

#### **4.2.8 PREMISES-BASED IP VPN SERVICES (PBIP-VPNS) (L.34.1.4.6)**

***Qwest achieved an industry first with our premises-based IP VPN services. Our Networx PBIP-VPNS employs a proven service delivery model to ensure high quality and secure services.***

Qwest has been delivering standards-based PBIP-VPNS, which includes secure intranet, extranet, and remote access connectivity, since [REDACTED]. Qwest's PBIP-VPN services combine Service Enabling Device (SED) health and welfare monitoring, Internet Protocol Security (IPsec) tunnel management, encryption, key management and security access controls. To provide maximum flexibility in meeting a wide range of bandwidth, cost, and security requirements, Qwest delivers the same features and functionality across multiple hardware and software platforms from industry leaders [REDACTED]

[REDACTED] Qwest believes securing a network goes beyond encrypting the data traveling on the network. We will include access controls to sensitive data by authentication and security policy. We have extended our proposed PBIP-VPNS solution to include services that combine routing, IPsec encryption, auditing, and security policy enforcement.

As an industry leader, with [REDACTED] VPN locations under management, Qwest has extensive experience delivering secure networking solutions to educational institutions, city and state governments [REDACTED]

[REDACTED]  
[REDACTED]  
[REDACTED]  
[REDACTED]

**Figure 4.2.8-1** provides an easy reference to correlate the narrative requirement to our proposal response.

**Figure 4.2.8-1. Table of PBIP-VPNS Requirements**

Req_ID	RFP Section	Proposal Response
31811	C.2.7.2.3.1 (1)	4.2.8.3.3
31812	C.2.7.2.3.1(2)	4.2.8.3.3
31814	C.2.7.2.3.2 (1)	4.2.8.3.3
31815	C.2.7.2.3.2 (2)	4.2.8.3.3
31816	C.2.7.2.3.2 (3)	4.2.8.3.3
31817	C.2.7.2.3.2 (4)	4.2.8.3.3
31818	C.2.7.2.3.2 (5)	4.2.8.3.3
31819	C.2.7.2.3.2 (6)	4.2.8.3.3
31820	C.2.7.2.3.2 (7)	4.2.8.3.3

**4.2.8.1 Reserved (L.34.1.4.6 (a))**


**4.2.8.2 Reserved (L.34.1.4.6 (b))**

**4.2.8.3 Satisfaction of PBIP-VPNS Requirements (L.34.1.4.6(c))**

Qwest will deliver PBIP-VPNS that exceeds RFP requirements for secure intranet, extranet, and remote access connectivity using standards compliant, industry-leading technology. Qwest understands that different Agencies have different application sets, security requirements, and cost controls.

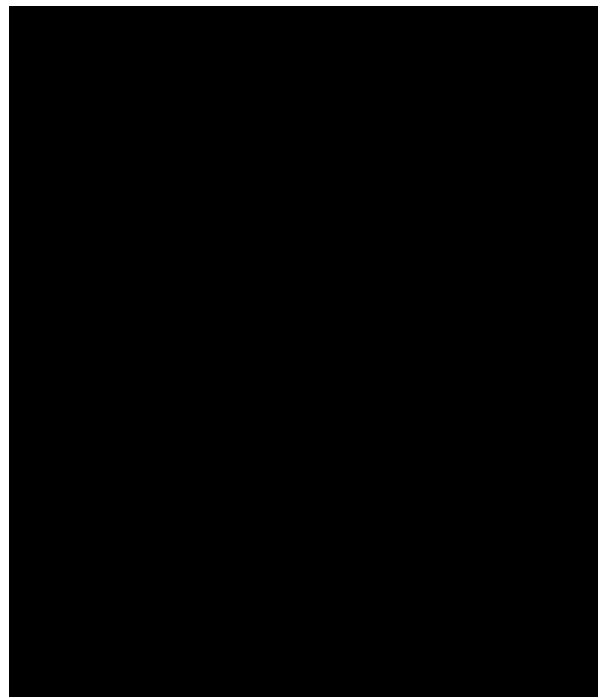
We offer a flexible building block approach to meet varying needs. Agencies can take advantage of Qwest’s wide range of interoperable FIPS-140-2 compliant SEDs that deliver encryption, routing, auditing, and firewall policy enforcement. Qwest can tailor a solution from these building blocks to best meet an Agency’s diverse requirements. For example, a branch site might use a Cisco routing device with IPsec encryption capabilities to securely interact with a headquarters location using a Check Point VPN device delivering auditing, access control, and encryption. Simultaneously, a remote access user might be accessing Agency resources via a secure

desktop VPN client or browser using SSL. Qwest will manage all of these technologies as a single PBIP-VPNS or Agency Closed User Group (CUG) if required. The PBIP-VPNS is transport and access agnostic, however, if the entire underlying network is Qwest-provided, additional advantages can be realized by the Agency. For example, if desired, users can take extra advantage of a security-aware network that allows PBIP-VPNS traffic to be prioritized over non-encrypted traffic. Users will receive integrated reporting that provides a view into VPN activity, network usage, and bandwidth utilization statistics.

Qwest offers a wide range of PBIP-VPNS solutions. Qwest broadly defines PBIP-VPNS as secure site-to-site, remote-to-site, and external partner-to-site connectivity. Secure connectivity is achieved through configuring, managing, and maintaining tunnels between intranet, partner, and remote worker locations.  shows an example of a PBIP-VPNS solution spanning these three domains.

In most cases, secure routing is achieved through SEDs that operate as VPN gateways or encrypting devices. For small locations, a Qwest-provided desktop client can deliver security and IPsec encryption features, and may be a more effective mechanism to access Agency resources.

Qwest PBIP-VPNS solutions are delivered as an overlay service



to a transport or access solution that can be Qwest-provided or non-Qwest-provided. While PBIP-VPNS have traditionally existed as self-contained networking solutions, Qwest believes Agencies may need to combine Wide Area Network (WAN) solutions which include PBIP-VPNS and Network-Based Internet Protocol VPNS (NBIP-VPNS). For example, an Agency implementing a Multi-Protocol Label Switching (MPLS)-based WAN may need to securely communicate with another Agency utilizing PBIP-VPNS. Agencies may also be merged as part of a reorganization effort with a goal of minimizing disruption and retaining original investments in network infrastructure. Qwest’s experience with large scale network deployments, in support of extranet or intranet expansion, suggests that there will be opportunities to integrate VPN technologies. For that reason, Qwest supports interoperability between our Networx NBIP-VPNS and PBIP-VPNS.

Qwest is proposing support for a range of FIPS-140-2 compliant devices to meet the needs of the Agency. SEDs will be available for all mandatory interface types. Some of the proposed SEDs that provide routing and encryption can function as Agency edge routers. Other SEDs combine firewall, encryption, and audit controls, but do not natively provide routing functionality. These SEDs will be deployed behind a router at the Agency’s location. Smaller locations can use either a desktop client or a small-office gateway. Redundancy and failover options exist for all proposed solutions.

**Figure 4.2.8-3** describes the approach for each solution type.

**Figure 4.2.8-3 Description of Qwest’s Approach to Networx PBIP-VPN Solution Types**

Type		
Intranet		
Extranet		

Type		
Remote		

#### 4.2.8.3.1 Satisfaction of PBIP-VPNS Capabilities Requirements (L.34.1.4.6(c))

Qwest satisfies all capability requirements for PBIP-VPNS, as described in **Figure 4.2.8-4**. Qwest fully complies with all mandatory stipulated and narrative capabilities requirements for PBIP-VPNS. The text in Figure 4.2.8-4 provides the technical description required per L.34.1.4.6(c) and does not limit or caveat Qwest’s compliance in any way.

