4.1.8 PREMISES-BASED IP VPN SERVICES (PBIP-VPNS) (L.34.1.4)

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 1999. Qwest's PBIP-VPNS combines 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 [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.

Figure 4.1.8-1 provides an easy reference to correlate the narrative requirement to our proposal response.

Figure 4.1.8-1. Table of PBIP-VPNS Requirements

Req ID	RFP Section	RFP Requirement	Proposal Response
5814	C.2.7.2.3.1 (1)	Interface for Intranet and Extranet Premises-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	4.1.8.3.1.3

Req ID	RFP Section	RFP Requirement	Proposal Response
7850	C.2.7.2.3.2 (1)	Interface for Remote Access Premises-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	4.1.8.3.1.3
7849	C.2.7.2.3.2 (2)	Interface for Remote Access Premises-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 (See Note 1): Point-to-Point Protocol, Ipv4/v6	4.1.8.3.1.3
5810	C.2.7.2.3.2 (3)	Interface for Remote Access Premises-based IP VPNs UNI Type 3 Interface/Access Type: Cable high speed access Network-Side Interface: 320 kbps up to 10 Mbps Protocol Type (See Note 1): Point-to-Point Protocol, Ipv4/v6	4.1.8.3.1.3
5809	C.2.7.2.3.2 (4)	Interface for Remote Access Premises-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 Protocol Type (See Note 1)	4.1.8.3.1.3
5808	C.2.7.2.3.2 (5)	Interface for Remote Access Premises-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 Protocol Type (See Note 1)	4.1.8.3.1.3
5807	C.2.7.2.3.2 (6)	Interface for Remote Access Premises-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 Protocol Type (See Note 1)	4.1.8.3.1.3
5806	C.2.7.2.3.2 (7)	Interface for Remote Access Premises-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 (See Note 1): Point-to-Point Protocol, Ipv4/v6	4.1.8.3.1.3

4.1.8.1 Qwest's Technical Approach to PBIP-VPNS Delivery (L.34.1.4.1)

The Qwest technical approach to providing a fully compliant PBIP-VPNS is based on adherence to proven engineering practices and a standards-based, global IP network. The sections that follow describe our approach to service delivery and how our approach benefits Government Agencies. We will also describe how Qwest PBIP-VPNS will facilitate the Federal Enterprise Architecture (FEA) objectives, how Qwest proposes to address problems that may be encountered in providing PBIP-VPNS, and how our synchronization network architecture supports PBIP-VPNS.

Qwest PBIP-VPNS is available worldwide. As an industry leader[redacted] Qwest has extensive experience delivering secure networking solutions to educational institutions and governments at all levels[redacted]

4.1.8.1.1 Approach to PBIP-VPNS Delivery (L.34.1.4.1 (a))

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 SED devices 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-based 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. [redacted] The PBIP-VPN is transport and access agnostic; [redacted]

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 IPsec-based tunnels between Intranet, partner, and remote worker locations. [redacted] shows an example of a PBIP-VPNS solution spanning these three domains.

[redacted]

In most cases, secure routing is achieved through SEDs that operate as VPN gateways or encrypting devices. For small locations, Qwest-provided desk-top client SEDs delivering security and IPsec encryption features 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 or non-Qwest provided. [redacted]

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. [redacted]

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 required 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 4.1.8-3*** describes the approach for each solution type.

Figure 4.1.8-3 Description of Qwest's Approach to Networx PBIP-VPN Solution Types

Type	Solution	Description
Intranet	VPN gateway at Service Delivery Point (SDP)	VPN device provides routing and encryption between agency sites. The goal is to create a private, CUG between locations.
Extranet	VPN gateway at Partner location and SDP	PBIP-VPNs built between partner locations and Agency locations will be configured with a VPN gateway SED at each end point. These SEDs encrypt traffic between locations. The SDP edge gateway will also enforce security rules preventing unauthorized access from partner network locations.
Remote	VPN gateway or secure client	Qwest offers two alternatives: a secure desktop client appropriate for sites with one or two users, or a small office gateway which provides security enforcement and encryption via a gateway solution designed for broadband access.

