Entity. At the end of the initial TSR Order Term, the term will continue on a month-to-month basis. Sprint or the Subscribing Entity may terminate the TSR Order at the end of the initial term or during a renewal term by providing the other party thirty (30) days' prior written notice.

3. **Primary Service Components.** The primary service components for the Services are as follows:

    3.1.   **Global MPLS VPN Port(s).** A Port is the physical entrance to the Sprint network.

    A. **Port Charges.** Sprint will charge Subscribing Entity a Non-Recurring Charge ("NRC") and a monthly charge for each Services Port, including all sub-elements or configurable attributes to the Port. The Network Design Document and Port Order will specify the sub-elements or configurable attributes to the Port (e.g. Port speed, link protocol, routing protocol, VRF policy, Class of Service (for DS3/E3 and below), and where Subscribing Entity requests, Multicast VPN). For monthly charges, Sprint offers both fixed rate (Monthly Recurring Charge or "MRC") and usage-based (Burstable) Port pricing. For Burstable Port pricing, Sprint will provide Subscribing Entity with a full Port at a given bandwidth and will charge Subscribing Entity a variable monthly charge based on Subscribing Entity's sustained Port utilization. Sprint will determine Subscribing Entity's Port utilization and charges at the end of each month. Additional information regarding Sprint's Port utilization computation is available upon request.

    B. **Port Upgrades.** Subscribing Entity may upgrade an existing Port before a TSR Order Term expires without incurring early termination liabilities for that Port, if the upgraded Port: (1) is installed at the same location as the replaced Port; (2) is installed within 10 days after the replaced Port is disconnected; (3) has a TSR Order Term equal to or greater than the remaining TSR Order Term of the replaced Port, subject to a one year minimum; and (4) has greater Port bandwidth than the replaced Port.

    C. **Additional Port Terms and Conditions.** Ports are subject to availability of capacity. If Subscribing Entity's Port resides in a Sprint Shared Tenant Facility, Subscribing Entity is responsible for working with the Service Provider to order the cross connect and will be invoiced by the site vendor for any fees associated with the cross-connect.

    3.2.   **Digital Signature Client Software.** This software is used to encrypt email communication between Subscribing Entities and Sprint regarding TSR service order requests. Sprint will provide Subscribing Entities digital certificates and digital signature client software licenses for two (2) Subscribing Entities' points of contact at no charge. If Subscribing Entity requires more than two (2) software licenses, Subscribing Entity may purchase additional licenses from Sprint. If Subscribing Entity purchases Sprint Managed Network Services, Subscribing Entity will receive two (2) additional licenses at no charge.

4. **Additional Required Components.** The Services also require Subscribing Entities to have the following:

4.1. **Dedicated Local Access.** Dedicated local access is required for the Services. Subscribing Entity may purchase Sprint-provided local access facilities or Subscribing Entity may provide its own local access facilities.

4.2. **Subscribing Entity's Premise Equipment ("CPE").** CPE is required for the Services. Subscribing Entity may elect to purchase CPE from Sprint or provide its own CPE. CPE includes, but is not limited to the following:

    A. **Routers.** Unless Subscribing Entity has separately contracted with Sprint to provide additional support services, Subscribing Entity is fully responsible for the router, including configuration, maintenance, and management. In addition, if Subscribing Entity elects not to obtain a router from Sprint, Subscribing Entity must furnish the necessary ancillary equipment (cables, routing software, etc.) to ensure interoperability with the Services.

5. **MPLS over Digital Subscriber Line ("DSL").** Subscribing Entity sites may qualify for alternate access via MPLS DSL. This eliminates the need for an MPLS Port and access at the qualifying site. MPLS DSL sites may communicate freely with other MPLS DSL and MPLS locations. Subscribing Entity must have at least one MPLS Port in its network.

6. **Value-added Services.** Sprint provides Value-added Services ("VAS") that Subscribing Entity may opt to purchase as part of its Global MPLS VPN solution. VAS have both a monthly charge and an NRC. For monthly charges, Sprint offers both fixed rate and variable (usage-based) VAS pricing. For usage-based VAS pricing, the monthly charge will vary based on the aggregate bandwidth Subscribing Entity utilizes each month. Subscribing Entity must select either fixed rate or usage-based pricing for its entire network.

6.1. The following VAS are Network-based:

    A. **Secure Internet Access ("SIA") with Network-based Firewall.** Regional VAS gateways provide secure access from the Services to the Internet. Each site in Subscribing Entity's Global MPLS VPN will receive Internet access secured by a stateful inspection firewall located within Sprint's network.

    B. **Remote Access Service ("RAS").** RAS allows Subscribing Entities to obtain remote access to the Services through the use of a VPN client. This client is installed on a Subscribing Entity's laptop and builds an IPSec tunnel back to a VAS gateway to enable Subscribing Entities to run applications while away from the office.

    C. **Virtual System (VSYS).** A VSYS is a subdivision of the main system that appears to the user to be a stand-alone entity. An additional VSYS will be required when the default number of VSYS provisioned for the Subscribing Entity is not sufficient.