**Figure 4.2.8-4. Qwest’s Technical Approach to PBIP-VPNS Capabilities**<sup>[g1]</sup>

ID	Capability	
1	Multiple Tunneling Standards	
2	Encryption Levels	
3	Authentication Services	
4	Reserved	
5	Access Methods	
6	Dial Access Connectivity	
7	Layered Security Architecture	
8	Pro-Active Management	

ID	Capability	
9	Network Design & Engineering Service	
10	Secure Routing Service	
11	Traffic Management	

### PBIP-VPNS Design and Engineering

[Redacted content]



Depending on the scope of individual Agency deployments and on availability of existing access or SED, there may be some variations to the process outlined below. In general, a project manager coordinates multi-site installations for an Agency. The project manager understands the overall goals of the deployment projects, associated timelines and related dependencies. By example, assume Qwest is deploying a dynamic, multipoint VPN for a mid-size Agency. This deployment will include VPN gateways with firewall enforcement at the headquarters' location, encrypting VPN SEDs at branch locations, and desktop clients deployed for mobile workers. **Figure**



[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]	[Redacted]

[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]	[REDACTED]

Once service is turned up at a particular location, the overall Agency CUG is regression tested for interoperability. If testing indicates that traffic is flowing, encrypted and security policies are properly being enforced across all sites, Qwest operations assumes day-to-day management of Agency's VPN.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Large redacted text block]

[Redacted content]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

[Redacted]

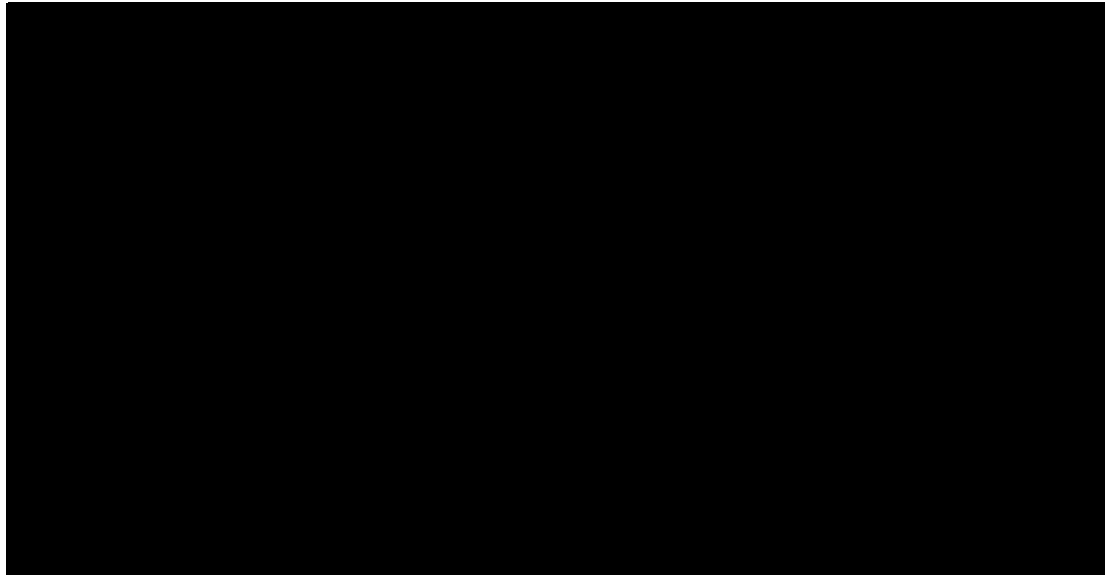
[Redacted]

[Redacted]

[Redacted]

[Redacted]

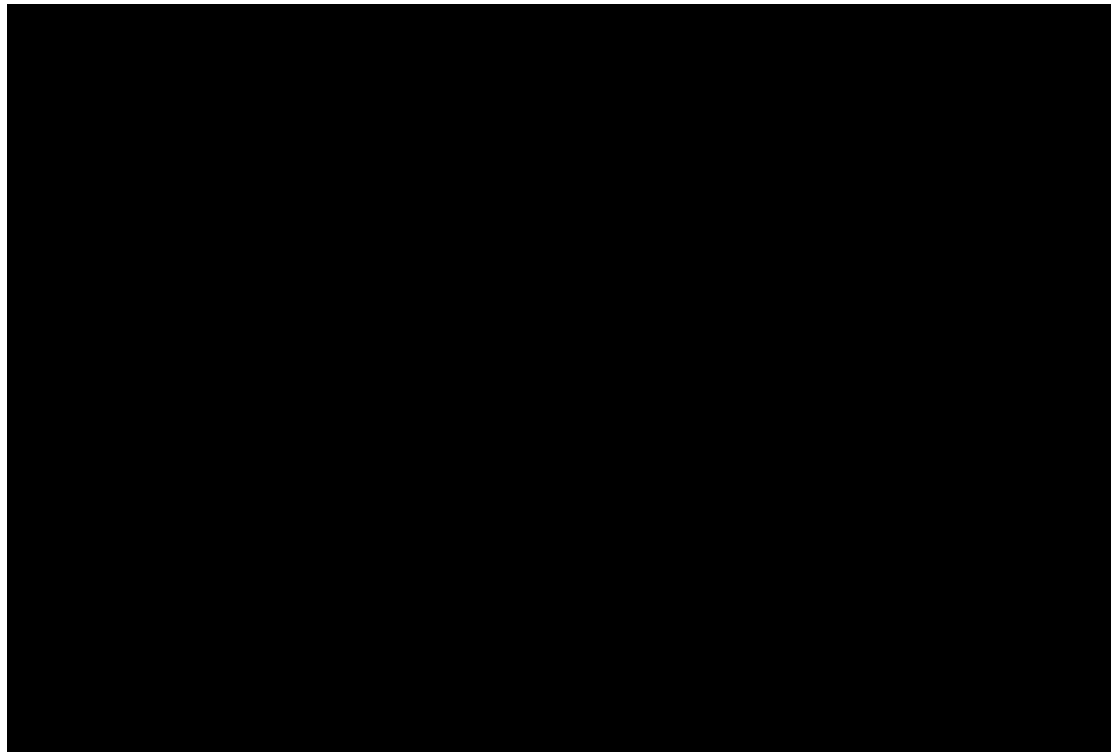
[Redacted]



When building IPsec tunnels to partner locations, information on the remote termination site must be determined in order to synchronize configuration settings that allow secure communication. [REDACTED]



Agency users will employ the secure Qwest Control Network Portal as a primary method for contacting Qwest for change requests, to open trouble tickets, to schedule maintenance windows, and to view topology and usage reports.



Qwest will provide 24x7x365 configuration and ongoing management, monitoring, and administration of our Networx PBIP-VPNS. Managed VPN gateways provide secure, end-to-end encrypted tunnel communication between:

- Agency locations (intranet)
- Partner locations and the Agency (extranet)
- Remote or mobile workers and the Agency (remote)

Qwest service delivery teams extend from sales engineering groups that assist in understanding and defining the requirements, to project management teams who coordinate the installation process, to operations teams that provide 24x7x365 management of the VPN gateways, to risk management groups which audit operational process and controls consistent

with Qwest's position as an industry-leading service provider, and finally, to our forward-looking new technology groups that evaluate new software versions, hardware configurations, and potential enhancements as part of our service innovation program.

Qwest provides full-lifecycle support on our PBIP-VPN solutions from pre-sales engineering through ongoing monitoring, management, and administration [REDACTED]

[REDACTED]

[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]	[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

**4.2.8.3.2 Satisfaction of PBIP-VPNS Features Requirements  
(L.34.1.4.6(c))**

Qwest satisfies all features requirements for PBIP-VPNS as described in [REDACTED] Qwest fully complies with all mandatory stipulated and narrative features requirements for PBIP-VPNS. The text in Figure 4.2.8-14 provides the technical description required per L.34.1.4.6(c) and does not limit or caveat Qwest's compliance in any way.

**Figure 4.2.8-14. Qwest's PBIP-VPNS Supports All Features Required for Networkx**

ID	Feature	
1	High availability options for Customer Premise Equipment (CPE)	[Redacted]
2	Internet Gateway Service	[Redacted]
3	Interworking Services	[Redacted]
4	Key Management	[Redacted]



ID	Feature	
5	Security services	<div style="background-color: black; width: 100%; height: 100%; min-height: 300px;"></div>

Qwest supports the required user types for PBIP-VPNS. Qwest will manage the connectivity and SED required to create, maintain, and administer secure IPsec tunnels between Agency locations:

- Locations comprising single Closed User Group (CUG)
- CUG and extranet partner
- CUG and remote access user

Qwest PBIP-VPNS solutions use FIPS-140-2 compliant devices at Agency or partner endpoints accessing public, private, or MPLS networks in speeds ranging from dial-up to broadband to high speed optical. Qwest VPN services are layered on top of FIPS-140-2 compliant, standards-based solutions from industry leaders [REDACTED]

[REDACTED] All applicable IPsec authentication, encryption, and key management protocols are supporting including AH,

ESP, 3DES, AES, and RC4. Qwest is an active member and driving force on a number of Internet Engineering Task Force (IETF) task forces including those which are IPsec, MPLS, Layer 3 VPN, and IPv6 specific. Qwest will support Agencies as required to comply with Office of Management and Budget (OMB) IPv6 directives as Qwest deploys IPv6 commercially. Qwest supports SSL-based VPN options allowing secure Web-based access to resources.

