

4.2.11 Converged IP Services (CIPS) (L34.1.4.6)

Qwest leads the telecommunications industry with our deployment of a converged network infrastructure. Networkx Converged IP Services are a natural extension of this proven IP-based platform.

Qwest provides Networkx Converged IP Services (CIPS) by directly leveraging our IP Service (IPS) transport and IP Telephony (IPTeLS) services. The Qwest converged platform, and any access approach, means that Qwest can provide CIPS using multiple network access methods, including complete Class of Service (CoS), secure access to the Internet, and access to an Agency’s intranet.

Qwest’s CIPS enables Agency-driven configurations and parameters including packet prioritization schemes, flexible IP addressing schemes, Web-based reporting and service configuring tools, dial plans, and call features. It also includes IP-enabled value-added services, Local Number Portability (LNP) and Enhanced 911 (E911) adherence, and a secure and hardened infrastructure protected against unauthorized access.

Figure 4.2.11-1 provides an easy reference to correlate the narrative requirements to our proposal response.

Figure 4.2.11-1. Table of CIPS Narrative Requirements

Req_ID	RFP Section	Proposal Response
32368	C.2.7.11.1.4 (2)	4.2.11.3.1
32371	C.2.7.11.1.4 (5)	4.2.11.3.1
32373	C.2.7.11.1.4 (6)	4.2.11.3.1
32377	C.2.7.11.1.4 (8)(b)	4.2.11.3.1
32390	C.2.7.11.1.4 (13)	4.2.11.3.1
32392	C.2.7.11.1.4 (14)	4.2.11.3.1
32393	C.2.7.11.1.4 (15)	4.2.11.3.1
32394	C.2.7.11.1.4 (15)	4.2.11.3.1
32395	C.2.7.11.1.4 (15)(a)	4.2.11.3.1
32396	C.2.7.11.1.4 (15)(b)	4.2.11.3.1
32397	C.2.7.11.1.4 (15)(c)	4.2.11.3.1
32398	C.2.7.11.1.4 (15)(d)	4.2.11.3.1

4.2.11.1 Reserved (L.34.1.4.6(a))

4.2.11.2 Reserved (L.34.1.4.6(b))

4.2.11.3 Satisfaction of CIPS Requirements (L.34.1.4.6(c))

The following three sections describe how Qwest will satisfy the capability, feature, and interface requirements of the RFP.

4.2.11.3.1 Satisfaction of CIPS Capabilities Requirements (L.34.1.4.6(c); C.2.7.11.1.4)

The underlying IP-based network for the CIPS enables access to our VoIP infrastructure and access to the Internet. The VoIP infrastructure also provides full access to the Public Switched Telephone Network (PSTN) for both originating and terminating traffic. Access to an Agency's intranet (based on Network Based IP Virtual Private Network Service (NBIP-VPNS), Premises Based IP-VPNS (PBIP-VPNS), Layer 2 VPNS (L2VPNS), Asynchronous Transfer Mode Service (ATMS), or Frame Relay Service (FRS)) is also enabled by the Qwest IP architecture.

Qwest's CIPS is based on a Qwest-owned and operated Tier 1 global Internet backbone. This backbone is the foundation to enable service convergence and enables additional preventative measures built into the core network. This infrastructure enables Qwest to fully support the Government's CIPS capabilities shown in **Figure 4.2.11-2**. Qwest fully complies with all mandatory stipulated and narrative capabilities requirements for CIPS. The text in Figure 4.2.11-2 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 4.2.11-2. Qwest's Technical Approach to CIPS Capabilities

ID #	Name of Capability	[Redacted]
1	Deliver data, video, and voice services	[Redacted]
2	Provide CoS or prioritization scheme	[Redacted]
3	Ensure priority of time-sensitive packets	[Redacted]
4 [Optional]	Agency determines prioritization of applications	[Redacted]
5	Gateways	[Redacted]
6	Network Capacity	[Redacted]
7	Dynamic IP Addressing	[Redacted]
8	Secure Website	[Redacted]

ID #	Name of Capability	[REDACTED]
		[REDACTED]
9	Minimum Voice Capabilities	[REDACTED]
10	Directory Assistance and Operator Services	[REDACTED]
11	Local Number Portability	[REDACTED]
12	SEDS	[REDACTED]
13	Compatible with Agency Active Directory services	[REDACTED]
14	Traverse Agency Firewalls	[REDACTED]
15	Security Practices and Safeguards	[REDACTED]

The following are specific narrative responses as required by the RFP.

Routing Prioritization Scheme (Req_ID 32368; C.2.7.11.1.4 (2))

Qwest's CIPS solutions provide a routing prioritization scheme (CoS) to distinguish between applications that require real-time (or high priority) treatment over near- or non-real-time applications. Qwest differentiates at points where the traffic flows through active NEs that have the capability to prioritize traffic routing. [REDACTED]

[REDACTED]. Both predetermined and customizable QoS templates are available to address Agency business needs.

[REDACTED]

[REDACTED] Qwest will work with Agencies to engineer their CoS design to ensure that the service meets application requirements.

[REDACTED]

[REDACTED] Agencies may select any of the queuing implementations on a per-port basis, restricted only by what options are available on the applicable access type for the port.

All queuing methods described are applied at the network egress router port (traffic leaving the Qwest network Provider Edge (PE) on the access line toward the Agency Customer Edge (CE) router). Therefore, the queuing prioritizes one or more types of Agency traffic over other types of traffic. Because it is applied at the port level, these mechanisms are not prioritizing Agency traffic over another customer's traffic and vice versa. All traffic that exceeds the speed of the Agency's port is buffered or discarded at the egress point in the network.

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[Redacted content]

[REDACTED]

Gateways for Protocol Conversion, CIPS interface and External Networks (Req_ID 32371; C.2.7.11.1.4(5))

The Qwest convergence solution provides the appropriate gateways from Qwest's CIPS to the Internet, Agency networks, and the PSTN. Layer 2 services such as Frame Relay, ATM, and Ethernet are used as access vehicles to Layer 3 services such as Layer 3 VPNs and IPS. These interconnections are implemented as distributed gateways that interconnect the Layer 2 access to the Layer 3 service. The distribution of the access gateways is determined based on support of SLAs and traffic requirements for the interconnections. The gateways provide interconnection between the Layer 2 and Layer 3 services, but no internetworking at the protocol level is required.

Qwest uses PSTN/IP gateways to interface with the PSTN network. Qwest employs [REDACTED] gateways for conversion between IP voice traffic and Time Division Multiplexing (TDM) voice traffic and [REDACTED] gateways to interface with the SS7 network. Qwest uses [REDACTED] Session Border

Controller (SBC) systems at the IP-to-IP network boundaries to manage traffic and convert protocols.