4.1.8.1.2 Benefits of PBIP-VPNS Technical Approach (L.34.1.4.1 (b))

Qwest's technical approach to meeting the PBIP-VPNS requirements benefits Agencies through enhanced flexibility, including standard features which exceed requirements, worldwide coverage, seamless interoperability, and Qwest's Spirit of Service customer support. [redacted]

[redacted]

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

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

Qwest's proposed solution delivers additional benefits for Agencies aligned with overarching Federal Enterprise Architecture objectives as summarized below in ***Figure 4.1.8-5***.

Figure 4.1.8-5 Qwest's PBIP-VPNS Support to FEA Objectives

Federal Enterprise Objective	Benefits
Enhance cost savings and avoidance	Virtual Private Networking solutions exist to allow organizations to securely, productively, and economically communicate and collaborate between locations. The goal is to provide security controls, encryption of sensitive materials, and audit trails without excessively burdening cost or impacting network performance. Qwest believes that by offering flexible options on FIPS-compliant, standard-based technologies that can interoperate, we offer significant opportunities for cost savings and cost avoidance. One size does not have to fit all. Solutions can be selected from a broad menu for best fit by requirement and cost. Similarly, by delivering only on certified IPsec platforms, secure interoperability between Government organization, extranet partners, and remote users can be accomplished with minimal risk and investment.
Increase cross-agency and inter-government collaboration	Typical barriers to inter-government collaboration include mis-matched security devices between organizations, lack of verifiable risk documentation on interconnection, differing security requirements, and the most basic – no common network where connectivity between agencies could be established. IPsec-compliant devices, audited management practices, and a private MPLS network with hooks to the Internet via hardened gateways eliminate many of the original barriers. Qwest's proposed solution does not require that all access come from one provider – we expect different organizations will have multiple service providers. Qwest's proposed solution does not require identical SED configurations at all endpoints to be inter-networked – we expect each organization to select based on their cost/security requirements. Qwest's ability to commonly manage these diverse components and networks increases the possibilities for cross-agency and inter-government collaboration.

Federal Enterprise Objective	Benefits
Improve utilization of Government information resources to focus on core agency mission and service delivery to citizens by using the FEA	In addition to supporting mutliple SED types within a single Agency VPN, Qwest also engineers support for VPNs which combine many sites connected via NB-IPVN with PB-IPVPN extensions. Qwest provisioning builds IPsec tunnels between network and premise-based locations to meet Agency requirements for seemless and secure connectivity.

4.1.8.1.3 Solutions to PBIP-VPNS Problems (L.34.1.4.1(c))

Qwest has been delivering PBIP-VPNS since 1999. Since that time, we have developed a highly efficient, VPN-specific operations team experienced in solving common and complex problems. Qwest is the single point of contact (SPOC) for any troubleshooting and problem resolution. We will coordinate with site administrators at partner locations when debugging issues with extranet connectivity. PBIP-VPNS problems most commonly relate to:

- Issues establishing and maintaining IPsec tunnels between locations
- Regression testing when new locations are added
- Verifying that diversity options are functioning properly
- Adjusting security policies which are creating unexpected side effects.

Figure 4.1.8-6 summarizes typical problems and solutions Qwest expects to encounter when delivering PBIP-VPNS.

[redacted]

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

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

4.1.8.1.4 Synchronization Network Architecture (L.34.1.4.1 (d))

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

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

[redacted]

4.1.8.2 Satisfaction of PBIP-VPNS Performance Requirements (L.34.1.4.2)

Qwest will report on all required Key Performance Indicators (KPIs) and will meet all Acceptable Quality Levels (AQLs) for PBIP-VPNS components that we provide including SEDs, associated management and Internet Protocol Service (IPS)/transport. In cases where Qwest IPS is used as the transport solution for an Agency PBIP-VPNS, we will meet all requirements. In cases where another vendor's IPS is purchased by an Agency, Qwest will provide all reporting data needed to assist the Agency with managing their alternate transport provider to fulfill the service requirements. Additionally, when appropriately authorized by an Agency to act on their behalf, Qwest will actively manage all suppliers contributing to PBIP-VPNS performance to meet all AQLs.

4.1.8.2.1 PBIP-VPNS Quality of Service (L.34.1.4.2 (a))

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] Qwest will recommend upgrades when utilization thresholds are exceeded.