In addition to MPLS Virtual Route Forwarding, Qwest supports standards such as L2TP, GRE, and those associated with IPsec specifications. SSL-based VPNs can also be used to access network resources.

Qwest supports all required encryption standards including 3DES, AES, and RC4. Qwest will provide a wide range of SED options to ensure that the needs of each individual location or Agency can be met by one or more available service options.

Qwest remote access clients support all of the listed authentication mechanisms. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Qwest VPN solutions are access and SED-agnostic allowing Qwest and non-Qwest provided access to be used. Qwest views PBIP-VPNS as a security feature of transport. Access options range from broadband DSL, local ISP, and cable, to dedicated access options that span speeds from

DS-0 to Gigabit Ethernet to OC-48. Qwest provides dial access connectivity with voice grade service to 56 Kbps and ISDN access of Nx64 Kbps.

Qwest uses a layered security architecture that combines access control via firewall policies, address hiding via network address translation, authentication, and encryption to mitigate the risk of attacks. The proposed architecture incorporates multiple challenges and does not allow single entry points into the network.

[Redacted]

[Redacted]

Qwest will provide network design and engineering service to provide bandwidth and SED design as part of the standard pre-installation process and as part of ongoing service management as needed.

Qwest uses a comprehensive security management platform that allows centralized policy enforcement across the VPN. Qwest provides

secure routing via a number of mechanisms; privatization of our core network which prevents IP addresses used between private edge routers from being “seen” by public networks, network and port address translation that allows customer to use unregistered address space on their internal networks, and encryption allowing inter-site routing to occur without exposing any of that information to other network users.

Qwest will ensure that customers that require traffic management will be provisioned with SEDs that allow an Agency’s VPN administrators to classify packets for preferential treatment or QoS.

Qwest also satisfies all feature requirements for PBIP-VPNS as described in Figure 4.2.8-14.

#### **4.2.8.3.3 Satisfaction of PBIP-VPNS Interface Requirements**

**(L.34.1.4.6(c)) (C.2.7.2.3.1 (1), C.2.7.2.3.1(2), C.2.7.2.3.2 (1), C.2.7.2.3.2 (2), C.2.7.2.3.2 (3), C.2.7.2.3.2 (4), C.2.7.2.3.2 (5), C.2.7.2.3.2 (6), C.2.7.2.3.2 (7), Req\_IDs 31811, 31812, 31814, 31815, 31816, 31817, 31818, 31819, 31820)**

Qwest supports the required interfaces and protocol types with the SEDs identified as shown below in **Figure 4.2.8-15** (for intranet and extranet applications) and **Figure 4.2.8-16** (for remote access applications). Qwest fully complies with all mandatory stipulated and narrative interface requirements for PBIP-VPNS. The text in Figures 4.2.8-15 and 4.2.8-16 provides the technical description required per L.34.1.4.6(c) and does not limit or caveat Qwest’s compliance in any way.

Over the contract length, hardware manufacturers may add/delete systems from their list of supported devices. Qwest will use our Technology Management teams to evaluate new hardware and software platforms to offer the most cost-effective, feature-rich platforms to Agencies using PBIP-VPNS.

All proposed solutions are IPv4 compliant and will support Federal Agencies as required to comply with OMB IPv6 directives.

**Figure 4.2.8-15. Summary of Qwest’s Support for Intranet and Extranet PBIP-VPNS User-to-Network Interfaces (UNIs)**

UNI Type	Interface/ Access Type	Network-Side Interface	Protocol Type (See Note 2)	[REDACTED]
1	Ethernet Interface	1. 1 Mbps up to 1 GbE (Gigabit Ethernet) 2. 10 GbE (Optional)	IPv4/IPv6 over Ethernet	[REDACTED]

**Figure 4.2.8-16. Summary of Qwest’s Support for Remote Access PBIP-VPNS UNIs**

UNI Type	Interface/Access Type	Network-Side Interface	Protocol Type (See Note 1)	[REDACTED]
1	Voice Service	Analog dialup at 56 Kbps	Point-to-Point Protocol, IPv4/v6	[REDACTED]
2	DSL Service	xDSL access at 1.5 to 6 Mbps downlink and 384 Kbps to 1.5 Mbps uplink	Point-to-Point Protocol, IPv4/IPv6	[REDACTED]
3	Cable high speed access	320 kbps up to 10 Mbps	Point-to-Point Protocol, IPv4/IPv6	[REDACTED]
4 [Optional]	Multimode/Wireless LAN Service	MWLANS User-to-Network Interfaces:	Not Applicable	[REDACTED]
5 [Optional]	Wireless Access	Wireless Access Arrangement Interfaces.	Not Applicable	[REDACTED]
6 [Optional]	Satellite Access	Satellite Access Arrangement Interfaces	Not Applicable	[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	Point-to-Point Protocol, IPv4/IPv6	[REDACTED]

**Interface for Intranet and Extranet Premises-Based IP VPNs UNI Type 1,  
Network-Side Interface 1 (Req\_ID 31811)**

Qwest's PBIP-VPNS solutions are access-agnostic and can be delivered on top of a wide range of Qwest and non-Qwest provided access methods. These PBIP-VPNS solutions are typically delivered via an edge device or combination of edge devices that provide access termination, encryption and security enforcement.

In situations where Ethernet access is required, Qwest will deploy terminating SEDs that support Ethernet interfaces. For speeds up to 100 Mbps, Qwest will deploy configurations with 10/100 Base T connections. For faster connections, Qwest will deploy Gigabit Ethernet interfaces. The device will provide access to the network and VPN tunnel connectivity that supports IPv4 and will support Agencies as required to comply with OMB IPv6 directives as Qwest deploys this service commercially.

**Interface for Intranet and Extranet Premises-based IP VPNs UNI Type 1,  
Network-Side Interface 2 (Req\_ID 31812)**



## Interface for Remote Access Premises-Based UNI Type 1 (Req\_ID 31814)

Remote access VPNs over dial-up access will be supported via client installed software on the user desktop. [REDACTED]

[REDACTED] Dial-up access would typically allow users to connect to a public dial-up network with connectivity to the Internet. Agencies can purchase their dial-up access from Qwest under the Networkx services that include this option (for example, IPS or NBIP-VPN offerings), or they may procure the dial-up access component from another provider. After authentication to the dial-up network, an encrypted session will be established between the user desktop and VPN SED on the Agency's network. The client can be directed to one primary and multiple backup entry points into the network. Layered security architecture provides an additional security check on security gateways prior to entering the Agency's network. Point-to-Point Protocol (PPP) would be a supported standard for dial-up access. [REDACTED]

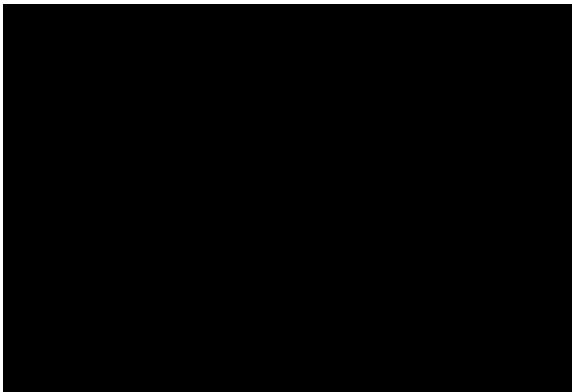
[REDACTED] provides an overview of remote access to our PBIP-VPNS. While hardware-based solutions could be offered for dial-up locations, the client solution will be most cost-effective in all situations. Qwest offers options which combine the VPN termination and security gateways into one edge device or they can remain separate.


**Interface for Remote Access Premises-Based IP VPNs UNI Type 2  
(Req\_ID 31815)**

For DSL access up to 6 Mbps, Qwest offers two options: the client option described above for UNI Type 1 or a SED alternative. For these options, Qwest expects that the existing termination device (e.g. DSL modem) will provide access termination and the SED will provide security enforcement and/or encryption functionality. The connection from the DSL termination device and the Qwest managed SED will be 10/100 Ethernet. PPP is supported. Currently, Qwest supports IPv4 and will support Federal Agencies as required to comply with OMB IPv6 directives as Qwest deploys this service commercially.

