4.1.9 NETWORK-BASED IP VPN SERVICES (NBIP-VPNS) (L.34.1.4)

Qwest achieved an industry first with our Network-based IP VPN services. Our Networx NBIP-VPNS uses our converged IP core network to support any access method and deliver multiple classes of service.

Qwest's Network-based IP VPN Services (NBIP-VPNS) are delivered using Qwest's Multiprotocol Label Switching (MPLS)-based private IP network, and Qwest integrated Secure Remote Access solutions. Qwest's NBIP-VPNS is ideal for seamless integration of Agency sites with a variety of security and bandwidth requirements of up to OC-192. Qwest uses cutting edge MPLS-based VPN, Label Switched Path (LSP) Routing, and Quality of Service (QoS) technology based on RFC-4364 standards defined by the Internet Engineering Task Force (IETF). In addition to a robust domestic capability, Qwest's NBIP-VPNS solutions connect VPN users from domestic and non-domestic locations using the Qwest network and our multiple international MPLS service provider partners with end-to-end Qwest responsibility.

Leading-edge Inter-AS MPLS connections into the Qwest Private MPLS VPN network enhance Qwest's ability to provide seamless, standards-based MPLS VPNs around the world. Qwest currently provides world-class customer support, NBIP-VPN access and transport solutions and integrated router-based solutions to demanding Government and commercial customers

[redacted]

Figure 4.1.9-1 provides an easy reference to correlate narrative requirements to our proposal response.

Figure 4.1.9-1. Table of NBIP-VPNS Narrative Requirements

Req ID	RFP Section	RFP Requirement	Proposal Response
5684	C.2.7.3. 3.1 (1)	Interface for Intranet and Extranet Network-based IP VPNs UNI Type 1 Interface/Access Type: Ethernet Interface Network-Side Interface: 1. 1 Mbps up to 1 GbE (Gigabit Ethernet) 2. 10 GbE (Optional) Protocol Type: Ipv4/v6 over Ethernet	4.1.9.3.1.3
5683	C.2.7.3. 3.1 (2)	Interface for Intranet and Extranet Network-based IP VPNs UNI Type 2 Interface/Access Type: Private Line Service Network-Side Interface: 1. DS0 2. Fractional T1 3. T1 4. T3 5. Fractional T3 6. OC-3c 7. OC-12c 8. OC-48c 9. OC-192c Protocol Type: Ipv4/v6 over PLS	4.1.9.3.1.3
5682	C.2.7.3. 3.1 (3)	Interface for Intranet and Extranet Network-based IP VPNs UNI Type 3 Interface/Access Type: IP over SONET Service Network-Side Interface: 1. OC-3c 2. OC-12c 3. OC-48c 4. OC-192c Protocol Type: IP/PPP over SONET	4.1.9.3.1.3
5680	C.2.7.3. 3.2 (1)	Interface for Remote Access Network-based IP VPNs UNI Type 1 Interface/Access Type: Voice Service Network-Side Interface: Analog dialup at 56 kbps Protocol Type: Point-to-Point Protocol, Ipv4/v6	4.1.9.3.1.3
5678	C.2.7.3. 3.2 (2)	Interface for Remote Access Network-based IP VPNs UNI Type 2 Interface/Access Type: DSL Service Network-Side Interface: xDSL access at 1.5 to 6 Mbps downlink, and 384 Kbps to 1.5 Mbps uplink Protocol Type: Point-to-Point Protocol, Ipv4/v6	4.1.9.3.1.3
5677	C.2.7.3. 3.2 (3)	Interface for Remote Access Network-based IP VPNs UNI Type 3 Interface/Access Type: Cable high speed access Network-Side Interface: 320 Kbps up to 10 Mbps Protocol Type: Point-to-Point Protocol, Ipv4/v6	4.1.9.3.1.3
5676	C.2.7.3. 3.2 (4)	Interface for Remote Access Network-based IP VPNs UNI Type 4 Interface/Access Type: Multimode/Wireless LAN Service Network-Side Interface: See Section C.2.14.3.3.1 MWLANS User-to-Network Interfaces	4.1.9.3.1.3
5675	C.2.7.3. 3.2 (5)	Interface for Remote Access Network-based IP VPNs UNI Type 5 Interface/Access Type: Wireless Access Network-Side Interface: See Section C.2.16.2.3.3.1 Wireless Access Arrangement Interfaces	4.1.9.3.1.3
5674	C.2.7.3. 3.2 (6)	Interface for Remote Access Network-based IP VPNs UNI Type 6 Interface/Access Type: Satellite Access Network-Side Interface: See Section C.2.16.2.4.3.1 Satellite Access Arrangement Interfaces	4.1.9.3.1.3
5673	C.2.7.3. 3.2 (7)	Interface for Remote Access Network-based IP VPNs UNI Type 7 Interface/Access Type: Circuit Switched Data Service Network-Side Interface: 1. ISDN at 64 Kbps 2. ISDN at 128 Kbps 3. ISDN dial backup at 64 Kbps 4. ISDN dial backup at 128 Kbps Protocol Type: Point-to-Point Protocol, Ipv4/v6	4.1.9.3.1.3
7827	'C.2.7.3. 1.4 (10)(a)	The following network-based IP VPN capabilities are mandatory, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage, unless marked optional 10. The contractor shall support one or more of the following application level QoS objectives, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage: a. Intserv model for selected individual flows; b. Diffserv model for aggregated flows.	4.1.9.3.1.1
8319	C.2.7.3. 1.4 (7)(a)(b) (c)(d)(e)	The following network-based IP VPN capabilities are mandatory, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage, unless marked optional. 7. The contractor shall support QoS in one or more of the following standardized modes: a. Best effort; b. Aggregate Customer Edge (CE) Interface level QoS (hose level); c. Site-to-site level QoS (pipe level); d. Intserv (RSVP) signaled; e. Diffserv marked.	4.1.9.3.1.1

4.1.9.1 Technical Approach to NBIP-VPNS Delivery

Qwest NBIP-VPNS enables the Government to create secure Virtual Private Networks (VPNs) that range from dial-up voice and Integrated Services Digital Network (ISDN) Internet access to dedicated high-speed optical connections. Qwest has dedicated support organizations, coordinated by the Qwest Networx Program Management Office (PMO), to engineer, install, maintain, and evolve our delivered service to meet the Government's NBIP-VPNS requirements. Qwest delivers NBIP-VPNS using Provider Edge (PE) network routers. [redacted] This PE platform leverages the tremendous backbone bandwidth of our 10 Gbps-based private MPLS core. Its any-access-anywhere design is completely in step with the Networx requirements for flexible, dedicated access. As required Qwest supports a full range of Wireline Access Arrangement (WLNAA), Broadband, Wireless Access Arrangements (WLSAA), and Satellite Access Arrangements (SatAA) access methods for this service. Qwest provides end-to-end engineering, monitoring, and trouble management to ensure service excellence for the NBIP-VPNS user.