Qwest's PBIP-VPNS meets the latency requirements. Qwest meets or exceeds the time to restore AQL with and without dispatch service under the definitions outlined in Section 3.3.1.2.4, Fault Management (***Figure 4.1.8-9***).

[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]

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]

[redacted]

[redacted]

4.1.8.2.2 Approach for Monitoring and Measuring PBIP-VPNS KPIs and AQLs (L.34.1.4.2 (b))

[redacted]

[redacted]

For the PBIP-VPNS, all of the point-to-point AQL/KPI metrics listed in Figure 4.1.8-9 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 PBIP-VPNS SEDs via SNMP [redacted]. The PBIP-VPNS performance data information is distributed to Qwest's NOC. PBIP-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 Agency specified AQLs are met.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

- [redacted]

- [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

4.1.8.2.3 PBIP-VPNS Performance Improvements (L.34.1.4.2(c))

[redacted]

4.1.8.2.4 Additional PBIP-VPNS Performance Metrics (L.34.1.4.2(d))

[redacted]

4.1.8.3 Satisfaction of PBIP-VPNS Specifications (L.34.1.4.3)

Section 4.1.8.3.1 describes how Qwest's IP/MPLS network infrastructure enables a broad range of technical service capabilities and supports all of the technical capabilities, features and interfaces required for Networx PBIP-VPNS.

Section 4.1.8.3.2 discusses service enhancements. Qwest's homogeneous ATM/FR network represents a major service enhancement that Qwest already delivers to all of our customers. Qwest's Networx customers will benefit from the ability to connect lower and higher-volume locations cost-effectively through the already-integrated Qwest network. In addition, Qwest offers a diversity feature as an additional service enhancement, which provides a second, distinct custom-engineered Qwest ATM connection to the customer.

Section 4.1.8.3.3 provides a discussion of Qwest's network and service delivery approach which is already configured to support our Networx customers' ATM needs, reducing the Government's risk.

Section 4.1.8.3.4 presents a discussion of Qwest's long and successful experience in offering Frame Relay Service (FRS) and ATMs to commercial and Government clients, providing the Government with a low-risk solution to our FRS and ATMs requirements.

4.1.8.3.1 Satisfaction of PBIP-VPNS Requirements (L.34.1.4.3(a))

The following three sections describe how Qwest will satisfy the capabilities, features, and interfaces requirements of the RFP.

4.1.8.3.1.1 Satisfaction of PBIP-VPNS Capabilities Requirements (L.34.1.4.1(a), C.2.7.2.14)

Qwest satisfies all capability requirements for PBIP-VPNS as described in [redacted]. Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for

PBIP-VPNS. The text in Figure 4.1.8-12 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.

[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]

PBIP-VPNS Design and Engineering

To accommodate scalability and support for multiple applications, Qwest recommends a specified configuration based on individual requirements. [redacted]

[redacted]

[redacted]

[redacted]

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, multi-point 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. [redacted] outlines the process for adding a new site into the Agency's network.

[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]

[redacted]

[redacted]

It is typical practice for Intranet users to use private IP address space on their internal networks but to translate addresses to valid public IP addresses when accessing resources on the Internet or partner networks. This provides an additional level of security by not having a public routable path to private Agency resources. [redacted] shows a sample Network Address Translation (NAT) configuration that can be established by a Qwest administrator under Agency direction.

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]

[redacted]

[redacted]

[redacted]

[redacted]

Agency users will employ the secure Qwest Control Networx 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.

4.1.8.3.1.2 Satisfaction of PBIP-VPNS Feature Requirements (L.34.1.4.1(a), C.2.7.2.2)

Qwest satisfies all feature requirements for PBIP-VPNS as described in [redacted]. Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for PBIP-VPNS. The text in Figure 4.1.8-20 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.

[redacted]

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

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

4.1.8.3.1.3 Satisfaction of PBIP-VPNS Interface Requirements (L.34.1.4.1(a); C.2.7.2.3)

Qwest supports the required interfaces and protocol types with the SEDs identified in [redacted] (for Intranet and extranet applications) and [redacted] (for remote access applications). Over the contract length, hardware manufacturers may add/delete systems from their list of commercially supported devices. Qwest will 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 with the capability to support IPv6 when standard on carrier networks.

Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for PBIP-VPNS. The text in Figures 4.1.8-21 and 4.1.8-22 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.

[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]

Intranet and Extranet PBIP-VPNS UNI Type 1 (Req_ ID 5814; C.2.7.2.3.1 (1))

Qwest’s PBIP-VPNS solutions are access-agnostic and can be delivered on top of a wide range of Qwest and non-Qwest provided transport. 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 IPv6 when commercially available.

Interface for Remote Access PBIP-VPNS UNI Type 1 (Req_ ID 7850; C.2.7.2.3.2 (1))

Remote access VPNs over dial-up access will be supported via client installed software on the user desktop. The Qwest Remote Office Virtual Assistant (ROVA) client supports IPsec tunnel origination, personal firewall, and phonebook features. 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 Networx 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] provides an overview of remote access to our PBIP-VPNS.

[redacted]

While hardware-based solutions can be offered for dial-up locations, the client solution will be the most cost effective in the majority of 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 PBIP-VPNS UNI Type 2 (Req_ID 7849; C.2.7.2.3.2(2))

For DSL access up to 6 Mbps, Qwest offers two options: the client option previously described 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. Point-to-Point Protocol (PPP) is supported. Currently, Qwest supports IPv4 and will support IPv6 when commercially available.

Interface for Remote Access PBIP-VPNS UNI Type 3 (Req_ ID 5810; C.2.7.2.3.2(3))

For cable access up to 10 Mbps, Qwest offers two options: the client option previously described for 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 Cable termination device and the Qwest managed SED will be 10/100 Ethernet. [redacted] summarizes both DSL and cable remote access options. PPP is supported. Today, Qwest supports IPv4 and will support IPv6 when commercially available.

[redacted]

Interface for Remote Access Premises-based IP-VPNS UNI Type 4 (Req_ ID 5809; C.2.7.2.3.2(4))

IP-based VPN services on top of Multimode/Wireless LAN service will use the client model previously described for UNI Type 1. Today, Qwest supports IPv4 and will support IPv6 when commercially available. Qwest's Networx Multimode Wireless Network-Side option is described in Section 7.2 of Qwest's response.

Interface for Remote Access PBIP-VPNS UNI Type 5 (Req_ ID 5808; C.2.7.2.3.2(5))

IP-based VPN services on top of wireless access service will use the client model previously described for UNI Type 1. Today, Qwest supports IPv4 and will support IPv6 when commercially available.

Qwest is offering Broadband Dedicated Access Wireless service of speeds from DS-1 through DS-3. Broadband Wireless Access Arrangement (WLSAA) Service has been developed, implemented and managed using wireless point-to-point protocol-transparent (i.e., physical level) transmission connection between an SDP and the Qwest POP for Networx services (e.g., VS, NBIP-VPNS, and VTS). Qwest's Networx Wireless Access Network-Side option is described in Section 3.2.1.2.3 of Qwest's Technical Volume.

Interface for Remote Access PBIP-VPNS UNI Type 6 (Req_ ID 5807; C.2.7.2.3.2 (6))

Satellite access sites requiring VPN services would use a model similar to DSL and cable previously described. The existing devices terminating the satellite access would still be required. Network interfaces between the Qwest managed VPN device and satellite termination device would be 10/100 Ethernet. Today, Qwest supports IPv4 and will support IPv6 when commercially available.

[redacted]

Interface for Remote Access PBIP-VPNS UNI Type 7 (Req_ ID 5806; C.2.7.2.3.2(7))

ISDN access sites requiring VPN services will use a model similar to DSL and cable previously described. 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. Qwest supports IPv4 and will support IPv6 when commercially available. Qwest's Networx Circuit Switched Data Services (CSDS) Network-Side option is described in Section 4.1.2 of Qwest's response.