**Interface for Remote Access Premises-Based IP VPNs UNI Type 3  
(Req\_ID 31816)**

For cable access up to 10 Mbps, Qwest offers two options: the client option described above in the section above for Req\_ID 31814, *Interface for Remote Access Premises-based UNI Type 1*, or the SED alternative. For these VPN options, Qwest expects that the existing termination device (e.g.



cable modem) will provide access termination and the SED will provide security enforcement and/or encryption functionality. The connection from the DSL termination device and the Qwest managed CPE will be 10/100 Ethernet. 

summarizes both DSL and cable remote access options. Point-to-Point Protocol (PPP) is supported. Currently, Qwest supports IPv4 and will support



Agencies as required to comply with OMB IPv6 directives as Qwest deploys this service commercially.

**Interface for Remote Access Premises-Based IP VPNs UNI Type 4  
(Req\_ID 31817)**

[Redacted]

**Interface for Remote Access Premises-Based IP VPNs UNI Type 5  
(Req\_ID 31818)**

[Redacted]

**Interface for Remote Access Premises-Based IP VPNs UNI Type 6  
(Req\_ID 31819)**

[Redacted]

**Interface for Remote Access Premises-Based IP VPNs UNI Type 7  
(Req\_ID 31820)**

ISDN access sites requiring VPN services will use a model similar to DSL and cable described above using ISDN BRI at primary access or dial backup speeds of 64 or 128Kbps. The existing devices terminating ISDN will still be required. Network interfaces between the Qwest-managed VPN device and ISDN device will be 10/100 Ethernet. Today, PPP is supported. Currently, Qwest supports IPv4 and will support Agencies as required to comply with OMB IPv6 directives as Qwest deploys this service commercially.

**4.2.8.4 PBIP-VPNS Quality of Service (L.34.1.4.6(d))**

Qwest’s PBIP-VPNS is layered on top of existing access services which may be delivered by Qwest, or many different network providers. Qwest will design solutions with appropriate SED processing power to minimize latency caused by encryption or firewall policy applications. [REDACTED]

[REDACTED]

Qwest’s PBIP-VPNS meets the latency requirements when deployed on Qwest transport using VPN gateways with appropriate processing power. When an Agency is not using Qwest as the access provider, Qwest will provide the Agency with latency reporting data necessary to manage the Agency’s access provider to the required AQLs. Qwest meets the time to restore targets with and without dispatch service under the definitions outlined in RFP Section 3.3.1.2.4, Fault Management (**Figure 4.2.8-19**).

**Figure 4.2.8-19. Qwest Performance Standards for PBIP-VPNS**

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	[REDACTED]
Av(VPN)	Routine	99.9 percent	≥ 99.9	[REDACTED]
Latency (CONUS)	Routine	120 ms	≤ 120 ms	[REDACTED]
Latency (OCONUS)	Routine	300 ms	≤ 300 ms	[REDACTED]
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	[REDACTED]
	With Dispatch	8 hours	≤ 8 hours	[REDACTED]

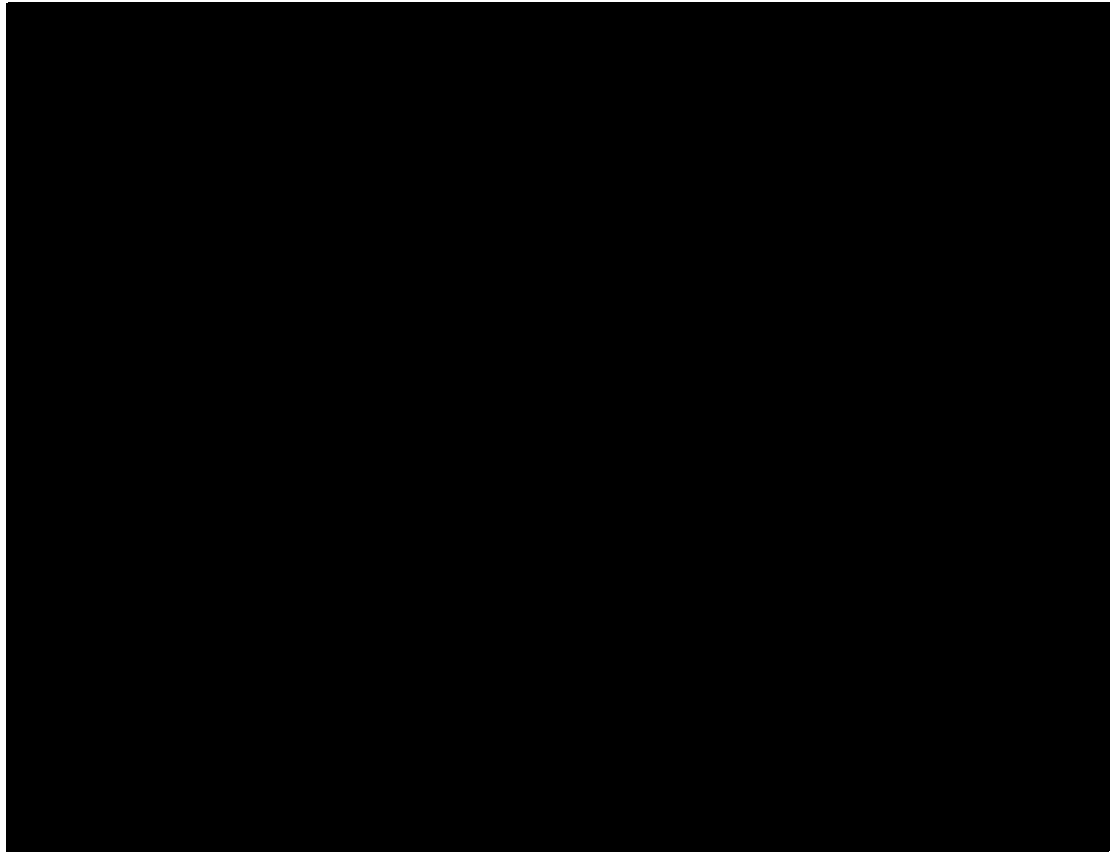
[REDACTED]

[Redacted text block]

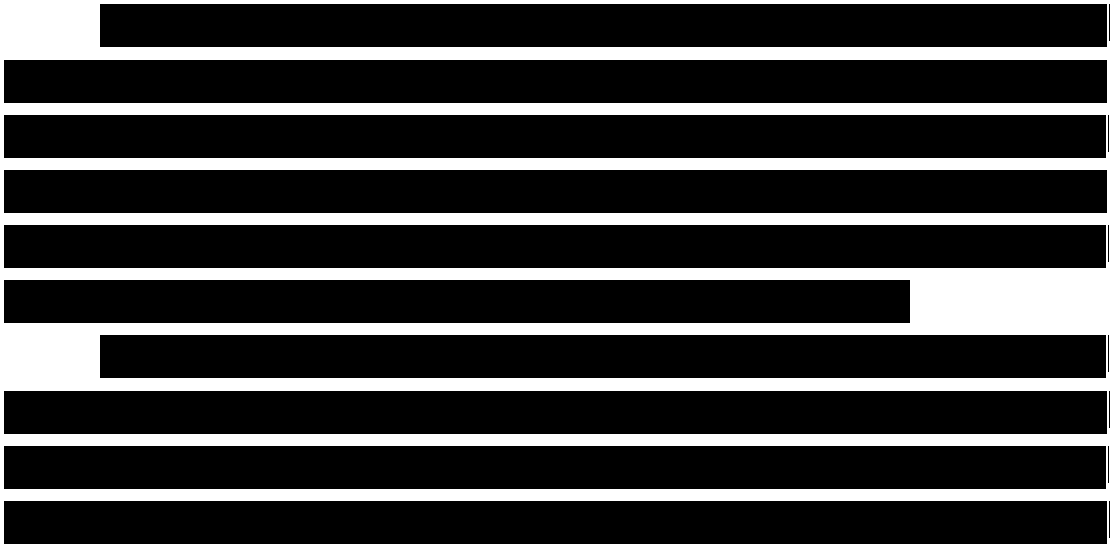
Qwest's engineering objective with VPN performance targets is to prevent the management component from introducing performance impacts that would cause the underlying transport performance metrics not to be met. Qwest uses a comprehensive end-to-end performance monitoring system to verify that VPN services are not impacting transport service delivery metrics.

