4.1.12 Converged IP Services *(L.34.1.4)*

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

Qwest provides Networx Converged IP Services (CIPS) by directly leveraging Internet Protocol Service (IPS) transport and our Voice over Internet Protocol (VoIP) 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 Internet Protocol (IP)-enabled value-added services, Local Number Portability (LNP) and E911 adherence, and a secure and hardened infrastructure protected against unauthorized access.

Figure 4.1.12-1 provides an easy reference to correlate the narrative requirement to our proposal response.

Figure 4.1.12-1. Table of CIPS Narrative Requirements

Req_ ID	RFP Section	RFP Requirement	Proposal Response
5086	C.2.7.11 .1.3	The contractor shall provide CIPS for domestic locations and it is optional for non-domestic locations.	4.1.12.1.1
5082	C.2.7.11 .1.4 (2)	The following Converged IP Services capabilities are mandatory unless marked optional. 2. The contractor shall provide a routing prioritization scheme or class of service to distinguish between applications that require real-time (or high priority) treatment over near, or non real-time applications.	4.1.12.3.1.1
5078	C.2.7.11 .1.4 (5)	The following Converged IP Services capabilities are mandatory unless marked optional. 5. The contractor shall provide gateways and/or service enabling devices, where required, (a) for protocol conversions, (b) to interface with the contractor's CIPS network or (c) for access to external networks.	4.1.12.3.1.1
5076	C.2.7.11 .1.4 (6)	The following Converged IP Services capabilities are mandatory unless marked optional. 6. The contractor shall ensure adequate network capacity to	4.1.12.3.1.1

Req_ ID	RFP Section	RFP Requirement	Proposal Response
		deliver CIPS service for the subscr bing Agency.	
5072	C.2.7.11 .1.4 (8)(b)	The following Converged IP Services capabilities are mandatory unless marked optional. This shall include but is not limited to: b. Utilization statistics	4.1.12.3.1.1
5058	C.2.7.11 .1.4 (13)	The following Converged IP Services capabilities are mandatory unless marked optional. 13. The contractor's CIPS shall be compat ble and interoperate with Agency provided Active Directory services.	4.1.12.3.1.1
5055	C.2.7.11 .1.4 (14)	The following Converged IP Services capabilities are mandatory unless marked optional. 14. The contractor shall verify with the Agency that the Agency firewall is compatible with this service.	4.1.12.3.1.1
5054	C.2.7.11 .1.4 (15)	The following Converged IP Services capabilities are mandatory unless marked optional. 15. The contractor shall ensure security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access.	4.1.12.3.1.1
5053	C.2.7.11 .1.4 (15)	The following Converged IP Services capabilities are mandatory unless marked optional. 15. The contractor shall ensure security practices and policies are updated and audited regularly.	4.1.12.3.1.1
5052	C.2.7.11 .1.4 (15)(a)	The following Converged IP Services capabilities are mandatory unless marked optional. a. Denial of service - The contractor shall provide safeguards to prevent hackers, worms, or viruses from denying legitimate CIPS users and subscribers from accessing CIPS.	4.1.12.3.1.1
5051	C.2.7.11 .1.4 (15)(b)	The following Converged IP Services capabilities are mandatory unless marked optional. b. Intrusion - The contractor shall provide safeguards to mitigate attempts to illegitimately use CIPS service.	4.1.12.3.1.1
5050	C.2.7.11 .1.4 (15)(c)	The following Converged IP Services capabilities are mandatory unless marked optional. c. Invasion of Privacy - The contractor shall ensure CIPS is private and that unauthorized third parties cannot eavesdrop or intercept CIPS communications.	4.1.12.3.1.1
5049	C.2.7.11 .1.4 (15)(d)	The following Converged IP Services capabilities are mandatory unless marked optional. d. Encryption and secure tunneling (Virtual Private Network (VPN)) at the Sensitive but Unclassified (SBU) through National Security Information (NSI) levels available under section C.2.10 Security Services and C.2.7.4 Managed Tier Security Services.	4.1.12.3.1.1

4.1.12.1 Qwest's Technical Approach to CIPS Delivery (L.34.1.4.1)

Qwest's technical approach to providing a fully compliant CIPS (i.e., data, voice, and video on a single network) is based on our well established, highly reliable, and secure fiber optic infrastructure; our commitment to our customers by our Operations and Engineering personnel; and our adherence to proven engineering practices. Qwest has fine-tuned processes to research, evaluate, engineer, deploy, and operate new CIPS features and functionality.

The sections that follow describe our approach to service delivery and how our approach benefits the Government. We'll also describe how Qwest CIPS will facilitate the Federal Enterprise Architecture (FEA) objectives, how

Qwest proposes to address problems that may be encountered in providing CIPS, and how our synchronization network architecture supports CIPS.