4.1.8.3.2 Proposed Enhancements for PBIP-VPNS (L.34.1.4.3(b))

Qwest's PBIP-VPNS offers additional capabilities not required in the RFP as standard components of the solution. Our offering provides additional flexibility in regard to vendors' support and the ability to support diverse service endpoints. Qwest understands that this flexibility is critical to serving the needs of a diverse user population. [redacted]

[redacted]

Qwest believes that a managed VPN solution should incorporate management, monitoring and administration of the transport network, the health and welfare of the edge devices, tunnel creation and security policy enforcement.

PBIP-VPNS is defined as management of secure IPsec tunnels between locations, extranet partner and Agency CUGs, and remote access users and Agency CUGs. [redacted]

[redacted]

[redacted]

4.1.8.3.3 Network Modifications Required for PBIP-VPNS Delivery (L.34.1.4.3(c))

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

4.1.8.3.4 Experience with PBIP-VPNS Delivery (L.34.1.4.3(d))

Since 1999, Qwest has focused on delivering secure wide area networking solutions to our customers. Qwest currently manages [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.

4.1.8.4 Robust Delivery of PBIP-VPNS (L.34.1.4)

Qwest has the sales engineering staff, vendor relationships, program management and operations support necessary to delivery PBIP-VPNS solutions to Agencies.

4.1.8.4.1 Support for Government PBIP-VPNS Traffic (L.34.1.4(a))

The Government traffic model does not specify any quantities for PBIP-VPNS. Today, Qwest's NOCs and Security Operations Center (SOC) support over [redacted] for similar services, operating at [redacted]. We can easily expand our capacity for these services through the expansion of our operations teams and updates to software licenses.

4.1.8.4.2 PBIP-VPNS Measures and Engineering Practices (L.34.1.4(b))

Qwest builds its network to provide high availability to its customers, ensuring that the Networx customer can grow easily and transparently in size and speed on the Qwest network. A PBIP-VPN consists of transport solutions connecting locations privately via MPLS or publicly via Internet and SED devices, which create IPsec tunnels and encrypt traffic between those locations. Qwest has built a management infrastructure to support a large number of Agency customers. Typically, the tools used are licensed by the number of customers or ports supported. [redacted]

Qwest dedicated a team of engineers to review, analyze, and recommend version and patch upgrades to SED devices and server infrastructure. Typically, this involves regression testing and vendor interaction to ensure that no upgraded deployment impacts existing functionality. In addition, Qwest's centralized engineering team applies a consistent capacity management model to all data services.

4.1.8.5 PBIP-VPNS Optimization and Interoperability (L.34.1.4.5)

Qwest closely monitors the AQLs for latency, packet loss and jitter and constantly optimizes the network. For VPN services, Qwest addresses additional optimizations specific to IPsec tunnel creation, selection of encryption standards, and port capacity at interconnect points.

4.1.8.5.1 Optimizing the Engineering of PBIP-VPNS (L.34.1.4.5(a))

Qwest's approach for optimizing the engineering of 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.

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

Qwest takes a proactive stance on network optimization; when the network architecture is optimized, it scales well and becomes easier to manage. Since PBIP-VPNS combine transport services with SED devices capable of encrypting data traversing the network between Agency locations, optimization typically involves examining the WAN architecture of the underlying transport network and verifying that the SED device is adequately configured to support required traffic levels.

The transport network and associated Agency CUG may be configured sub-optimally. This can occur as new sites are added to an architecture designed for a limited number of original locations. In these situations, Qwest traffic engineers work in conjunction with the Agency's IPS provider to verify that appropriate bandwidth exists between sites consistent with the measured traffic flows between locations. Qwest will recommend bandwidth upgrades in situations where that is the problem cause. Latency and other targets may be positively impacted by recommending re-grooming of circuits and establishing better routing paths between Agency sites.

Similarly, the SED devices may need upgrading as the number of sites or bandwidth increases at particular sites. Qwest SNMP monitors SED deployments and establishes thresholds that trigger trouble ticket activity when exceeded. [redacted]

4.1.8.5.3 Access Optimization for PBIP-VPNS (L.34.1.4.5(c))

[redacted]

[redacted]

4.1.8.5.4 Vision for PBIP-VPNS Internet working (L.34.1.4.5(d))

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] This benefits Agencies where CONUS and OCONUS locations might be served with different access or transport services. Since Qwest designed the PBIP-VPNS service 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-VPN services to Agencies.