[Redacted text block]

[Redacted text block]



**4.2.8.5 Qwest's PBIP-VPNS Exceeds Service Requirements  
(L.34.1.4.6(e))**



[REDACTED]

**4.2.8.6 Experience with PBIP-VPNS Delivery (L.34.1.4.6(f))**

Since [REDACTED], Qwest has focused on delivering secure wide area networking solutions to our customers. Qwest currently manages over [REDACTED] VPN sites that address a wide range of customer scenarios. Understanding that there is no single solution appropriate for all environments, Qwest's VPN solutions were engineered to support multiple hardware and software solutions. All support IPsec tunneling capabilities, by incorporating platforms that embed routing, firewall, address translation, port translation, authentication, and auditing features.

Qwest has invested heavily in training and certification of our provisioning and operations teams and we continue to update our knowledge database tools daily with experience gained from thousands of customer VPN deployments. Most recently, Qwest has begun integrating traditional VPN solutions as extensions or as overlays to MPLS-based offerings. As VPN and MPLS technologies evolve, Qwest is committed to providing secure wide area networking solutions that meet all Agency requirements.

[REDACTED]

**4.2.8.7 Characteristics and Performance of Access Arrangements  
(L.34.1.4.6(g))**

PBIP-VPN deployments are SED-oriented, secure management services which are delivered over separately ordered IP transport and access services. The characteristics and performance of the access arrangements that will connect to Qwest's backbone network to ensure service quality and delivery of IP services are described in Section 4.1.1 Internet Protocol Services.

**4.2.8.8 Approach for Monitoring and Measuring PBIP-VPNS KPIs and  
AQLs (L.34.1.4.6(h))**

[REDACTED]

[Redacted text block]

[Redacted text block]

[Redacted text block containing multiple paragraphs of blacked-out content]



[Redacted content]

[Redacted content]

[Redacted]

**Use of Statistical Sampling in lieu of Direct KPI Measurements**

[Redacted]

**The Use of Government Furnished Property**

[Redacted]

[REDACTED]

#### **4.2.8.9 PBIP-VPNS Support of Time-Sensitive Traffic (L.34.1.4.6(i))**

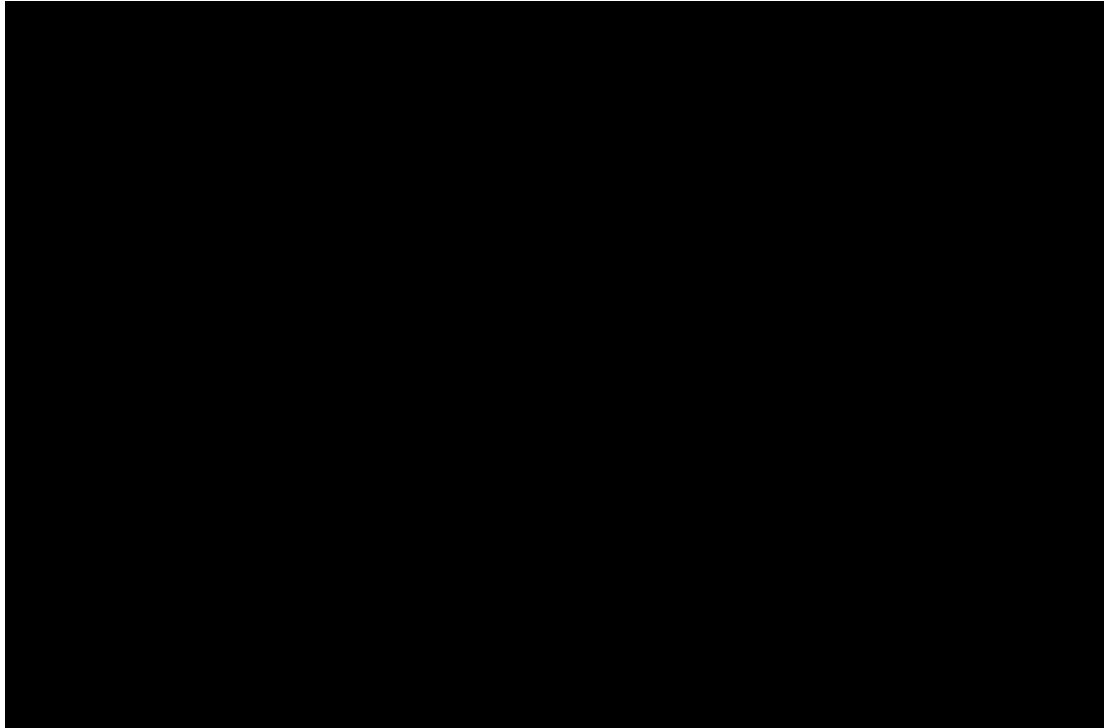
Qwest supports implementation and operation of PBIP-VPNS solutions using a range of access and transport methods that support CoS/QoS type mechanisms to ensure the quality of time-sensitive traffic. Our network engineering and capacity planning ensure our ability to meet the challenge of voice transport. Qwest uses Voice over Internet Protocol (VoIP) switches connected via our MPLS network to handle [REDACTED] of PSTN traffic every month, indistinguishable from traditional TDM-based switches.

Qwest has best-in-class technical solutions and implementations of QoS mechanisms for both our Integrated ATM/Frame Relay network and our IP/MPLS network.

For both ATM and Frame Relay, the Qwest network supports a virtual guarantee of cell or packet delivery using Constant Bit Rate (CBR), Variable Bit Rate-real time (VBR-rt), and Variable Frame Rate-non real time (VFR-nrt). With the network acting as a nearly perfect channel for these service classes, IP packet delivery for VoIP or video conferencing (for example, H.323) is correspondingly very high ([REDACTED]). Since the traffic contract is obeyed end-to-end, no other traffic on the network can interfere with the minimum data rate in the virtual circuit's traffic contract parameters. Combined with the capacity planning described in Section 3.2, even failures of core ATM switches or backbone circuits will not reduce the network capacity to a point where it impacts customers' minimum traffic contract parameters.

Traditional IP networks have evolved around “best effort” service and typically have not provided guarantees for key performance criteria. The need to support real-time services on IP networks has driven the development of IP prioritization and queuing mechanisms as well as MPLS technology. The Qwest network is engineered to enable QoS to prioritize certain types of traffic over other types of traffic if there is congestion in the network.

As described in Section 3.2, Qwest’s MPLS network supports the ability to prioritize LSPs. This means that the IP network supporting our VoIP network has a higher priority than our VPN network and than the network that provides Internet services. Because of our ability to manage and prioritize traffic, impacts from different traffic loads can be handled immediately to ensure no impact to the bandwidth required to support all of our customer’s VPN and VoIP traffic requirements. [REDACTED] highlights the quality of service enabled by Qwest’s converged IP MPLS.