4.1.12.1.1 Approach to CIPS Delivery (L.34.1.4.1(a))

Standards-Based, Global Network

Qwest will meet the service requirements of CIPS (i.e., data, voice, and video on a single connection) with the Qwest IP network and the Qwest VoIP infrastructure. Qwest's IP network provides converged services with a single backbone network. Qwest's converged infrastructure approach integrates Public Switched Telephone Network (PSTN) switches, VoIP gateways, the Internet, and VoIP application Network Elements (NEs). [redacted] shows a high-level description of the components that make up CIPS. CIPS includes VoIP phones and VoIP client Service Enabling Devices (SEDs), video SEDs, Agency Local Area Network (LAN) equipment, Agency router SEDs and the Qwest IP-based elements that enable all of the required services. With the addition of the VoIP application NEs, Qwest provides a comprehensive finished solution to address the CIPS VoIP requirements.

Qwest has been passing and managing long distance VoIP traffic over our converged architecture since 2001.

Qwest's IP and VoIP networks comply with all "best practice" security procedures and safeguards to minimize susceptibility to security issues and prevent unauthorized access and eavesdropping. [redacted]

Non-domestic CIPS (Req_ID 5086; C.2.7.11.1.3)

Qwest's solution is available for all domestic locations as required.

Proven Engineering Practices

In addition to Qwest's proven experience in technology, Qwest has the sales support, planning, engineering, and operations staff committed to collaborate with the Agencies to design, implement, support, and continually review CIPS performance and to upgrade as appropriate in order to ensure performance goals are maintained. The Qwest Sales Engineering Team will review the Agency's firewall and security structure and collaborate with the Agency to verify that the Agency's network architecture is reviewed for compatibility with CIPS. Qwest will make recommendations and provide full configuration information to ensure the proper operation of the CIPS at each Agency location.

Commitment to Customers

[redacted] The NOCs maintain and monitor all NEs on the Qwest data networks—including access and network backbone circuits—providing 24x7x365 service and proactively identifying, isolating, and resolving network issues and fault conditions. To provide emergency continuity of operations, the NOCs are redundant and staffed with cross-functional technical resources.

4.1.12.1.2 Benefits of Qwest's CIPS Technical Approach (L.34.1.4.1 (b))

Qwest's approach to convergence is built upon the principle of addressing and anticipating a multi-service converged environment. Qwest does so by employing integrated management and service controls and using a packet-based infrastructure that delivers end-to-end high value services via broadband access over high-capacity optical transport. Qwest provides

Agencies a reliable, secure, end-to-end service with the features and benefits, as summarized in ***Figure 4.1.12-3***.

Figure 4.1.12-3 Summary of Qwest's CIPS Features and Benefits

Features	Benefits	Substantiation
Converged VoIP service on IP network	[redacted]	[redacted]
Full IP Quality of Service	[redacted]	[redacted]
Flexible access methods available (e.g. IP Point-to-Point Protocol, FR, ATM, x Digital Subscriber Line)	[redacted]	[redacted]

The Qwest CIPS facilitates the FEA objectives, as summarized in ***Figure 4.1.12-4***.

Figure 4.1.12-4 Qwest's CIPS Support to FEA Objectives

FEA Objective	[redacted]
Improve utilization of Government information resources to focus on core Agency mission and service delivery to citizens by using the FEA.	[redacted]
Enhance cost savings and avoidance	[redacted]
Increase cross-Agency and inter-Government collaboration	[redacted]

4.1.12.1.3 Solutions to CIPS Problems (L.34.1.4.1(c))

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

CIPS is comprised of multiple component services that are independently reliable and secure. The end-to-end service is monitored as a whole, providing operations and Agencies with a service level view that integrates all the components. Systems and procedures are in place to ensure that CIPS is viewed as a whole, but can be monitored and managed independently. Qwest has built systems for each integrated service that enables operations personnel and Agencies to monitor and troubleshoot the service [redacted] Our broad experience with the component services that make up CIPS provides a solid foundation for understanding the problems that could be encountered in meeting CIPS service requirements. ***Figure 4.1.12-5*** summarizes these problems along with our proposed solutions.

Figure 4.1.12-5 Qwest's Approach to Common CIPS Delivery Challenges

Problem	[redacted]
Customer is managing disparate networks for voice and data traffic.	[redacted]
Call oversubscription can result in quality problems	[redacted]
Caller privacy is contaminated	[redacted]
Customer	[redacted]

Problem	
experiences a lack of security in a converged network	[redacted]

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

Time of Day Synchronization (IP Network)

[redacted]

Transport Network Synchronization

[redacted]

[redacted]

[redacted]

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

[redacted]

[redacted]

4.1.12.2 Satisfaction of CIPS Performance Requirements (L.34.1.4.2)

The Qwest CIPS solution meets all performance requirements stated in this section. Qwest has proven network monitoring and measuring systems, procedures, and evaluation methods in place to ensure compliance.