4.1.9.1.1 Approach to NBIP-VPNS Delivery (L.34.1.4.1(a))

Qwest's approach to NBIP-VPN service delivery encompasses the network platforms, people and operational processes that deliver exceptional services. Qwest collaborates with our customers to identify requirements and deliver the services that best suit their needs. Our NBIP-VPNS architecture takes full advantage of MPLS-enabled convergence to create one of the most efficient network platforms in the industry. Our network and partners provide the underlying service delivery infrastructure, ensuring worldwide continuity of

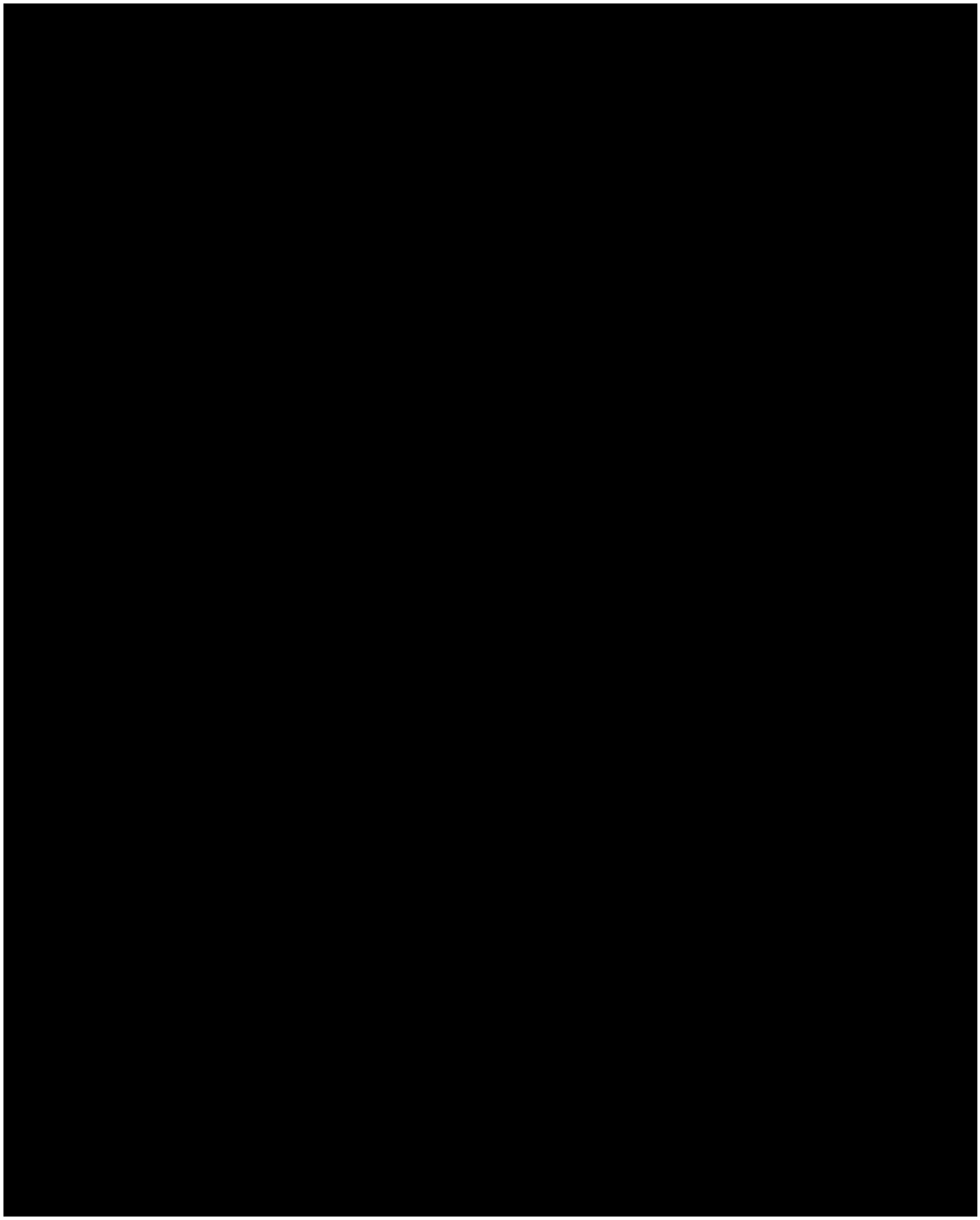
service for Agencies. Our NBIP-VPNS leverages the high-performance Qwest network widely in use by some of the most demanding Government customers today, [redacted]

Proven Engineering Practices

Qwest network planning and engineering organizations have created a highly robust private MPLS core [redacted] Qwest continually monitors network performance and capacity utilization end-to-end to ensure the highest performance for all Qwest customers.

Standards-Based, Global Network

Domestically, Qwest's NBIP-VPNS uses Qwest's nationwide OC-192 private MPLS core network as its backbone. The OC-192 backbone is explained in greater detail in Section 3.3, Approach to Networx Architecture. [redacted]



[redacted]

The Qwest NBIP-VPN consists of a global private routed infrastructure Autonomous System (AS) ID with [redacted] major TeraPOPs that are interconnected with OC-192 wavelengths. To access this infrastructure, Qwest has [redacted] regional IP Points of Presence (POPs) connected via SONET circuits [redacted] We also maintain approximately [redacted]

dial access POPs for Continental United States (CONUS) Local Access and Transport Area coverage. In addition, there are over [redacted] domestic network access points that can terminate a customer's dedicated local access. [redacted]

Qwest has extensive experience supporting real-time services on our MPLS-enabled network. We transport over 4 billion minutes of voice services as Voice over Internet Protocol (VoIP) traffic every month. Real-time Agency applications, like VoIP and IP-based videoconferencing, as well as access to Qwest's real-time services, are supported. To enable the convergence of customer applications with required performance Qwest provides a [redacted] Class of Service (CoS) queue design:

[redacted]

[redacted]

Qwest uses its MPLS core to provide bandwidth for a completely private MPLS VPN network to build multiple VPNs based on IETF RFC-4364. [redacted]

Alternate access approaches supported by our NBIP-VPN include DSL, cable access, broadband wireless and satellite. [redacted] Dial access for both voice services and ISDN Basic Rate Interface (BRI) and Primary Rate Interface (PRI) access is provided by Qwest's nationwide dial access network—with [redacted] ports and local access across the country. Cable access is provided through Internet Service Provider (ISP) peering, with [redacted] direct peering with our cable ISP providers.