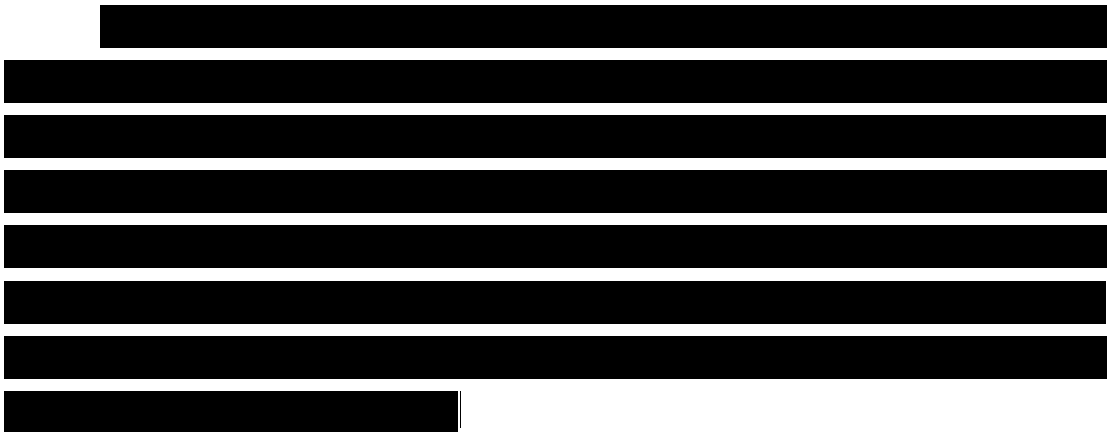
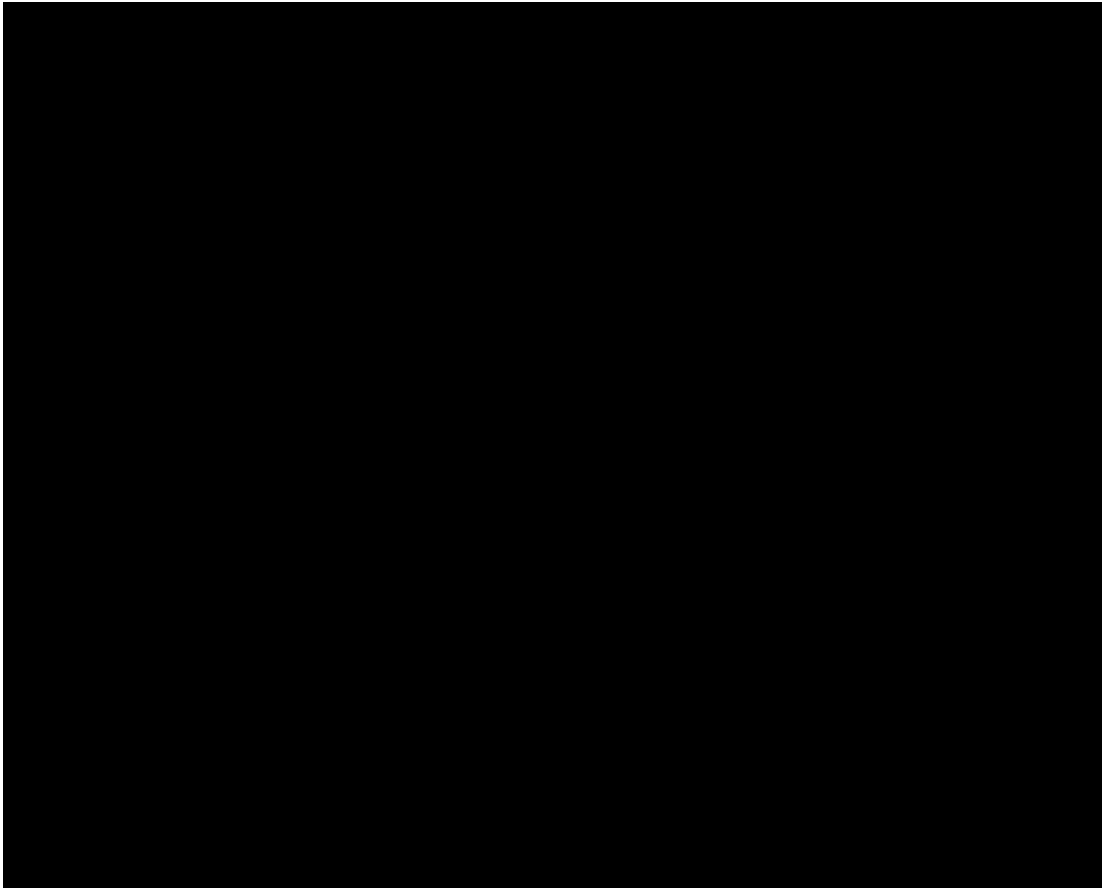


Qwest's IP MPLS network employs standards-based MPLS and IP-based QoS mechanisms to enable high quality voice, video, and data over an IP backbone. The process of applying QoS in a network, as previously shown in Figure 4.2.8-22, consists of multiple actions, defined as follows:

- **Classification:** Classifies different applications based on their relative network performance needs. For example, is the point-of-service application more or less sensitive to latency, jitter and loss than the VoIP application?
- **Marking:** Marks packets belonging to the applications are classified so they may be recognized. For example, setting the Internet protocol precedence or DiffServ Code Point (DSCP) bits.
- **Policing:** Packets determined to be out of profile (that is, not conforming to the QoS policy), are either dropped or re-marked into lower priority packets (for example, rate-limiting).

- **Shaping:** Out-of-profile packets may also be buffered and shaped to conform to the configured QoS policy.
- **Queuing:** Scheduler resources are allocated to different classes (or queues) so traffic may be serviced (for example, last in, first out; first in, first out; weighted fair queuing; and low-latency queuing).

[Redacted content]





[REDACTED]

These QoS actions ensure that low-latency, real-time applications such as voice can share the same access lines and core with non real-time data applications. Our convergence approach means that Qwest data services will migrate to a common IP/MPLS network, so we can easily plan and identify any QoS issues. As described in Section 3.2, Qwest's conservative and aggressive backbone and access bandwidth planning methodology ensures that there is sufficient bandwidth to meet our customer's full port-limited capability, even in the event of core router failure or an access router or backbone trunk failure.

**4.2.8.10 PBIP-VPNS Support for Integrated Access (L.34.1.4.6(j))**

PBIP-VPNs deployments are SED-oriented secure management services which are delivered over separately ordered IP transport and access services. Qwest's approach to providing integrated access to locations that support customer applications with different performance requirements (e.g., voice, data, and video) include traffic allocation via separate virtual circuits or traffic shaping via quality of service parameters. Those approaches are defined in Section 3.3.1.

**4.2.8.11 Infrastructure Enhancements and Emerging Services (L.34.1.4.6(k))**

Qwest has mature processes that enable us to envision, research, evaluate, engineer, deploy, and operate new or emerging services. Driven initially by the Chief Technology Office, headed by the Qwest CTO, Qwest evaluates new products and technologies for incorporation into the Qwest network, in partnership with Qwest Product Management.

[REDACTED]

[Redacted]

[Redacted]

Qwest recognizes that converged customer care and support will be a major challenge that impacts processes, systems and people. Convergence extends and impacts every facet of the traditional telecommunications value chain.

[Redacted]


[Redacted text block containing multiple paragraphs of blacked-out content]

[Redacted text block]

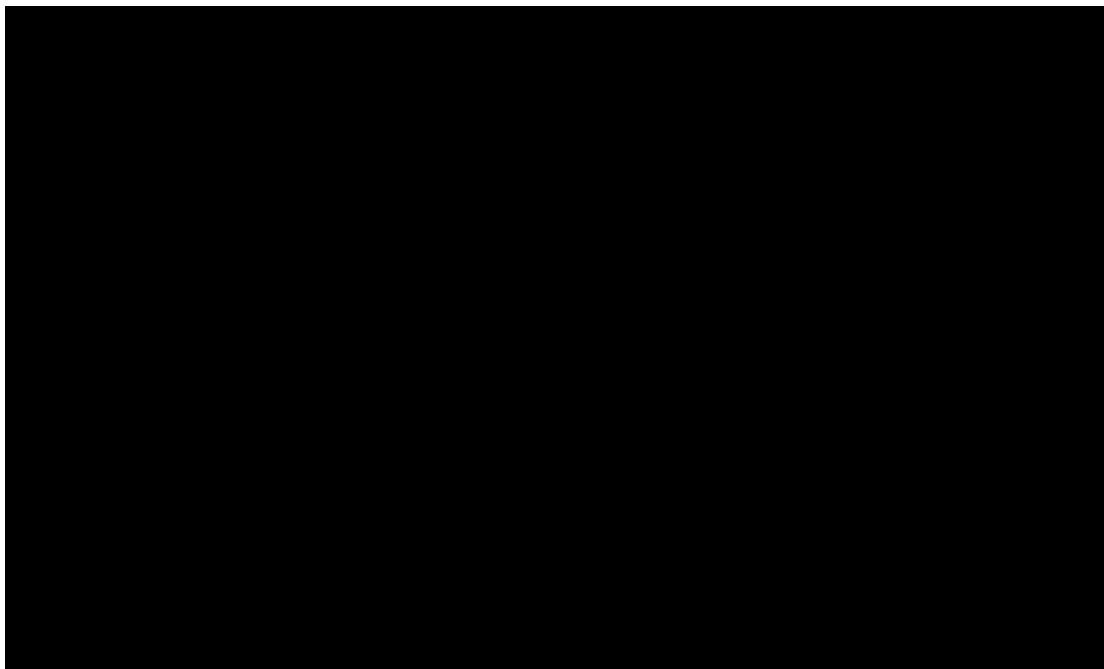
#### **4.2.8.12 Approach for Network Convergence (L.34.1.4.6(I))**

Qwest already has a clear approach and has made significant progress in deploying a network that not only enables convergence from the Agency's perspective, but is also a highly converged platform in itself. Qwest has moved to a packet-based architecture to enable network evolution and convergence. Centered on our private MPLS-based core, we have already converged our IP-based services over this network.