Network Capacity to Deliver CIPS (Req_ID 32373; C.2.7.11.1.4(6))

Qwest's OC-192 core network will assure adequate network capacity to deliver CIPS service for all Agencies. Qwest built our 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, and prepare for growth. Our design procedures, network modeling, and circuit route checks provide a high level of customer service.

[REDACTED]

A consistent capacity management model is applied by a centralized engineering team for all data services. Qwest establishes design rules for both edge and backbone NEs. Using these rules as a guide, we gather usage statistics to verify network status and take corrective action as necessary.

We have also addressed our approach to ensure robustness, resiliency, and optimum network configurations in Sections 4.2.11.20 and 4.2.11.22 for further information regarding the availability of adequate network capacity.

Utilization Statistics (Req_ID 32377; C.2.7.11.1.4 (8)(b))

Statistics will be available through the Qwest Control Networx Portal.

[REDACTED]

Active Directory Compatibility (Req_ID 32390; C.2.7.11.1.4 (13))

Qwest's CIPS is currently compatible with Agency-provided Active Directory (AD) services using Lightweight Directory Access Protocol (LDAP) to interface with the Qwest Control Network Portal. [REDACTED]

[REDACTED]

Agency Firewall Compatibility (Req_ID 32392; C.2.7.11.1.4 (14))

The Qwest Voice Implementation Team will work with the Agency at the time of Agency turn-up to ensure that an Agency's firewall is configured to interoperate with the Qwest CIPS. If any issues are detected by Qwest, we will work with the Agency to isolate them and will guide the Agency to the appropriate configuration.

Security Practices (Req_ID 32393; C.2.7.11.1.4 (15))

Qwest will ensure that security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access. Qwest conducts full compliance, performance, and robustness testing on NEs and services deployed in our network. Service provider best practices are followed for protection of the management, control, and data planes through the NEs. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] ACLs, rate limits, and firewall rules throughout our network restrict access to the individual NEs used in Qwest Hosted VoIP. DDoS detection is provided via our [REDACTED] DDoS detection system. Session Border Controllers (SBCs) are used to protect our VoIP network and customers from attacks and discovery. There are two types of SBCs in our core infrastructure: business SBCs and aggregation SBCs. The business subscriber's VoIP traffic is directed to a business SBC. The business SBC provides hosted Network Address Translation (NAT) traversal and partitions out rogue messages. The aggregation SBC resides between the business SBC and the [REDACTED] feature servers/IP unity servers. Additionally, the aggregation SBC resides between the public edge router and the [REDACTED] feature servers/IP unity servers. This boundary is used as a managed IP network Demilitarized Zone (DMZ).

Regular Audit and Update of Security Practices (Req_ID 32394;

C.2.7.11.1.4 (15))

Qwest will ensure that security practices and policies are updated and audited regularly. Qwest performs ongoing audit scans on production NEs. We have a mature process that includes regularly scheduled audits, a Configuration Management process, [REDACTED]

[REDACTED]

Qwest implements industry standard security to ensure data assurance, integrity, and confidentiality of customer and company information in support of our telecommunications services. These practices include implementing controls specifically in the areas of personnel, systems, and facility security. Qwest has also implemented comprehensive business continuity and disaster recovery measures and controls to ensure the availability of customer and corporate networks.

To ensure that the security architecture stays current with best practices, Qwest takes a lead role in developing standards, working with vendors, and implementing new, innovative approaches to improve our products including security services. Qwest maintains relationships with key network equipment vendors to provide a bi-directional dialog on best security practices and new feature development along with our membership and participation in a variety of industry and standards forums including:

- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]
- [REDACTED]

Additionally we provide a dedicated representative at the National Communications System's National Coordinating Center for Telecommunications.

Safeguards to Prevent Denial of Service Attacks (Req_ID 32395;

C.2.7.11.1.4 (15)(a)

Qwest will provide safeguards to prevent hackers, worms, or viruses from denying legitimate CIPS users and subscribers from accessing CIPS. Qwest also uses a combination of physical security, operational procedures, and logical separation of services to ensure the integrity of CIPS and prevent hackers, worms, or viruses from penetrating or spreading across NEs and degrading CIPS.

[Redacted content]

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

[REDACTED]

Safeguards to Mitigate Illegitimate CIPS Use (Req_ID 32396; C.2.7.11.1.4 (15)(b))

Qwest will provide safeguards to block attempts to illegitimately use CIPS. Qwest uses a combination of physical security, operational procedures, and logical separation of services to ensure the integrity of CIPS and prevent unauthorized intrusion.

[REDACTED]

Prevent Invasion of Privacy (Req_ID 32397; C.2.7.11.1.4 (15)(c))

The combination of physical security, operational procedures, and logical separation of services ensures the privacy of Agency CIPS traffic. Qwest ensures the privacy of customer CIPS traffic through security built into the design of the network and operational procedures that provide ongoing security. The network is physically and logically protected. Qwest facilities ensure physical security with the use of controlled access equipment rooms.

Qwest will ensure that the CIPS cannot be intercepted and unauthorized third parties cannot eavesdrop on the packet payloads through the use of encryption and message authentication. [REDACTED]

[REDACTED]

Encryption and Secure Tunneling at SBU Level (Req_ID 32398;

C.2.7.11.1.4 (15)(d))

Encryption and secure tunneling (VPN)—at the SBU through NSI levels available under Sections C.2.10 Security Services, C.2.7.2 Premises Based IP VPN Services, and C.2.7.3 Network Based IP VPN Services—is provided via the service. Qwest’s VPN products meet FIPS140 encryption requirements and therefore can be used for SBU traffic.

4.2.11.3.2 Satisfaction of CIPS Feature Requirements (L.34.1.4.2(a); C.2.7.11.2)

RFP C.2.7.11.2 contains no CIPS feature requirements.

4.2.11.3.3 Satisfaction of CIPS Interface Requirements (L.34.1.4.2(a); C.2.7.11.3)

Qwest CIPS User-to-Network Interface (UNI) types and their associated SEDs are shown below in **Figure 4.2.11-3**. Qwest may substitute these SEDs over the course of the Networkx program with SEDs of comparable functional and performance capabilities. Qwest fully complies with all mandatory stipulated and narrative interface requirements for CIPS. The text in Figure 4.2.11-3 provides the technical description required per L.34.1.4.2(a) and does not limit or caveat Qwest’s compliance in any way.