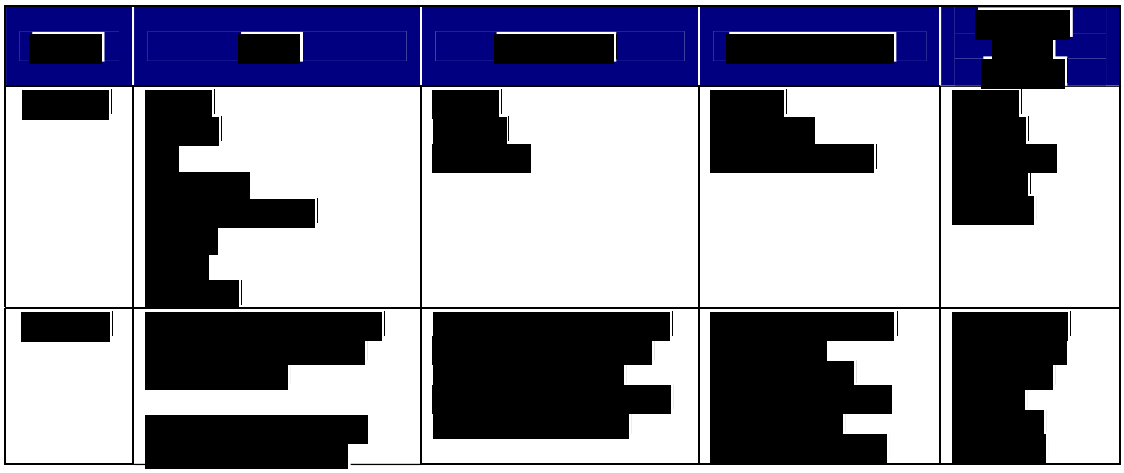
Qwest's OC-192 backbone spans the Asia Pacific region, Hawaii and CONUS, with [redacted] public and private peering points [redacted]

[redacted]

Qwest extends our domestic nationwide NBIP-VPNS network footprint to the global community through extension of Qwest-owned PE access POP facilities [redacted]. Qwest has deployed PE Access POPs [redacted] enabling direct on-net NBIP-VPNS services in the Asia Pacific rim region.

Qwest is able to deliver unparalleled global network reach through strategic relationships with key best-of-breed international network alliance providers, summarized below in [redacted] Understanding that local knowledge is key, Qwest has partnerships that give our customers the benefit of a single service provider ensuring service consistency, while assuring them that our regional alliance providers understand their region better than anyone else. [redacted]

[redacted] We continuously monitor monthly, quarterly and yearly Key Performance Indicator (KPI) performance metrics. Qwest has designed and implemented service improvements and new access and features to remain competitive. [redacted]



Qwest's secure remote access service provides a multi-faceted secure client, strong authentication, and diverse access technology solution to the Federal Government. Secure remote access integrates seamlessly into the Qwest NBIP-VPNS solution:

- A premium VPN IPsec client that supports interoperable access flexibility, VPN security tunnel enablement, strong authentication, firewall integration, end-user control, grouping, messaging, tracking, and reporting.
- Secure remote access User to Network Interfaces (UNIs) include high-speed Internet ISDN BRI, enterprise-class integrated ADSL and SDSL, global roaming dial up Internet access, integration of V.90, V.92, ISDN, wireless client and nationwide WiFi 802.11, and robust and universally available satellite Internet access.

Commitment to Customers

As the first major operator in the US to offer Network-Based IP VPN Services (NBIP-VPNS), Qwest has been designing high-performance, secure NBIP-VPNS and Premises-Based IP VPN Services (PBIP-VPNS) solutions for Government customers and Fortune 500 financial, healthcare, manufacturing and high-technology companies since 1999. Qwest's engineering and program management expertise, as well as hands-on technical integration experience with all facets of dedicated, remote, wireless, and satellite-based NIPB-VPNS access solutions, reduces the Government's operational risks. Qwest's network technology management, architecture, planning, engineering, and operations organizations are all aligned to ensure network availability and feature flexibility.

Qwest will work with Agencies to recommend and help select the right SED to meet their requirements. Qwest takes complete responsibility for the provisioning of any NBIP-VPN service. This includes the ordering and installation of the SED, the ordering and provisioning of the requested access method, configuration of the NBIP-VPNS, and complete test and turn-up.

Once provisioned, a key element of service delivery involves the operational support that ensures the service meets performance goals [redacted]

[redacted] The Qwest NOC is staffed with highly trained and experienced personnel who understand the Government's network and internetworking equipment.

NOC senior management continually reviews KPIs and best practices, verifying that appropriate preventive steps are taken to avoid problems and validate that customer service meets Acceptable Quality Levels (AQLs). From a single, accountable one-call-resolve support structure, to convenient, quick Web-based management and reporting tools, Qwest teams will address any issues that affect service. The portal accessible management tools enable dynamic management including support for Agency initiated adjustments of allocated bandwidth in near-real-time.

4.1.9.1.2 Benefits of Qwest's NBIP-VPNS Technical Approach (L.34.1.4.1 (b))

Qwest NBIP-VPNS offers a converged networking service based on leading technologies that will allow Agencies to build networks using legacy ATM and Frame Relay protocols, as well as advanced IP-centric, MPLS-based solutions. ***Figure 4.1.9-5*** summarizes the key features and benefits of our NBIP-VPNS.

Figure 4.1.9-5. Qwest's NBIP-VPNS Features and Benefits

Feature	Benefit	[redacted]
High-Availability, High-Capacity 10 Gbps-based Multi Protocol Labeled Switched MPLS Core	Extremely high packet delivery rates with low latency and jitter for today's demanding applications	
MPLS Fast Re-Route (FRR)	Built-in redundancy and resiliency provides service continuity for customers and their traffic	
Private, Internet-free Core and Edge Routers for NBIP-VPNS	High-level of security and no service affecting exposure to the Internet	
Flexible and standards-based access protocols that include HDLC, PPP, MLPPP, FR, ATM, DSL, T-1, DS-3, OC-x, and Ethernet	Service continuity for supporting customers with legacy interfaces as well as support of new interfaces to enable flexible access and new service types	
Class of Service Mechanisms with four Classes of Service and Class-Based Weighted Fair Queuing (CBWFQ)	Qwest can prioritize NBIP-VPNS traffic to enable applications such as VoIP	
Extranet access to NBIP-VPNS Internet VPN servers	Secure access from around the world to domestic NBIP-VPNS	
Qwest has [redacted] dial-up ports. Nationwide and international Wi-Fi and dial-up roaming is provided by our industry leading alliance provider, [redacted]	Remote access for mobile and teleworkers	
User configurable network-based firewall; Qwest has provided network-based IPS firewall services for over five years with user controlled configurations	Reduces the impact of attack on Networx IPS customers by rejecting traffic within the Qwest network before it gets to the Agency's premises	

Feature	Benefit	[redacted]
Qwest has [redacted] carrier neutral Layer 3 facilities and [redacted] CyberCenters	Enables customers to build enterprise architectures to services to meet their applications	[redacted]
Qwest has multiple worldwide Internet service provider alliances, [redacted]	Networking availability is global and is designed for worldwide company communications based on the latest MPLS network technology	[redacted]

Qwest's NBIP-VPNS facilitates the Federal Enterprise Architecture (FEA) objectives as summarized in ***Figure 4.1.9-6***.