    D. **Zone.** A zone is a segment of network space to which security measures are applied. Additional zones could be required to make the network security design more granular without deploying multiple security appliances.

    E. **Policy.** A policy provides a protection mechanism for the firewall allowing traffic to be passed on source/destination zone, source/destination IP address, ports and protocols. A policy, also known as a rule, or set of policies will be required in case of a complex Subscribing Entity's firewall for which the default number of policies is not sufficient.

6.2 The following VAS are site based:

    A. **IPSec Half Tunnel.** Internet Protocol Security ("IPSec") Half Tunnel is for Subscribing Entities who have sites outside Sprint's footprint or have the need to securely communicate with a select audience outside of their organization. IPSec Half Tunnel

allows Subscribing Entities to connect to the Services using Sprint's Managed CPE-based IP VPN, which can be used at locations where Subscribing Entity has existing dedicated internet access from Sprint or from another service provider. Alternatively, Subscribing Entity or a third party can elect to manage the CPE-based IP VPN device. In a Sprint-managed solution, Sprint will design, implement, maintain, and manage hardware at CPE-based IP VPN locations, providing a complete end-to-end VPN solution.

7.   **Subscribing Entity's Responsibilities**

7.1.   **Multicast VPN**

A.   If Subscribing Entity requests Multicast VPN, the following are Subscribing Entity's responsibilities:

(1)   Subscribing Entity must run its own rendezvous points (depending on the protocol it is using) and servers. Sprint does not provide (or have) rendezvous points for Multicast VPNs. The Sprint network is essentially invisible to Subscribing Entities.

(2)   Subscribing Entity must provide its own Multicast addresses. Sprint makes no restrictions on addresses, but Multicast is limited to the Class D range (224.0.0.0 - 239.255.255.255).

(3)   Except for verifying that Multicast traffic is coming in on one router and exiting on the other side, Subscribing Entity must manage Multicast. In other words, Sprint will verify that Multicast traffic is coming from Subscribing Entity and that Sprint is sending Multicast to Subscribing Entity on the other side. Sprint will not be able to access Subscribing Entity's Multicast transmissions and will not be able to verify that the transmissions are successfully working.

7.2.   **IPSec Half Tunnels**

A.   If Subscribing Entity elects to manage the CPE-based IP VPN device, the following are Subscribing Entity's responsibilities:

(1)   Subscribing Entity must coordinate communication between Sprint and any third parties involved in managing Subscribing Entity's network or with the LEC who is using the Half Tunnel connection.

(2)   Subscribing Entity must participate and support the service delivery objectives in the provisioning of the Half Tunnels and any associated transport orders.

(3)   Subscribing Entity must monitor Subscribing Entity-managed IP VPN devices.

(4)   Subscribing Entity is responsible for repairing any issues or outages with Subscribing Entity-managed devices.

8.   **Network Monitoring**

8.1.   As part of the Services, Sprint provides Subscribing Entity a trouble resolution team available to respond to Subscribing Entity's issues 24 hours a day, 365 days a year. Subscribing Entity may elect to purchase additional monitoring and management services as described in Section 9 below.

8.2.   Sprint will provide a trouble ticket number from Sprint's automated Trouble Reporting System ("TRS") to Subscribing Entity. For each trouble report, TRS will maintain information about the trouble, the steps taken to resolve the trouble, and the final disposition of the trouble report.

Sprint will keep Subscribing Entity'sTechnology Coordinator or his/her designee apprised of the status of service restoration actions.

9. **Enhanced Monitoring and Managed Services.** For Subscribing Entities interested in purchasing enhanced monitoring and managed services for the Services, Sprint offers the following:

   9.1 **Managed Network Services.** These services include a comprehensive suite of management and implementation services that support multi-protocol Wide Area Networks (WANs) and Local Area Networks (LANs) utilizing Sprint and non-Sprint provided transport services. These services support Subscribing Entities' premises-based routers, IP-VPN devices, switches, hubs, servers, and applications worldwide. Sprint Managed Network Services is comprised of engineering, design, and implementation of Subscribing Entities' networks, including WAN transport; LANs and CPE; day-to-day operational support; configuration management; network and CPE monitoring; proactive notification; fault management; trouble resolution; and network and device performance reporting.

   9.2 **Sprint E-mail Protection Services.** These services provide inbound and outbound content blocking, policy management, anti-virus and spam management (including message quarantine service), disaster recovery, outbound anti-virus management and SMTP Services, web reports, and web administration.

   9.3 **Managed Security Services.** These services include a comprehensive suite of management and implementation services that support security related functionality. The services support firewall, intrusion detection and prevention services, DDOS detection and mitigation, and URL and content filtering. Subscribing Entities' entitlements include engineering; design and implementation of services; day-to-day operational support; configuration management; security event monitoring; proactive notification; fault management; trouble resolution; and network and security event reporting.

10. **Definitions.**

    10.1 **"Remote Access"** means communicating with a data processing facility from a remote location or facility through a data link, i.e. VPN.

    10.2 **"Shared Tenant Facility"** means the location where all Vendor's circuits are housed.

    10.3 **"User"** means a person that uses Products and/or Services.