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

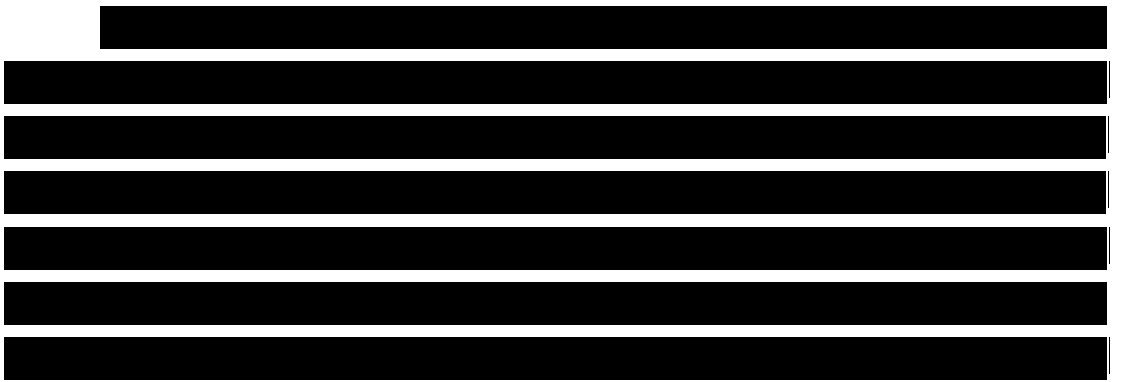
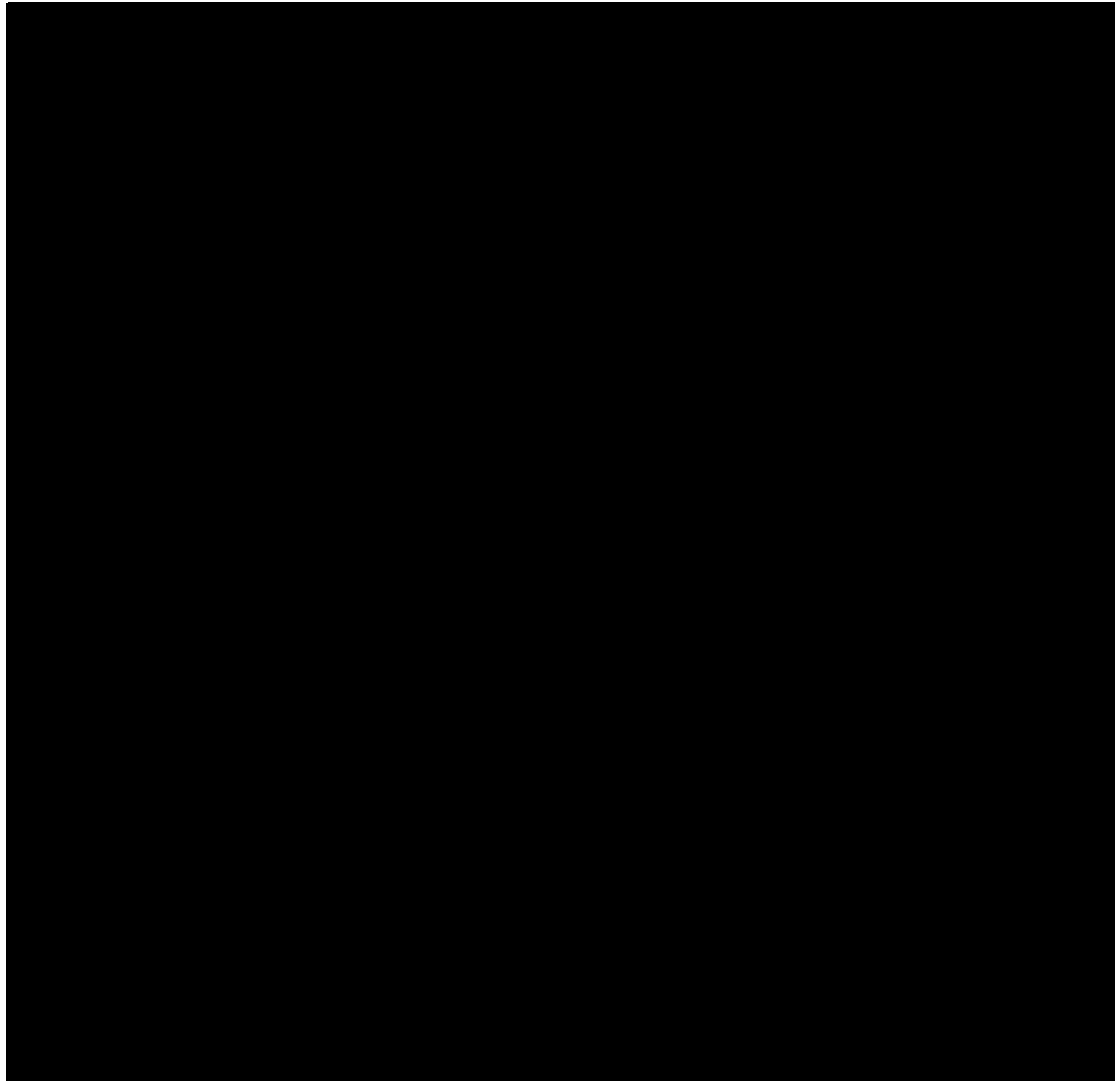
 shows Qwest's approach to ensure that services have a uniform view of network and support infrastructure.

Multiple overlay networks are no longer established to deliver new services. Value is shifted to network-based services, where Qwest becomes a solutions provider. Applications-based services are delivered independent of the network infrastructure. Excellent service quality is maintained during network convergence through the following practices:



- Consistent and rigorous technology management methodology that includes evaluation, selection and certification of network elements
- Accommodation of legacy services as the network evolves
- Network simplification through de-layering and introduction of multi- service access devices
- Coincident convergence of back-office systems, including introduction of a next generation Network Management Layer (NML) packet Operational Support System (OSS)

As shown in [REDACTED] the use of a converged MPLS core significantly eases the problems normally associated with backbone traffic engineering. Without a converged backbone, each services network (for example, one for Internet, one for private IP services, and one for voice) needs to be traffic-engineered independently. The normal state of affairs is that one network has too much capacity and another has performance limitations that require a backbone or router upgrade. The issue is that a carrier gets into a situation where the upgrade for one services network requires a large upgrade that is not cost effective. For example, the desired upgrade from OC-48c to OC-192c backbone circuits may require a complete nationwide upgrade that the carrier cannot afford, forcing them to settle for suboptimal performance regarding SLA fulfillment.





[Redacted content]

[REDACTED]

Qwest will evolve and improve overall quality of capabilities, service delivery and architectural requirements through continuous iteration. Converged capabilities will be simple to understand and easy to use. Qwest's success will be measured by the quality of the Agency experience.

**4.2.8.13 IP-PSTN Interoperability (L.34.1.4.6(m))**

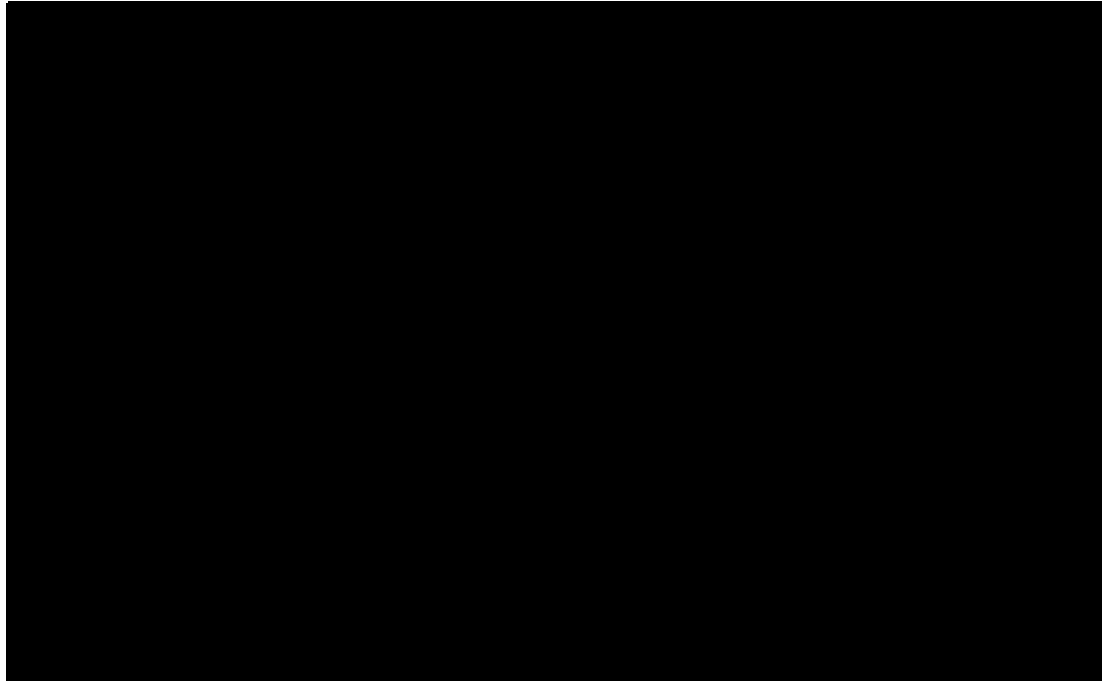
PBIP-VPN deployments are SED-oriented secure management services which are delivered over separately ordered IP transport and access services. Information on Qwest's approach to support and ensure interoperability between the IP networks and the PSTN is provided in Section 3.3.5.