Figure 4.1.9-6. Qwest's NBIP-VPN Support to FEA Objectives

FEA Objective	Qwest NBIP-VPNS Solutions
Improve utilization of Government information resources to focus on core Agency mission and service delivery to citizens by using the FEA	• Qwest's NBIP-VPNS is a cohesive and globally available IP communications platform with extensive connectivity to the worldwide Internet to enable remote workers to access their information resources – from xDSL, PCS, satellite, and WiFi • With our MPLS core technology, Qwest is able to provide extremely high network availability to ensure access to Government information resources
Enhances cost savings and avoidance	Qwest NBIP-VPNS ensures cost savings and avoidance of redundant support resources; by converging multiple voice, data, video, and transactional data needs onto a single, multi-function network platform enabled by our traffic prioritization capabilities
Increases cross Agency and inter-Government collaboration	Our flex ble customer configurable, NBIP-VPNS can provide multiple logical networks enabling cross Agency and inter-Government service while retaining logical separation of their respective networks

4.1.9.1.3 Solutions to NBIP-VPNS Problems (L.34.1.4.1(c))

Qwest has extensive experience in the delivery of NBIP-VPNS, and we apply this knowledge to ensure the delivery of high quality NBIP-VPNS to Agencies. Extensive pre-deployment laboratory system and integration testing identifies the majority of problems, and Qwest's proactive network and configuration management/fault management systems and methods are leveraged to quickly resolve unforeseeable operational issues.

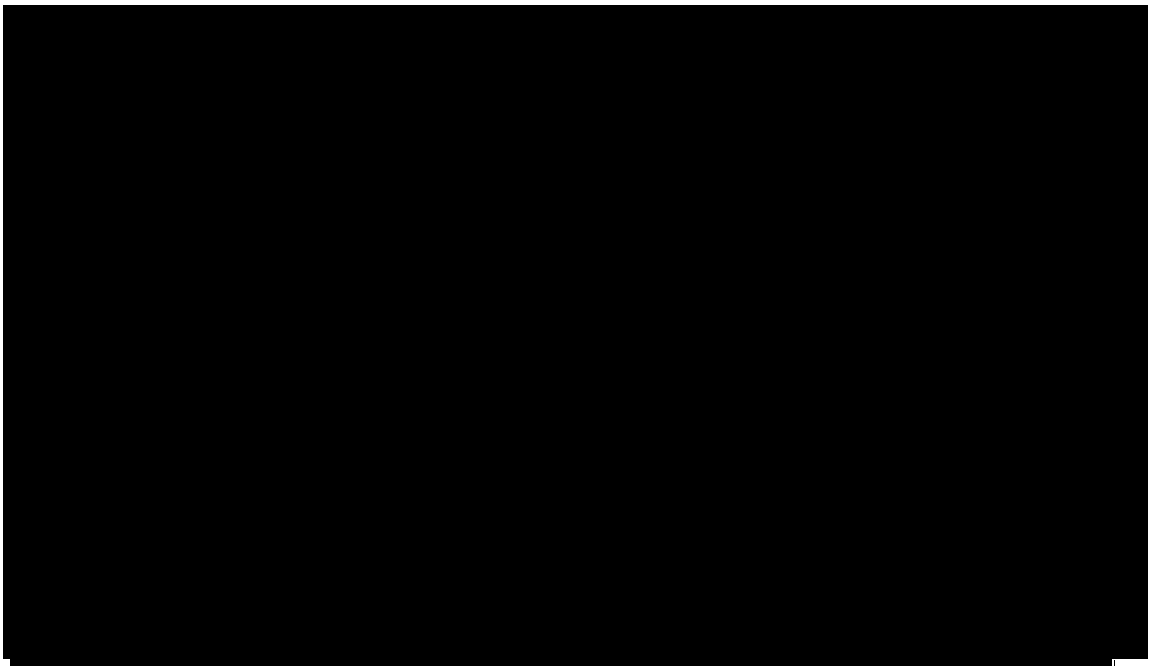
Qwest's NBIP-VPNS will meet the individual service requirements requested by Agencies. Qwest's Networx PMO and NOC will ensure service

delivery and continuing operations. [redacted] summarizes the typical problems we encounter in meeting NBIP-VPNS requirements and our solution.

Figure 4.1.9-7. Qwest's Approach to Common NBIP-VPNS Delivery Challenges

4.1.9.1.4 Synchronization Network Architecture (L.34.1.4 (d))

[redacted]



[redacted]

[redacted]		
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

[redacted]

4.1.9.2.1 NBIP-VPNS Quality of Service (L.34.1.4.2(a))

The Qwest Fiber Network (QFN) that supports NBIP-VPNS has tremendous backbone capacity and high availability. In general, most Service Delivery Point (SDP) outages are caused by either customer site power failures or local access facility failures. We have compiled statistics over the

past four years on the performance of networks for similar requirements. [redacted]

Figure 4.1.9-10 summarizes our compliance with Networx requirements for NBIP-VPNS services:

Figure 4.1.9-10. Qwest Compliance with Government NBIP VPNS Performance Metrics

KPI	Service Level	Performance Standard (Threshold)	AQLs	[redacted]
Latency (CONUS)	Routine	70 ms	≤ 70ms	[redacted]
Latency (Outside Continental United States (OCONUS))	Routine	150 ms	≤ 150ms	[redacted]
Availability	Routine	99.9%	≥ 99.9%	[redacted]
	Critical	99.99%	≥ 99.99%	[redacted]
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	[redacted]
	With Dispatch	8 hours	≤ 8 hours	[redacted]

All Qwest IP-based services are supported by a highly robust, highly available transport infrastructure. Qwest engineers monitor and manage end-to-end transport solutions. Qwest will support availability from our Network Operations Center (NOC) [redacted]

[redacted]

4.1.9.2.2 Approach for Monitoring and Measuring NBIP-VPNS KPIs and AQLs (L.34.1.4.2 (b))

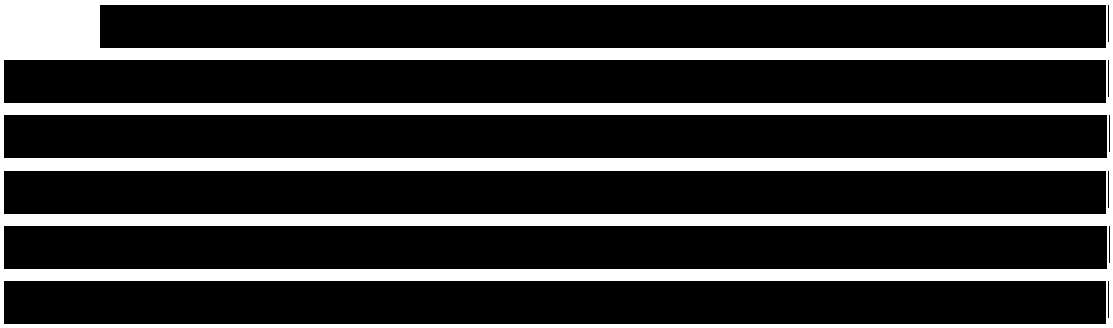
Qwest monitors and measures the KPIs and AQLs via an automated process that pulls data from the root source, summarizes it, and displays it via Web tools. These Web tools display actual results and indicate via red/green colorizing whether or not goals are met. Our approach is to completely automate displaying results from data collection to Web display so that the focus is on results rather than "report generation." Further, our automated process ensures that business rules are established and there is no chance of manipulating the data.

For Network KPIs, we use the Statistical Analysis System (SAS) to display the Network Reliability Scorecard with the KPIs, the objectives, and an indication of whether the objectives are met or missed for each reporting period. The scorecard is our tool to show both upper management and network management the current health of the network. The scorecard is reviewed daily, both at the executive level to ensure the proper attention and focus, and by our network management teams to ensure AQL levels are consistently met.