Figure 4.2.11-3. Qwest Provided CIPS Interfaces at the Service Delivery Point

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type	
1	All 802.3 cable and Connector types	10/100/1000 Mbps	IPv4 (v6 when and where available commercially from Qwest) over Ethernet	[Redacted]
2 [Optional]	All 802.3 cable and connector types	10 Gbps Ethernet	IPv4 (v6 when and where available commercially from the contractor) over Ethernet	[Redacted]

4.2.11.4 CIPS Quality of Service (L.34.1.4.6(d))

Qwest's CIPS solutions provide unparalleled support in the marketplace. Agencies can be assured of a service that will provide a reliable, virtually error-free data transport highway. Qwest meets the thresholds for all Acceptable Quality Levels (AQLs) with our CIPS solution. Qwest’s performance measurement methodology is fully compliant with the

Government's requirement. **Figure 4.2.11-4** summarizes our support for CIPS performance requirements.

Figure 4.2.11-4 Qwest's Compliance with Government CIPS Performance Metrics

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	
Latency	Routine	200 ms	≤ 200 ms	
Grade of Service (Packet Loss)	Routine	0.4%	≤ 0.4%	
Availability	Routine	99.6%	≥ 99.6%	
Jitter	Routine	10 ms	≤ 10 ms	
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	
	With Dispatch	8 hours	≤ 8 hours	

Qwest understands latency to be the average round-trip time for a packet to travel between source and destination Service Delivery Points (SDPs). [REDACTED]

Qwest understands Grade of Service (packet loss) to be the percentage of packets sent by the source SDP that never arrive at the destination SDP. [REDACTED]

[REDACTED] Qwest provides CoS to and from the SDP, but actual packet loss to an SDP is a function of the engineering design. Qwest sales engineering will work with each Agency to ensure end-to-end application performance.

Qwest understands availability to be the percentage of the total reporting interval time that CIPS is operationally available to an Agency. The transport layer for Qwest IP services is engineered for high availability.

Qwest's experience is that access issues make up the largest percentage of availability failures. Qwest measures availability from the Agency perspective, using [REDACTED] Trouble Management and Ticketing System (which includes auto-generated trouble ticketing) as the measure of a site's availability.

Qwest's VoIP component of CIPS is provided on multiple server and gateway platforms in geographically diverse data centers and Qwest POPs.

[REDACTED]

Qwest understands jitter to be the variation in the delay between received packets of an IP data stream from SDP-to-SDP. Jitter is typically the result of congestion. [REDACTED]

[REDACTED]

[REDACTED] The monitoring methods defined in Section 4.2.11.8 describe in detail how Qwest monitors the network to ensure that we meet the AQLs.

4.2.11.5 CIPS Performance Improvements (L.34.1.4.6(e))

[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 a CIPS solution to serve unique Agency needs. Qwest is able to leverage our vast CIPS product portfolio that includes a variety of SED

providers and specific CIPS solutions. Through a special combination of vendor solutions and engineering capabilities, Qwest will serve the Agencies' business needs.

4.2.11.6 Experience with CIPS Delivery (L.34.1.4.6(f))

Qwest is a proven provider for both voice and data/IP services and has long been a leader in IP network technology. Our robust fiber-based OC-192 network provides IP services to a number of Government Agencies. Qwest has demonstrated our industry leadership in several areas:

- First network service provider to deploy a fully-meshed OC-192 backbone
- MPLS Fast Re-Route for redundancy in the network
- Private Edge MPLS Frame Relay enabled
- On-net and off-net service level agreements

Additionally, Qwest has years of experience in VoIP technology and a converged environment. Qwest has been carrying large portions of our long distance traffic over IP [REDACTED] since [REDACTED]. This has enabled Qwest to provide a more cost-effective and reliable long distance service. Qwest's proven leadership in voice and emerging voice solutions such as VoIP is demonstrated by the following:

- Experienced with VoIP since [REDACTED] and currently running more than [REDACTED] on our VoIP platform
- Deployment of [REDACTED] gateways
- Proven provider for long distance service
- Proven provider for local service
- Proven provider of hosted applications

In addition to the Qwest IP/MPLS network strategy to support CIPS, Qwest brings proven experience in the voice space. The existing Qwest voice

network is the result of an evolution of the traditional TDM based networks. Qwest has deployed a world class Inter-Exchange Carrier (IXC) network

[REDACTED]

[REDACTED]

[REDACTED] Qwest's experience with the TDM-based networks in addition to our expertise in data/IP networks has uniquely positioned us to offer VoIP-based services to Agencies. Qwest has added key network components/elements to our network architecture with the goal of providing and enabling IP-based voice solutions as part of a converged solution set. Qwest's VoIP solution includes call routing, call features, IP-enabled features/functionalities, and IP-enabled messaging capabilities.

Qwest's IP services solutions have supported Federal, commercial, and educational enterprises for more than [REDACTED]. Qwest expertly manages IPS narrowband, broadband, satellite, Integrated Services Digital Network (ISDN), and Wireless Fidelity (WiFi) access services, delivered by industry-leading suppliers such as Covad for nationwide Digital Subscriber Line (DSL) service and iPass for WiFi Internet access. Qwest's dedicated IP access service currently includes [REDACTED] public and private peering globally, including geographically distributed private peering with all top U.S. and Canadian networks. [REDACTED]

[REDACTED]

[REDACTED]

Qwest provides IP transport services to a majority of the Fortune 500 U.S.-based businesses and continues to exceed industry performance measurements for service, features, and availability. Qwest presently supports [REDACTED] dedicated IP access connections originating from Qwest's OC-192 IP MPLS Network. Qwest's 14-state DSL services coverage


supports corporate, Government, and educational institutions. [REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]