**4.2.8.14 Approach for IPv4 to IPv6 Migration (L.34.1.4.6(n))**

Qwest is well positioned to migrate its network from IPv4 to IPv6.

[REDACTED]





**4.2.8.15 Satisfaction of NS/EP Requirements (L.34.1.4.6(o))**

Qwest uses a structured multi-layered approach to supporting National Security and Emergency Preparedness (NS/EP) that is designed to address each required function. Qwest has integrated risk management and security organizationally and strategically to encompass information technology and physical security. Our priorities are to protect our customers from the physical layer up through the entire Open Systems Interconnection (OSI) stack including all facets of cyber security.

Our approach ensures that Qwest complies with and provides priority for the Government's telecommunications requirements for NS/EP survivability, interoperability, and operational effectiveness during an emergency threat, whether caused by natural hazards, manmade disasters, infrastructure failures, or cyber events. Our approach consists of multiple levels of NS/EP support including the assignment of a full-time dedicated liaison, established TSP policies and procedures, implementation of the basic

NS/EP telecommunications functional requirements, and our robust redundant network architecture in the National Capital Region.

Specifically, in accordance with RFP Section C.5.2.2.1, *NS/EP Basic Functional Requirements Matrix for Network Services*, Qwest supports the following basic functional requirements for PBIP-VPNS.

- **Enhanced Priority Treatment (C.5.2.1(1))** - PBIP-VPNS supporting NS/EP missions are provided preferential treatment over all other traffic.
- **Secure Networks (C.5.2.1(2))** - PBIP-VPNS supporting NS/EP missions have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
- **Non-Traceability (C.5.2.1(3))** - PBIP-VPNS users are able to use NS/EP services without risk of usage being traced (that is, without risk of user or location being identified).
- **Restorability (C.5.2.1(4))** - Should a service disruption occur, PBIP-VPNS supporting NS/EP missions are capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.
- **International Connectivity (C.5.2.1(5))** – According to RFP section C.5.2.2.1, this requirement is not applicable to PBIP-VPNS.
- **Interoperability (C.5.2.1(6))** - PBIP-VPNS will interconnect and interoperate with other Government or private facilities, systems, and networks which will be identified after contract award.
- **Mobility (C.5.2.1(7))** – The PBIP-VPNS infrastructure supports transportable, re-deployable, or fully-mobile voice and data

communications (i.e., PCS, cellular, satellite, high frequency (HF) radio).

- **Nationwide Coverage** (C.5.2.1.(8)) - PBIP-VPNS is readily available to support the national security leadership and inter- and intra-Agency emergency operations, wherever they are located.
- **Survivability/Endurability** (C.5.2.1(9)) - PBIP-VPNS is robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or man-made disaster up to and including nuclear war.
- **Voice Band Service** (C.5.2.1(10)) – According to RFP Section C.5.2.2.1, this requirement is not applicable to PBIP-VPNS.
- **Broadband Service** (C.5.2.1(11)) – PBIP-VPNS will provide broadband service in support of NS/EP missions (e.g., video, imaging, Web access, multimedia).
- **Scaleable Bandwidth** (C.5.2.1(12)) – NS/EP users will be able to manage the capacity of PBIP-VPNS to support variable bandwidth requirements.
- **Affordability** (C.5.2.1(13)) - PBIP-VPNS leverages network capabilities to minimize cost (for example, use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).
- **Reliability/Availability** (C.5.2.1(14)) – PBIP-VPNS perform consistently and precisely according to their design requirements and specifications, and are usable with high confidence.

Details of how Qwest supports all 14 basic functional requirements listed in RFP Section C.5.2.2.1 are provided in Section 3.5.1, *Approach to Satisfy NS/EP Functional Requirements*, in this Technical Volume.

**4.2.8.16 Support for Signaling and Command Links (L.34.1.4.6(p))**

[Redacted content]

**4.2.8.17 Service Assurance in the National Capital Region (L.34.1.4.6(q))**

As discussed in Section 3.2, *Approach to Ensure Service Quality and Reliability*, Qwest provides network services in the National Capital Region (NCR) with a robust network architecture designed and engineered to ensure service continuity in the event of significant facility failures or catastrophic impact. Qwest will continue to engineer critical services to meet each Agency's requirements to eliminate potential single points of failure or overload conditions that may impact their network service performance.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Qwest also provides functionality that enables Government Emergency Telecommunications Service (GETS) priority calling mechanisms.

Qwest operates [REDACTED] and an extensive fiber infrastructure in the NCR to connect NCR customers. Qwest pre-subscribed this infrastructure from an ILEC and numerous competitive local providers CLECs. As presented in Section 3.2.2, *Arrangements with Other Service Providers for Carrying and Exchanging Traffic*, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] The use of CLECs, who provide infrastructure that is generally separate from the ILECs, gives another level of resiliency to the architecture because these services would not be affected by an ILEC facility failure.

**4.2.8.18 Approach for Satisfying Section 508 Requirements (L.34.1.4.6(r))**

According to RFP Section C.6.4, *Section 508 Provisions Applicable to Technical Requirements*, Section 508 provisions are not applicable to PBIP-VPNS. Qwest has fully described our approach to satisfying Section 508 requirements for applicable, offered services in Section 3.5.4, *Approach for Meeting Section 508 Provisions*, of this Technical Volume.

**4.2.8.19 PBIP-VPNS Impact on Network Architecture (L.34.1.4.6(s))**

PBIP-VPNS is a SED-based service and Qwest does not have to modify our network or service delivery to meet the requirements of this service.



**4.2.8.20 Optimizing the Engineering of PBIP-VPNS (L.34.1.4.6(t))**

Qwest's approach for optimizing the engineering PBIP-VPNS begins with the collection and analysis of network performance data. The results of the data are then compared to their respective AQL targets. If the AQL objectives are not met, then the Qwest engineers will review CPU utilization, memory usage, routing configurations and IPsec tunnel characteristics to determine potential areas of performance improvements. Resolutions might include coordinating with IPS service provider for changes to underlying network or MPLS routing, upgrading the SED with additional processing power or memory, migrating to alternate encryption algorithms, redesigning redundancy options, or adjusting time-to-live and other settings on the IPsec tunnels connecting Agency locations.

**4.2.8.21 Vision for Service Internetworking (L.34.1.4.6(u))**

Qwest's PBIP-VPNS solutions are transport- and access-agnostic. As such, Qwest can deliver encryption, IPsec tunnel management, and security controls over any IP-centric architecture. All that is required is that Qwest have a path to remotely manage the SED device and configuration parameters. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] This benefits Agencies where Continental U.S. (CONUS) and Outside Continental U.S. (OCONUS) locations might be served with different access or transport services. Since Qwest designed the PBIP-VPNS to work with different underlying providers, the NOC-interaction, escalation, and provisioning coordination processes are well documented, well understood, and time-tested over years of delivering PBIP-VPNS to Agencies.

#### **4.2.8.22 Support for Government PBIP-VPNS Traffic (L.34.1.4.6 (v))**

The Government traffic model does not specify any quantities for PBIP-VPNS. Today, Qwest's NOCs and Security Operations Centers (SOCs) support [REDACTED] locations delivering similar services, [REDACTED]. Currently these centers are architected to handle a significant expansion of service delivery without impact to service quality, robustness, or redundancy. We can easily expand our capacity for these services through the expansion of our operations teams and updates to software licenses.

#### **4.2.9 RESERVED**