For all Networx services we use the [redacted] trouble ticketing system. [redacted] From this system, we collect many useful metrics that we use internally to evaluate and improve our processes including Time to Restore (TTR). The calculation for TTR uses the same business rules as the Government requires for its services.

For the NBIP-VPNS, all of the AQL/KPI metrics listed in Figure 4.1.9-10 are assessed on an individual site or site-pair basis where applicable. This data is used to ensure all Agency data network AQLs are systematically being supported by the network. Additionally, key network infrastructure interfaces (Aggregation Ports/Network to Network Interfaces, Trunk Ports) are monitored for Packet/Cell Loss (including errors and discards) and availability ensuring that no Agency AQL issues are traceable to key network infrastructure ports.

Qwest will ensure the services delivered to Agencies follow a stringent reporting, management, and network capacity strategy to verify that all AQLs are delivered at a consistent acceptable level. Qwest NOC network management systems collect performance data directly from the NBIP-VPNS routers via SNMP. Performance data is collected from the network and SEDs at industry standard five minute intervals. The NBIP-VPNS performance data information is distributed to Qwest's NOC, which continuously monitors the performance of the Qwest OC-192 IP MPLS network. NBIP-VPNS utilization is monitored by the Qwest NOC, which is responsible for reporting statistics to the Data Network Planning and Design Group. This information is distributed to internal databases where it will be posted to the Qwest Control Networx Portal. This portal provides Agencies with performance statistics to verify customer-specified AQLs are met.



[redacted]

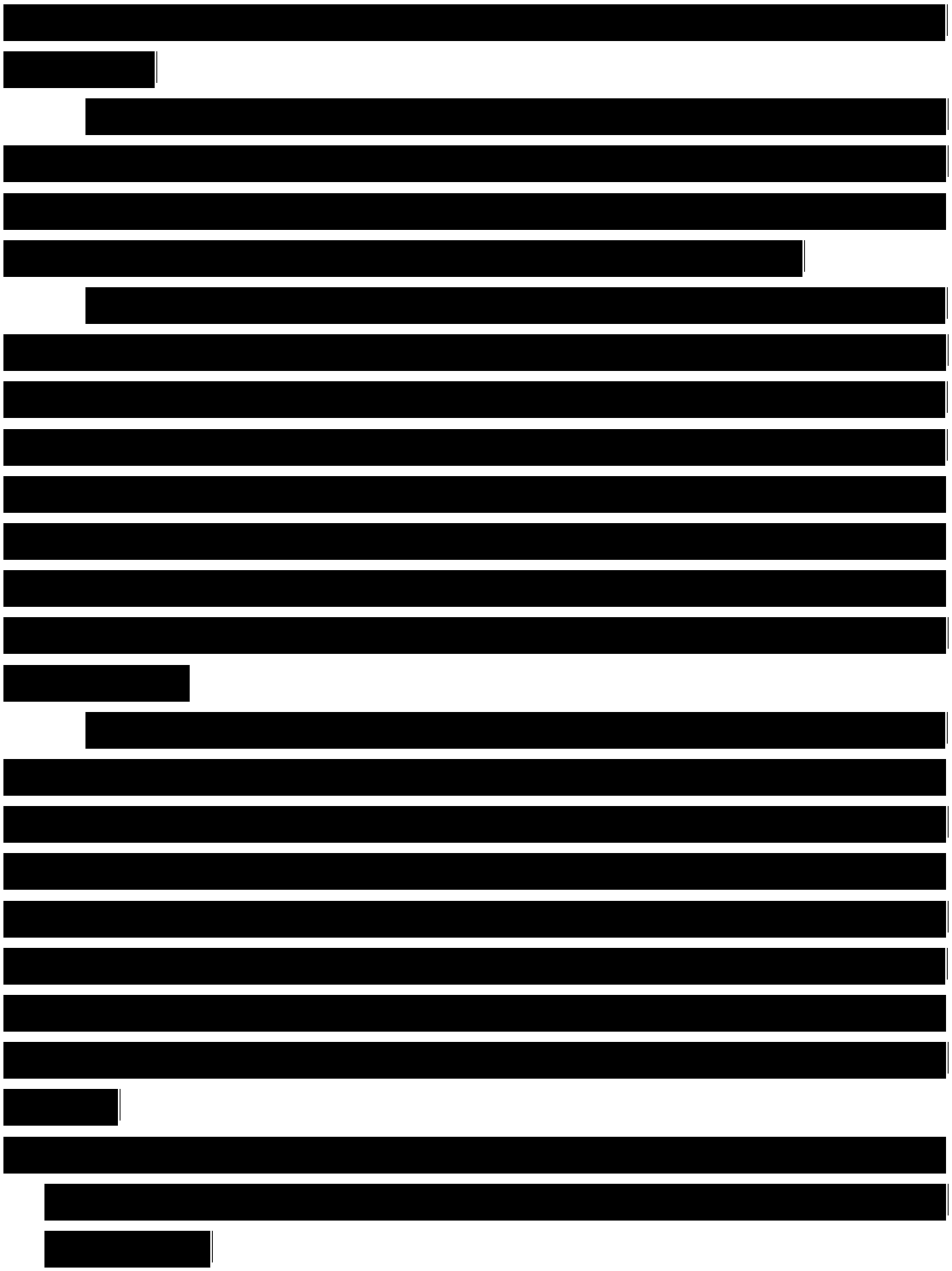
Measuring SDP-to-SDP Latency, and the Role of SEDs

[redacted]

[redacted]

[redacted]

Qwest's solution was originally designed for its commercial offering to be SED-vendor agnostic. Qwest's performance management (PM) architecture is standards-based, scalable, flexible, and network centric, imposing the minimal requirements or load at the SDP level to achieve a rich set of PM metrics. [redacted]



[redacted]

Use of Statistical Sampling in lieu of Direct KPI Measurements

Qwest does not propose to use statistical sampling in lieu of direct KPI measurements. While our approach to KPI measurements does use probe measurements, the measurements are taken on the actual network data and are direct, unfiltered measurements, not statistical extrapolations.

The Use of Government Furnished Property

[redacted]

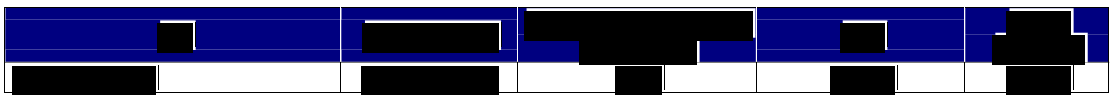
[redacted]

4.1.9.2.3 NBIP-VPNS Performance Improvements (L.34.1.4.2(c))

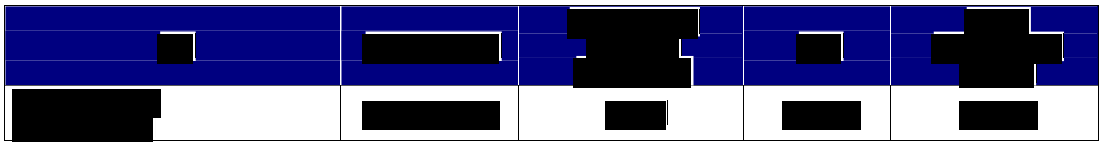
[redacted] In the event an Agency has a specific business need or application problem, Qwest is willing to discuss service enhancements. Qwest will operate in good faith to engineer an NBIP-VPNS solution to serve unique Agency needs. Qwest is able to leverage our vast NBIP-VPNS product portfolio, which includes a variety of SED providers and specific NBIP-VPNS solutions. Through a special combination of vendor solutions and talented engineering capabilities Qwest will serve all Agencies' business needs.