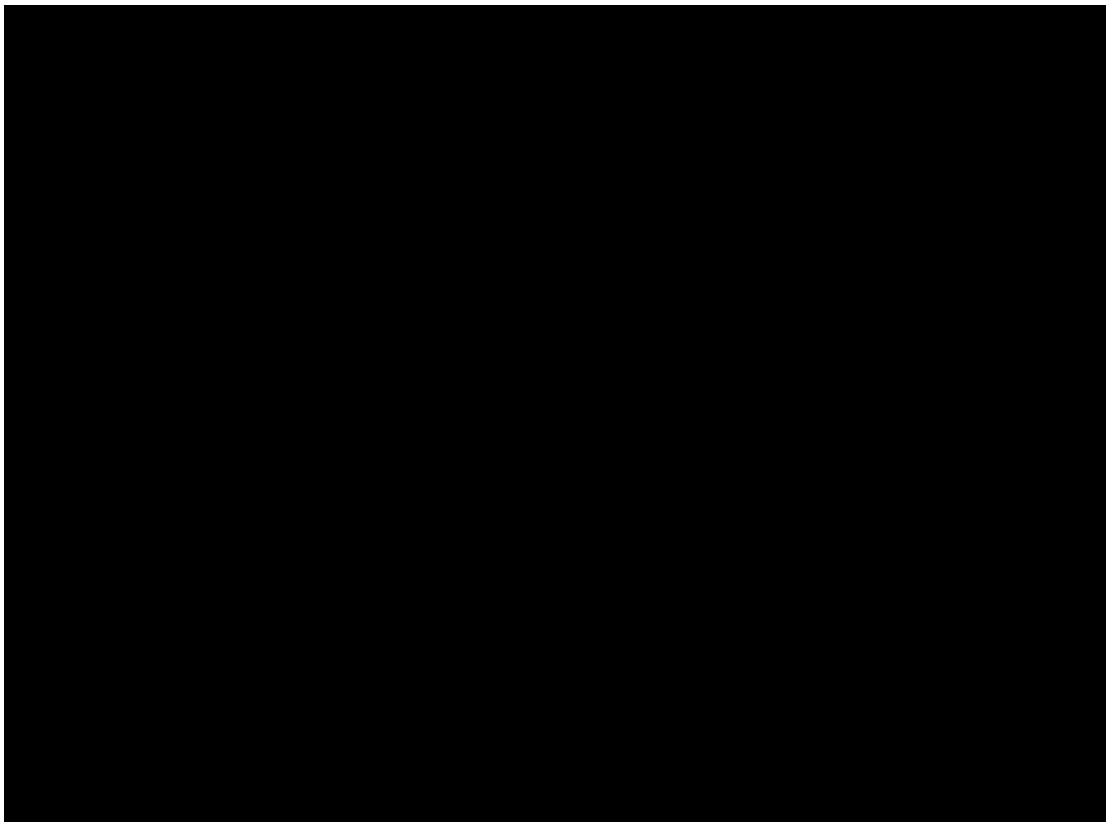
**4.2.11.7 Characteristics and Performance of Access Arrangements
(L.34.1.4.6(g))**

For the majority of Networkx services, SDP-to-SDP, service quality depends on the facilities of more than one provider. Qwest realizes that a key factor to our success on the Networkx program is the ability to manage access arrangements from Agency locations to our core network through both the traditional Incumbent Local Exchange Carriers (ILECs) and the growing diversity of Competitive Local Exchange Carriers (CLECs). As the only service provider to have successfully merged the operational aspects of an ILEC with a long distance company, Qwest can uniquely provide robust access solutions to meet our customers' needs. Qwest will apply the same discipline and approach that is used to maintain our own facilities-based portions of the service to provide end-to-end delivery of Networkx services to the Agencies.

Our customer-focused approach to delivering communications services results in [REDACTED] SDP-to-SDP service availability for Agencies. We also have the staff and procedures to engineer extremely high-availability access arrangements. For diversely connected customers, our services average more [REDACTED]
[REDACTED] our operational procedures have also enabled a Time to Restore (TTR) of less than [REDACTED] for our Government data networking customers.

A key aspect of access service involves the provisioning interval from order entry to generation of the Service Order Completion Notice. Qwest has leveraged our experience with Integrated Optical and Electrical Circuits technology and our experience as a Federal provider to build a long and excellent track record in on-time delivery service with reliable service delivery intervals.

As shown in  Qwest has maintained an excellent service delivery interval for Agencies. Figure 4.2.11-5 represents actual service turn-up from the customer's perspective—including all aspects of access, provisioning, demarcation extension, and equipment installation for a major Government department nationwide network.



Our provisioning performance has direct benefits to Agencies as it enables aggressive timelines for service transition. Effective transition allows Agencies to take advantage of next-generation services to achieve higher operational efficiency and lower unit costs. [REDACTED]

[REDACTED]

To provide access services, Qwest has a broad variety of agreements with local carriers to ensure flexibility, quality, and reliability. Qwest has strict quality standards for how we connect with other carriers to maintain this high level of performance. Section 3.2.1 provides further detail regarding our approach to dedicated Frame Relay and alternate access methods to support Networkx services.

4.2.11.8 Approach for Monitoring and Measuring CIPS KPIs and AQLs (L.34.1.4.6(h))

Qwest monitors and measures the KPIs and Acceptable Quality Levels (AQLs) using automated processes that pull data from the root source, summarize it, and provide a web-based display of the results. These Web tools display actual results and provide a color-coded visual indicating whether performance goals have been achieved. Our approach is to completely automate the Web display of results from data collection. This ensures that the focus is on responding to performance issues, rather than on performance report generation. The automated reporting process eliminates any question of manipulating the performance data.

Measuring SDP-to-SDP Latency, Packet Loss and Jitter, and the Role of SEDs

All of Qwest's IP-based services are provided over the same IP services infrastructure. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[Redacted content]

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

[Redacted content]

[Redacted text]

The Use of Government Furnished Property

[Redacted text]

4.2.11.9 CIPS Support of Time-Sensitive Traffic (L.34.1.4.6(i))

Qwest's CIPS solution ensures the quality of time-sensitive traffic through the combination of our network access architecture and our CoS


attributes. Our network access architecture and CoS capabilities (with four classes of service) provide converged IP services that include data, video, and voice. The Qwest SEDs for CIPS are also CoS aware to ensure the proper prioritization of traffic entering the Qwest network.

Qwest can ensure that time-sensitive IP packets are assigned a strictly higher priority than other traffic. This is accomplished by the proper selection and configuration of SEDs as well as the proper configuration of CoS templates for the Qwest IP ports associated with CIPS access. Qwest sales engineering will work with an Agency to design a CoS plan that meets application requirements.

4.2.11.10 CIPS Support for Integrated Access (L.34.1.4.6(j))

Qwest's network architecture and services already integrate several access methods, including:

- Dedicated access (Layer 1) using both domestic and international transitional TDM
- Frame Relay (FR), ATM, and xDSL access (Layer 2) via regional and international ATM/FR and ILEC/CLEC xDSL
- Ethernet integrated access (Layer 2) through Qwest, ILEC, and CLEC

 summarizes our integrated access approach.



Qwest engineers each of these access methods to deliver the data quality necessary to support the integration of voice, video, and data. Equally important, we match the access methods to the Qwest network architecture with the appropriate data service network, enabling technologies (i.e., ATM, FR, and MPLS/IP VPNs) and CoS/QoS mechanisms to enable real multimedia performance for Agencies. In all instances Qwest takes complete end-to-end responsibility for the planning, engineering, provisioning, monitoring, and trouble management of Network services from SDP to SDP.