4.1.9.2.4 Additional NBIP-VPNS Performance Metrics (L.34.1.4.2 (d))

[redacted]



[redacted]



[redacted]

4.1.9.3 Satisfaction of NBIP-VPNS Specifications (L.34.1.4.3)

Qwest will support all capabilities and locations, and will deliver design expertise and knowledge while complying with all technical service requirements specified by the Networx RFP. Qwest's NBIP-VPNS delivers a broad range of service features, functionality and technical capabilities, all delivered from our standards-based MPLS VPN internetworking platform.

Qwest's NBIP-VPNS solutions will globally connect VPN users by using interconnections and provider partner networks. Qwest has implemented encryption support and MPLS-based CUG context designs to support functions such as data concealment, virtual route forwarding, and tunneling protocols. Qwest's NBIP-VPNS MPLS CUG allows our converged IP NBIP-VPN platform to support [redacted] traffic that originates from multiple access types in the same CUG to communicate on an uninterrupted basis. [redacted]

4.1.9.3.1 Satisfaction of NBIP VPNS Requirements (L.34.1.4(a))

4.1.9.3.1.1 Satisfaction of NBIP-VPNS Capabilities Requirements (L.34.1.4.3(a), C.2.7.3.1.4)

Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for NBIP-VPNS. The text in ***Figure 4.1.9-13*** is intended to provide the technical description required per L.34.1.4.3 (a), and does not limit or caveat Qwest's compliance in any way.

Figure 4.1.9-13. Qwest's Technical Approach to NBIP-VPNS Capabilities

ID #	Name of Capability	[redacted]
1	Tunneling Standards	[redacted]
2	Encryption Levels	[redacted]
3	Authentication Services	[redacted]

ID #	Name of Capability	[redacted]
		[redacted]
4	Reserved	
5	IPv4 Support	[redacted]
6	IPv6 Support	[redacted]
7	QoS Support	[redacted]
8	Reserved	
9	Access QoS Support	[redacted]
10	Application-level QoS Support	[redacted]
11	Access Methods Supported	[redacted]
12	Fast Dial Access	[redacted]
13	Reserved	
14	Isolation of Traffic and Routing Information	[redacted]
15	Layered Security Architecture	[redacted]
16	NBVPN Management	[redacted]

ID #	Name of Capability	[redacted]
17	Mobile User Support	[redacted]
18	Multiple VPN Support	[redacted]
19	Network Design and Engineering Services	[redacted]
20	Dynamic Bandwidth Adjustment Support (Optional)	[redacted]
21	Secure Routing Service	[redacted]
22	Encryption, Decryption, Key Management Support	[redacted]
23	Support for Agency Security Mechanisms	[redacted]
24	Authentication Server Choices	[redacted]

Qwest's NBIP-VPNS solutions infrastructure complies with the accepted industry standards design development efforts–SSL and IPsec committees, and Layer 3 and Pseudo-Wire forums. Based on Qwest's private MPLS architecture, NBIP-VPNS solutions can connect Agency locations and trusted business partners [redacted]

QoS Modes Supported (Req_ ID 8319; C.2.7.3.1.4(7)(a)(b)(c)(d)(e))

[redacted]

[redacted]

Support for Application-Level QoS Objectives (Req_ ID 7827; C.2.7.3.1.4(10)(a))

[redacted]

4.1.9.3.1.2 Satisfaction of NBIP-VPNS Feature Requirements (L.34.1.4.3(a), C.2.7.3.2)

Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for NBIP-VPNS. The text in ***Figure 4.1.9-14*** is intended to provide the technical description required per L.34.1.4.3 (a), and does not limit or caveat Qwest's compliance in any way.

Figure 4.1.9-14. Qwest's Technical Approach to NBIP-VPNS Features

ID #	Name of Feature	[redacted]
1	CoS	[redacted]
2	High availability options for CPE	[redacted]
3	Internet Gateway Service	[redacted]

ID #	Name of Feature	[redacted]
4	Interworking Services	[redacted]
5	Key Management	[redacted]
6 (Opt.)	Non-peered Private IP Network	[redacted]
7	Security services	[redacted]

4.1.9.3.1.3 Satisfaction of NBIP-VPNS Interface Requirements (L.34.1.4.3(a), C.2.7.3.3)

Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for NBIP-VPNS. The text in ***Figure 4.1.9-15 and Figure 4.1.9-16*** is intended to provide the technical description required per L.34.1.4.3 (a), and does not limit or caveat Qwest's compliance in any way.

Figure 4.1.9-15. Qwest Provided NBIP-VPNS Interface at the SDP

UNI Type	Networx Service	Network-Side Interface	[redacted]	[redacted]
1	Ethernet Access	1. 1 Mbps up to 10 GbE (Gigabit Ethernet) 2. 10 GbE (Optional)	[redacted]	[redacted]
2	Private Line Service	1. DS-0 2. Fractional T-1 3. T-1 4. Fractional T-3 5. T-3 6. OC-3c 7. OC-12c 8. OC-48c 9. OC-192	[redacted]	[redacted]
3	IP over SONET Service	1. OC-3c 2. OC-12c 3. OC-48c 4. OC-192c	[redacted]	[redacted]

Note that the mandatory interfaces list mandates inclusion of SEDs that exceed the scope of the mandatory SED suites. Qwest has identified potential SEDs for each required interface.

In addition, as shown below in ***Figure 4.1.9-16***, Qwest's NBIP-VPNS supports all interfaces for remote access.

Figure 4.1.9-16. Summary of Remote Access Interface Support for Qwest's NBIP-VPNS

UNI Type	Networx Service	Network-Side Interface	[redacted]	[redacted]
1	Voice Service	Analog dialup at 56 kbps	[redacted]	[redacted]
2	DSL Service	xDSL access at 1.5 to 6 Mbps downlink, and 384 kbps to 1.5 Mbps uplink	[redacted]	[redacted]
3	Cable High Speed Access	320 Kbps up to 10 Mbps	[redacted]	[redacted]
4	Multimode/Wire-less LAN Service	MWLANS User-to-Network Interfaces: Air link: 2.4 GHz (Physical Interface is Type II PCMCIA card of handheld computers and card/chip in PDA).	[redacted]	[redacted]

UNI Type	Networx Service	Network-Side Interface	[redacted]	[redacted]
5	Wireless Access	Wireless Access Arrangement Interfaces: Air link: 2.4 GHz (Physical Interface is Type II PCMCIA card of handheld computers and card/chip in PDA).	[redacted]	[redacted]
6	Satellite Access	Satellite Access Arrangement Interfaces: V.35, RS-449, RS-232, RS-530, T1, T3, E1, and Air link.	[redacted]	[redacted]
7	Circuit Switched Data Service	1. ISDN at 64 Kbps 2. ISDN at 128 Kbps 3. ISDN dial backup at 64 Kbps 4. ISDN dial backup at 128 Kbps	[redacted]	[redacted]

Interface for Intranet and Extranet Network-based IP VPNs UNI Type 1 (Req_ ID 5684; C.2.7.3.3.1(1))

Qwest fully complies with the 1 Mbps to 1 Gbps Ethernet requirement with Qwest Ethernet Local Access for NBIP-VPNS. Qwest will provide a local loop connection from Agency premises (SDP) to Qwest IP POP, terminating on an Ethernet interconnection switch, and then interconnected to the PE MPLS infrastructure. [redacted]

See Section 3.3.1.3 Emerging Integrated Access for additional details about Qwest's network-side Ethernet interface.