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

Qwest complies with IETF, International Telecommunications Union, Telcordia, American National Standards Institute (ANSI), and all applicable industry, national, and international standards. Qwest is actively working with the standards bodies and holds the Technology and Operations chair position

in ATIS, an ANSI-accredited standards organization. Qwest's network is built on standards-based technologies, enables a building block approach to evolution, and supports the access methods required by the Government.

Qwest's converged access solutions provide unparalleled support in the marketplace. Agencies can be assured of an integrated access solution that will provide a reliable, virtually error-free data transport highway no matter what telephony, IP, or data services are used.

**4.2.11.11 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, Qwest evaluates new products and technologies for incorporation into the Qwest network in partnership with Qwest Product Management.

[REDACTED]

[REDACTED]

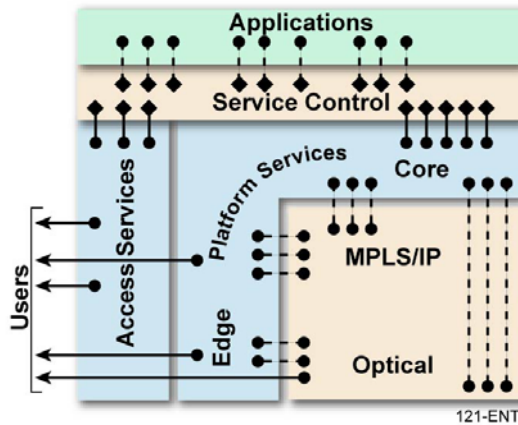
[REDACTED]

[REDACTED]

4.2.11.12 Approach for Network Convergence (L.34.1.4.6(I))

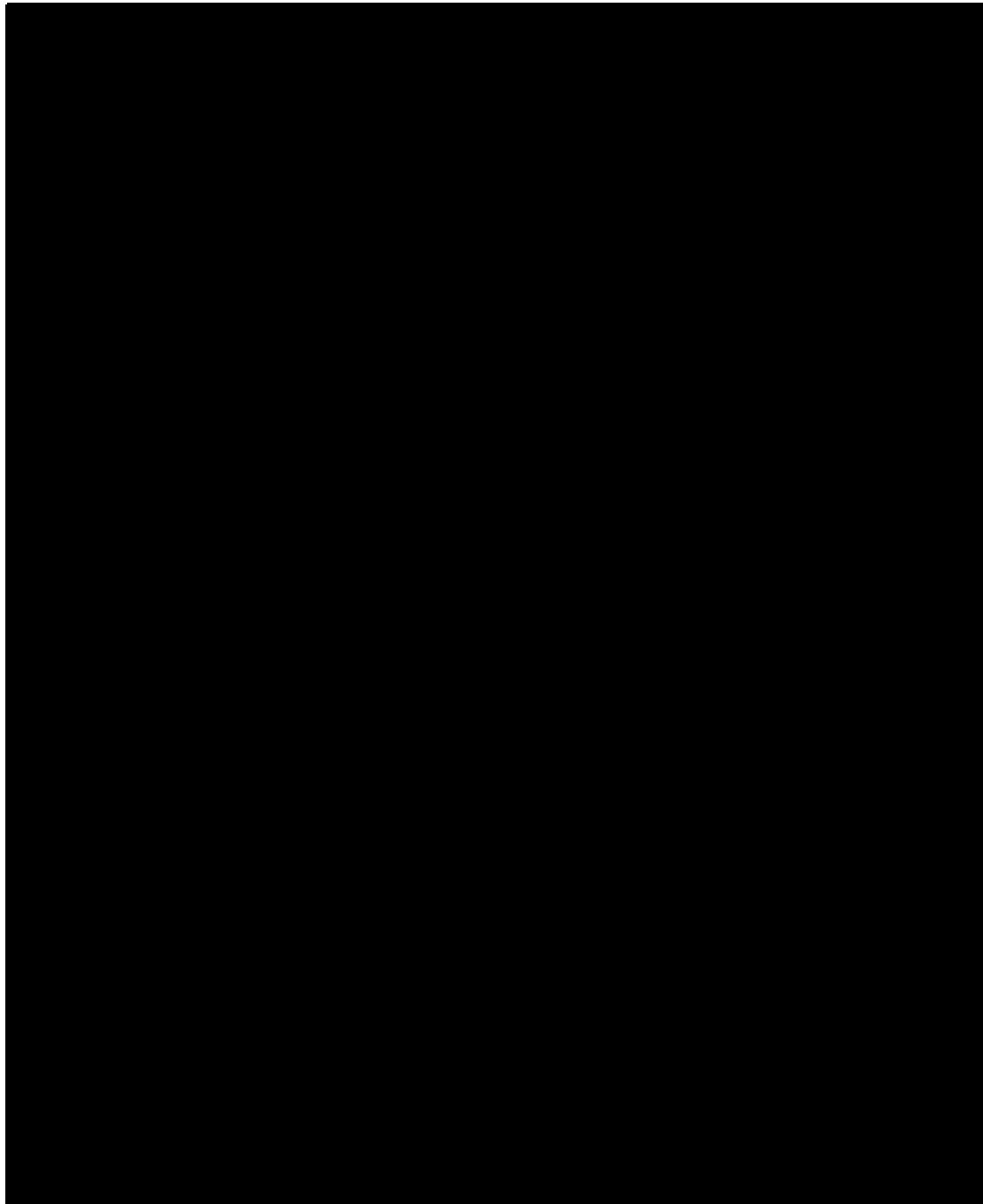
Qwest is committed to the elimination of single-purpose, stovepipe networks that create planning, operations, and interoperability issues for our customers. Qwest's service delivery model supports multiple types of customer requirements. [REDACTED]

Figure 4.2.11-8. Qwest Services Delivery Model. *Qwest's services delivery model is our established guide for technology evolution, convergence, and service interoperability.*



[REDACTED]

[REDACTED]



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

[REDACTED]

4.2.11.13 IP-PSTN Interoperability (L.34.1.4.6(m))

Qwest is a proven provider for both voice and data/IP services and has long been a leader in IP network technology. Our robust fiber-based OC-192 network provides IP and MPLS services to a number of Government customers. Qwest's IP/MPLS network was built as a fully-meshed OC-192 backbone with MPLS fast re-route for redundancy in the network and with private edge MPLS Frame Relay enabled.