Interface for Intranet and Extranet Network-based IP VPNs UNI Type 2 (Req_ ID 5683; C.2.7.3.3.1(2))

Qwest fully complies with the Private Line UNI requirements from DS-0 to OC-192c, including fractional T-1 and T-3, with Qwest Dedicated IP Access delivered over a private line local loop connection for NBIP-VPNS. Qwest will provide a private line access local loop connection from Agency premises (SDP) to Qwest IP POP, terminating on the NBIP-VPNS PE infrastructure. [redacted]

See Section 4.1.5.5 PLS Optimization and Interoperability for additional details about Qwest's PLS.

Interface for Intranet and Extranet Network-based IP VPNs UNI Type 3 (Req_ ID 5682; C.2.7.3.3.1(3))

Qwest complies with the IP over SONET Service UNI requirements with PPP enabled OC-3c to OC-192c IP to SONET interface [redacted]

See Section 4.1.16.3 Satisfaction of SONETS Specifications for additional details.

Interface for Remote Access Network-based IP VPNs UNI Type 1 (Req_ ID 5680; C.2.7.3.3.2(1))

[redacted]

[redacted]

Interface for Remote Access Network-based IP VPNs UNI Type 2 (Req_ ID 5678; C.2.7.3.3.2 (2))

[redacted]

Interface for Remote Access Network-based IP VPNs UNI Type 3 (Req_ ID 5677; C.2.7.3.3.2 (3))

[redacted]

Interface for Remote Access Network-based IP VPNs UNI Type 4 (Req_ ID 5676; C.2.7.3.3.2 (4))

[redacted]

Interface for Remote Access Network-based IP VPNs UNI Type 5 (Req_ ID 5675; C.2.7.3.3.2 (5))

[redacted]

Interface for Remote Access Network-based IP VPNs UNI Type 6 (Req_ ID 5674; C.2.7.3.3.2 (6))

[redacted]

Interface for Remote Access Network-based IP VPNs UNI Type 7 (Req_ ID 5673; C.2.7.3.3.2 (7))

[redacted]

4.1.9.3.2 Proposed Enhancements to NBIP-VPNS (L.34.1.4.3 (b))

[redacted]

[redacted]

[redacted]

4.1.9.3.3 Network Modifications Required for NBIP-VPNS Delivery (L.34.1.4.3 (c))

Qwest's current NBIP-VPNS solution supports all Networx requirements. Qwest does not need to generate network or service delivery modifications for this Networx service.

4.1.9.3.4 Experience with NBIP-VPNS Delivery (L.34.1.4.3 (d))

Qwest has been supporting Federal, enterprise, and educational Wide Area Network solutions for more than 20 years. Qwest currently supports [redacted] of VPN customers, which translate into more than [redacted] NBIP-VPNS circuit routes. Beginning in 1999, Qwest was one of the first Network Services Providers to deploy premises-based and network-based Virtual Private Networking solutions. Qwest revolutionized the service delivery experience of implementing and maintaining network-based IPsec VPNs for corporate clients through our initial network-based IPsec VPN services known as Private Routed Network. Our IPsec VPN services' expertise led to our production release of Qwest's iQ Networking MPLS-based VPNs in 2003.

[redacted]

Presently, Qwest delivers network based MPLS VPN services to Fortune 1000 financial, manufacturing, healthcare, and high technology corporations. Qwest's customers—as well as third party analyst reports such as Network World Computing—consistently praise our engineering and support services.

4.1.9.4. Robust Delivery of NBIP-VPNS (L.34.1.4.4)

Qwest has examined the demand set requirements for NBIP-VPNS and has determined that Qwest's proven potent planning process meets all requirements. Qwest has strict engineering and design rules to ensure

connectivity and robustness, as well as systems and capacity needed to ensure network performance.

4.1.9.4.1 Support for Government NBIP-VPNS Traffic (L.34.1.4.4(a))

Qwest has examined the NBIP-VPNS traffic requirements of the Government's traffic model. Based on our current backbone utilization and capacity, these bandwidth requirements will not require any significant backbone upgrades. In addition, the total number of ports required does not represent a number significant to our normal edge router capacity planning. Qwest closely and continuously monitors its edge router capacity and backbone network links, and has an aggressive upgrade policy to minimize any effects of congestion on customer traffic flows.

4.1.9.4.2 NBIP-VPNS Measures and Engineering Practices (L.34.1.4.4(b))

The speed and size of Agencies' telecommunications systems can grow easily and transparently on the Qwest network. Qwest has a history of adapting rapidly to meet customer requirements. [redacted]

Qwest built its network to provide high availability to our customers. Qwest's performance measures and engineering practices are designed to provide robustness of the access and backbone networks, to ensure resiliency, to prepare for growth. Our design procedures, network modeling, and circuit route checks provide a high level of customer service.

[redacted]

[redacted]

[redacted]

Qwest engineers continuously model network capacity using current and forecasted traffic to ensure that customer traffic is routed efficiently through the network. This assists with sizing backbone links.

[redacted]

[redacted]

Qwest's Network Planning and Engineering organizations use strict engineering rules to create the highly robust private MPLS core, Public PE and border router architectures that comprise the Qwest domestic and Asian IP network. These organizations continually monitor network performance, and the capacity utilization of core network connections and our peering points, to ensure the highest performance for our customers.

4.1.9.5 NBIP-VPNS Optimization and Interoperability (L.34.1.4.5)

Qwest's Network Engineering and Planning organizations continually improve the technology and performance of Qwest IPS. [redacted]

4.1.9.5.1 Optimizing the Engineering of NBIP-VPNS (L.34.1.4.5(a))

Qwest closely monitors the KPIs [redacted] and constantly optimizes network performance for our customers. Qwest's approach to optimizing the engineering of IP-based and optical services begins with the collection and analysis of network performance data [redacted] These data, along with historical growth rates, are input into network simulation models. The simulation results are compared to AQL targets. [redacted]

[redacted]

4.1.9.5.2 Methods Applied to Optimize the Network Architecture (L.34.1.4.5(b))

[redacted]

Architecture Optimization for Services

As Qwest is in the business of providing network services, the architecture and behavior of the network is predominantly based on the type of service being provided. Before it is launched, every product is developed

and tested against the current architecture. If the existing architecture does not support the product, it is modified and optimized.