In addition to the Qwest IP/MPLS network strategy to support convergence, Qwest brings proven experience in the voice space. The existing Qwest voice network is the result of an evolution of the traditional TDM-based networks. [REDACTED]

[REDACTED] This network leverages [REDACTED] [REDACTED] to offer services. Qwest's experience with the TDM-based networks in addition to our expertise in data/IP networks has

uniquely positioned us to offer VoIP-based services to our customers. Qwest has added key network components/elements to our network architecture with the goal of providing and enabling IP-based voice solutions as part of a converged solution set. [REDACTED]

Utilizing the Qwest IP/MPLS network in addition to our voice infrastructure, Qwest has been carrying large portions of our long distance traffic over IP since [REDACTED]. This has enabled Qwest to demonstrate the interoperability of our IP/MPLS network with the PSTN and to provide [REDACTED] more reliable long distance service to the customer [REDACTED]

[REDACTED]

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

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

[Redacted text block]

[Redacted text block]

[REDACTED]

[REDACTED]

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

Qwest uses a structured multi-layered approach to supporting NS/EP that is designed to address each required function. Qwest has organizationally and strategically integrated risk management and security 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 Telecommunications Service Priority (TSP) policies and procedures, implementation of the basic NS/EP telecommunications functional requirements, and our robust redundant network architecture in the National Capital Region (NCR).

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

- **Enhanced Priority Treatment** (C.5.2.1(1)) – CIPS supporting NS/EP missions are provided preferential treatment over all other traffic.
- **Secure Networks** (C.5.2.1(2)) – CIPS 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)) – CIPS 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, CIPS 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 CIPS.

- **Interoperability** (C.5.2.1(6)) – CIPS 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 CIPS infrastructure supports transportable, re-deployable, or fully mobile voice and data communications (i.e., Personal Communications Service, cellular, satellite, high frequency radio).
- **Nationwide Coverage** (C.5.2.1(8)) – CIPS 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)) – CIPS 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 CIPS.
- **Broadband Service** (C.5.2.1(11)) – CIPS 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 CIPS to support variable bandwidth requirements.
- **Affordability** (C.5.2.1(13)) – CIPS leverages network capabilities to minimize cost (for example, use of existing infrastructure, commercial-off-the-shelf technologies, and services).

- **Reliability/Availability** (C.5.2.1(14)) – CIPS 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.

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

[Redacted content]

**4.2.11.17 Service Assurance in the National Capital Region
(L34.1.4.1(q))**

As discussed in Section 3.2, *Approach to Ensure Service Quality and Reliability*, Qwest provides network services in the 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.

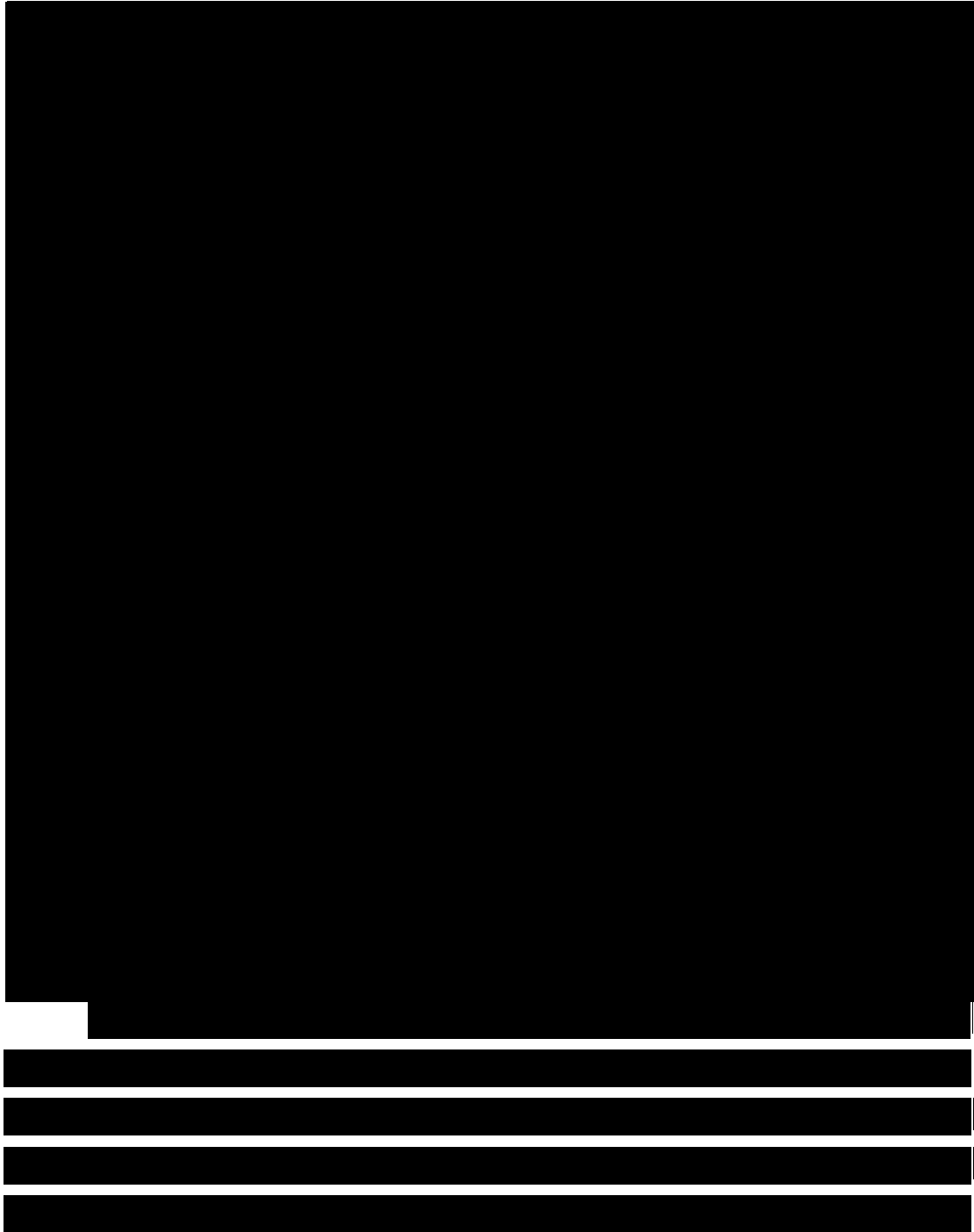
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED] Qwest also provides functionality that enables Government Emergency Telecommunications Service (GETS) priority calling mechanisms.

Qwest will provide full NS/EP Functional Requirements Implementation Plan (FRIP) documentation upon contract award when requested to proceed with plan delivery. Qwest will update plans, including Part B, addressing our strategy for supporting Agency NCR requirements in accordance with RFP Section C.7.16.

Qwest understands the Government's requirement to assure performance of network services in and around the NCR. Qwest has POP diversity [REDACTED]
[REDACTED] these gateways provides complete redundancy to access Qwest nationwide and international network capabilities as well as regional voice and data services. [REDACTED]

[REDACTED]
[REDACTED]

[REDACTED] shows the logical configuration of the major transport facilities as well as the services provided at each POP.



[REDACTED]

[REDACTED]

[REDACTED] This configuration enables these three locations to participate in the routing of access and backbone traffic, providing significant load-balancing and reconfiguration options in the event of a switch, router, or even a complete POP failure.

Qwest has recently acquired OnFiber, a metro SONET and Ethernet provider with yet another diverse network in the NCR. This gives Qwest at least [REDACTED] fiber optic networks to use to ensure redundancy and survivability in the greater Washington D.C. area. In effect, this means that Qwest can completely avoid Washington, D.C. to continue to provide services in an emergency.

Qwest operates seven other major SONET rings and an extensive fiber infrastructure in the NCR to connect NCR customers. Qwest pre-subscribed this infrastructure from an ILEC and numerous CLECs. As presented in Section 3.2.2, *Arrangements with Other Service Providers for Carrying and Exchanging Traffic*, Qwest connects to several major ILEC POP locations through SONET-ring protected networks to ensure multiple access paths to ILECs' services including voice termination and fiber access. 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.

[REDACTED]

[REDACTED] This ensures that Qwest can hand off traffic to at least one access tandem in the event of a complete Qwest POP failure. Qwest supports dual-homing arrangement for call overflow or load balancing between two or more diverse voice switch locations. Using Qwest diverse access infrastructure, this affords the maximum protection for an Agency in the event of the loss of a switch or transport system failure. In Section 3.2.3, *Congestion Flow Strategies, Control, and Redundancy*, Qwest demonstrates how network planning examines all failure modes and determines network capacity and switch or router redundancy placement to ensure performance during failures.

The route-diverse SONET backbone and access networks that service the NCR enable the transport of services to any Qwest POP nationwide [REDACTED]

[REDACTED]

[REDACTED] As with voice services, critical Qwest customers can be dual-homed to ensure extremely high availability of their data services—again protected from any single point of failure in the NCR.

[REDACTED]

[REDACTED] Qwest peers with the largest ISPs at [REDACTED] private peering locations geographically distributed throughout the United States, and the loss of a single peering point has virtually no effect on our ability to provide high-quality access to the Internet. Qwest also peers directly in Asia and Europe to improve international peering performance. In total, Qwest can dual-home critical customer connections with complete route diversity to all of Qwest's

data networking services to have complete resiliency from facility failures in the NCR.

To ensure 50 to 100 millisecond range service restoration in the event of a catastrophic backbone circuit or router failure, Qwest's IP-based MPLS fast-forwarding core design uses Fast Re-Route (FRR), which provides pre-provisioned multi-path healing for all Qwest IP services.

Qwest will address the strategy, technical systems and administration, management, and operation requirements for the NCR in Part B of our NS/EP FRIP (a draft appears as Appendix 2 to the Technical Volume).


**4.2.11.18 Approach to Satisfying Section 508 Requirements
(L.34.1.4.6(r))**

Qwest's approach to meeting Section 508 criteria includes a range of activities to ensure that all users are able to access all services offered through the Networx contract vehicle.

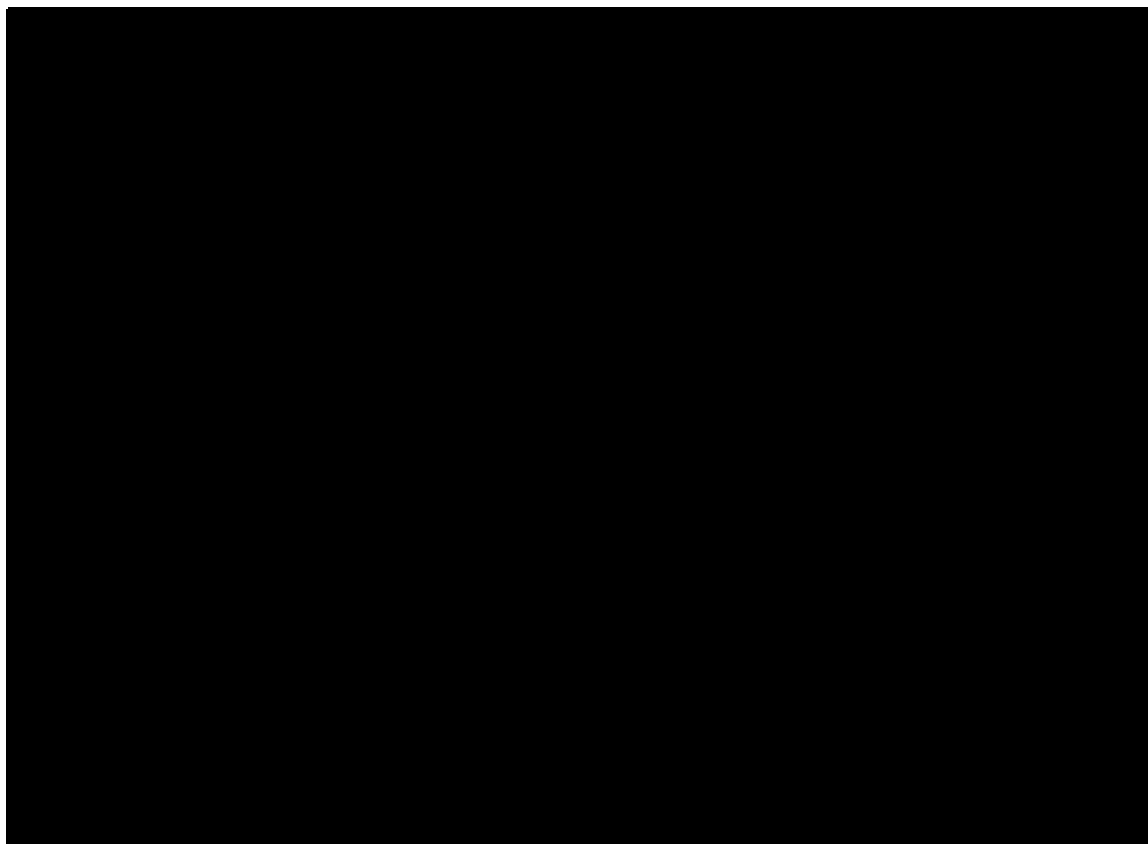
Qwest achieves compliance by performing the same rigorous testing and evaluation processes that all products and services go through before they are made available to the public. To ensure that products and services are 508 compliant, Qwest continues tests and evaluations with industry and specific Assistive Technology (AT) vendors to assess interoperability with text telephones (TTY) and AT devices.