[redacted]

Architecture Optimization for Network Growth

The IPS network has been carrying growing amounts of traffic. As the volume of traffic grows, the network architecture needs to be reviewed to ensure that it is still scalable and can be improved to continue providing excellent service to the customers.

[redacted]

Architecture Optimization for Technological Advances

Over the years, the IPS network has evolved to a strategic network for Qwest, and Qwest has always stayed ahead of the technology. As the equipment vendors have provided improved platforms with more features and functionality, Qwest evaluates them against the current architecture. With the help of this evaluation, Qwest can optimize any part of the network and grow with services and customer requirements. [redacted]

For Qwest, the architecture is dynamic and needs to be optimized by using any and all the technology and methodology available to meet customer requirements in a cost effective manner. We are a facility-based provider with our own fiber, transport and IPS network, as shown in the previous examples; we leverage technology and architecture at all layers of network to deliver and build the best of class network.

4.1.9.5.3 Access Optimization for NBIP-VPNS (L.34.1.4.5(c))

Qwest's IP network capability has global coverage. With [redacted] strategically located domestic IP POPs, [redacted] international IP POPs, and [redacted] network access points equipped with multi-service edge platforms to aggregate and transport Federal Government customer traffic to the Qwest IP network, Qwest is able to offer efficient, cost-effective access to IPS. In addition, through partner networks, Qwest supports access to an extensive list of countries.

Qwest has designed, engineered and deployed multi-service edge switch routers with high-port density to provide a full suite of services for diverse customer applications. These multi-service edges are connected directly to the core routers via multiple high-speed uplinks for diversity and redundancy. These intelligent edge routers allow Qwest to create new, differentiated service offerings, continue support for existing services, and optimize the network infrastructure. [redacted]

With these multi-service edges, the network has less equipment, fewer layers of equipment, and less complexity to operate and manage. Qwest will no longer have to add older IP routers and older Layer 2 switches that were built with limited services and port density, and thus will save in cost and rack spaces. Further reduction in capital and operating expenses can be realized

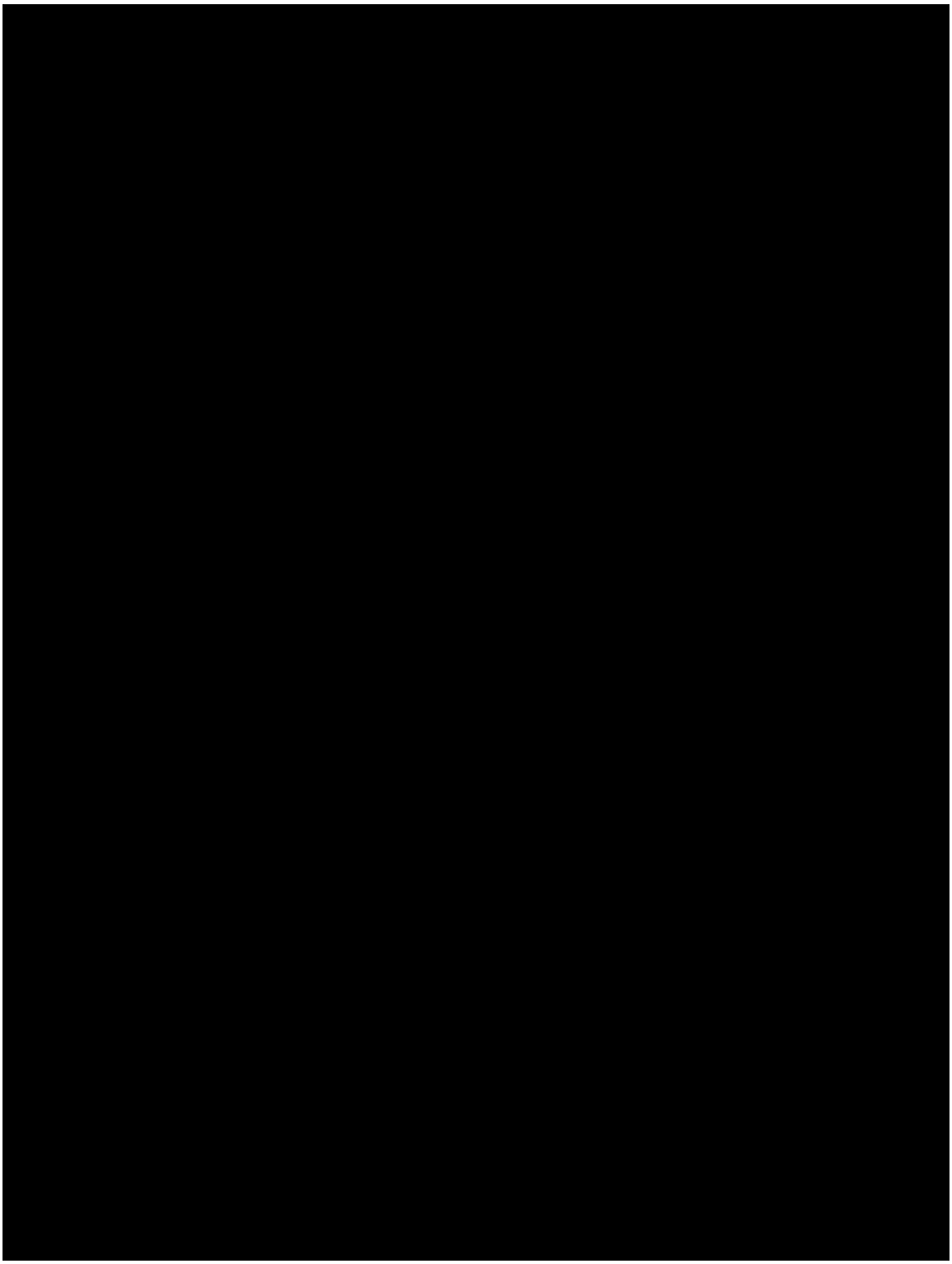
as older equipment at the POPs are being decommissioned and removed after traffic has been migrated over to the new multi-service edges.

4.1.9.5.4 Vision for NBIP-VPNS Service Internetworking (L.34.1.4.5 (d))

Qwest is committed to the elimination of single-purpose, stovepipe networks that create planning, operations, and interoperability issues for our customers.

Qwest's service delivery model supports multiple types of customer requirements. Qwest's approach for network architecture evolution guides our investments and provides the overall direction for our technology evolution and services convergence. Qwest's service delivery model also allows us to assess the interoperability impacts of changes in the technical elements in each network area (e.g., Access, Service Control, Edge, Core, MPLS and Optical).

[redacted] shows Qwest's model for a migration to a packet oriented infrastructure with a comprehensive control plane that links the MPLS to the optical transport environment. Using this model, Qwest has already evolved our architecture [redacted]



[redacted]

An integrated service control system is required to enable service convergence that complements network convergence. Together, these capabilities define an adaptable, enabled, and integrated architecture for Qwest's future services that meet changing business needs. [redacted]

Within the context of Qwest's Network Architecture evolution, the Services Control Architecture provides a structured framework for using the capabilities of the underlying transport and access networks to develop, deploy, customize and integrate enhanced communication services.

[redacted]

[redacted]