Qwest has enlisted a single toll-free number for 24x7x365 access, 1-866-GSA-NETWorx (1-866-472-6389), that will provide Agencies with direct access to our Customer Support Office, which will also be 508 compliant, enabling access by email, fax, TTY, telecommunications display devices, text messaging, or other methods as required. Qwest customer service support will be accessible around the clock for all Agency users, wherever they may be located. To ensure this, the Qwest Control Networx Portal, the gateway to Qwest Networx support systems, will also be 508 compliant. This Portal will

serve as the primary conduit for daily status pertaining to ongoing projects and other service delivery activities for Agencies.

As part of Qwest's Networx deliverables,  lists the voluntary product accessibility templates (VPATs) developed for each offered product and service applicable for Networx services as required. The VPATs, including the relevant provisions of Subparts B, C, and D listed below in Figure 4.2.11-13, are included in the Technical Volume Appendices.

- 1194.21 Software Applications and Operating Systems
- 1194.22 Web-based Internet Information and Applications
- 1194.23 Telecommunications Products
- 1194.31 Functional Performance Criteria
- 1194.41 Information, Documentation, and Support



The following steps describe Qwest's approach for maintaining compliance with Section 508. Our approach for 508 compliance starts at lifecycle initiation and flows through transition, testing, and operations.

Step 1 – Discovery and Scoping

Step 2 – Publish Design Guidelines

Step 3 – Ensure Future Releases are Compliant

More information about how Qwest will maintain 508 compliance is in Section 3.5.4, *Approach for Meeting Section 508 Provisions*, of this Technical Volume.

4.2.11.19 CIPS Impact on Network Architecture (L.34.1.4.6(s))

We do not expect the delivery of CIPS to have any impact on our already-converged architecture.

4.2.11.20 Optimizing the Engineering of CIPS (L.34.1.4.6(t))

Qwest closely monitors the KPIs 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 such as availability, packet delivery rate, delay, and jitter. These data, along with historical growth rates, are input into network simulation models. The simulation results are compared to AQL targets. Based on the results, the Qwest engineers perform additional analyses and take steps to reroute traffic or add network resources as necessary to maintain AQLs.

[REDACTED]

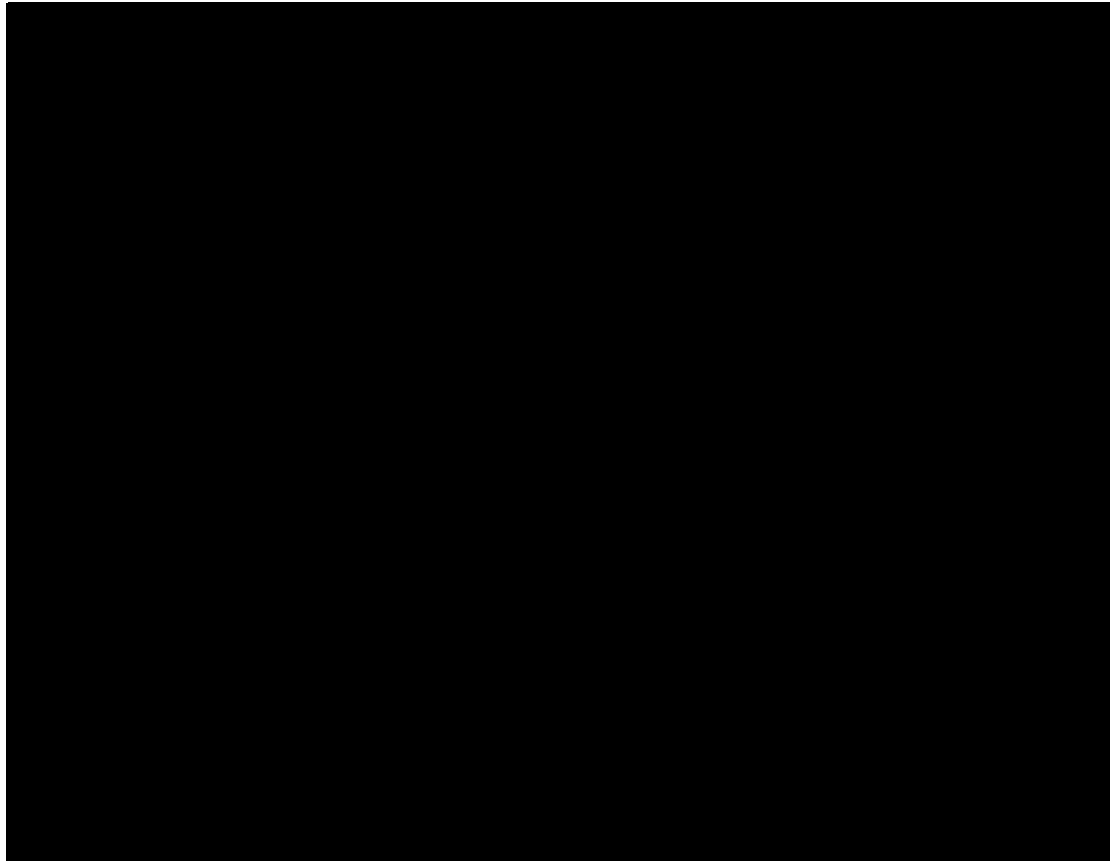
4.2.11.21 Vision for Service Internetworking (L.34.1.4.6(u))

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. The service delivery model allows us to assess interoperability impacts of service layer changes. At the core of Qwest IP-centric approach are the optical transport and IP/MPLS networks. The service delivery model gives Qwest a guide of how to layer from the core resources to edge services, integrated services control layers, and access all the way to the SDP at the Agency location. It is this layered approach that enables users to request both network resources, such as bandwidth, and application resources, such as call control, security services, messaging, and conferencing. Additional detail can be found above in Section 4.2.11.12, *Approach for Network Convergence*.

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]

[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.

Network convergence not only allows Qwest to eliminate multiple physical network overlays, it also eliminates separate control planes. For example, legacy control protocols such as Private Network-to-Network Interface and Spanning Tree Protocol are no longer required to provision and manage standalone L2 services. Common, unified IP/MPLS signaling and routing protocols will be used to provision and manage L2 and L3 VPN services, greatly simplifying the overall network architecture.

[Redacted text block]

[Redacted text block]

[Redacted text block]

4.2.11.22 Support for Government CIPS Traffic (L.34.1.4.6(v))

Converged services deployed over existing Qwest networks inherit the robust and extensible design of each underlying network. In addition, systems

and procedures are in place to provide seamless integration and to ensure that the overall integrated service is provided in a highly available, high performance manner.

Qwest will use our robust, state-of-the-art IP networking platform and VoIP platform to provide CIPS. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Qwest will easily absorb the projected traffic onto our existing service infrastructure.