4.1.12.2.1 CIPS Quality of Service (L.34.1.4.2 (a))

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 its CIPS solution. Qwest's performance measurement methodology is fully compliant with the Government's requirement. ***Figure 4.1.12-8*** summarizes our support for CIPS performance requirements.

Figure 4.1.12-8 Qwest's Compliance with Government CIPS Performance Metrics

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

Qwest understands latency to be the average round trip time for a packet to travel between source and destination Service Delivery Points (SDPs). Qwest's IP backbone network capacity and Point of Presence (POP) locations [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] 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, [redacted]

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

[redacted]

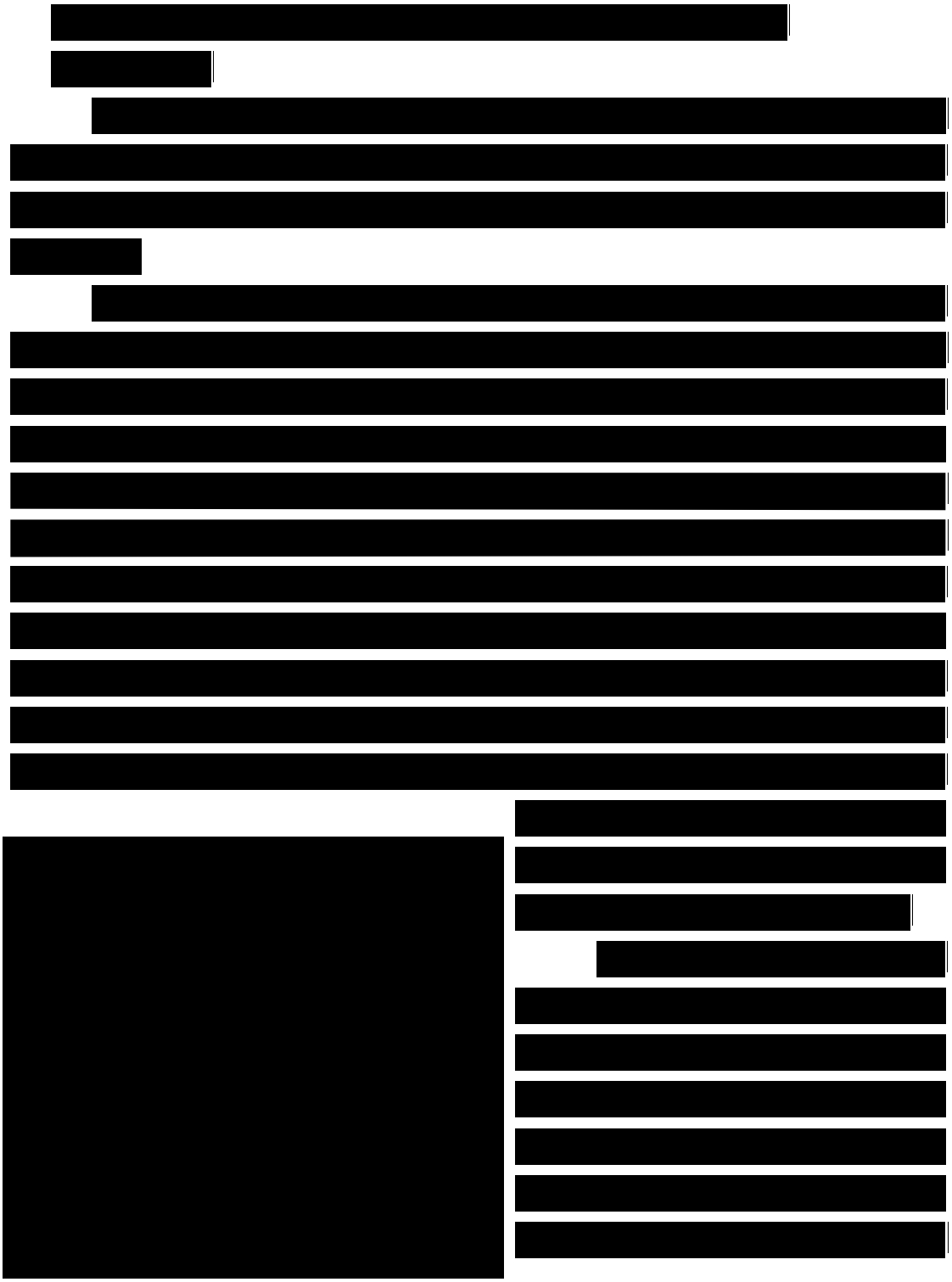
Qwest understands jitter to be the variation in the delay between received packets of an IP data stream from SDP-to-SDP. Jitter is typically the result of congestion. [redacted] The monitoring methods defined in the following section (4.1.12.2.2) describe in detail how Qwest monitors the network to ensure that we meet the AQLs.

4.1.12.2.2 Approach for Monitoring and Measuring CIPS KPIs and AQLs (L.34.1.4.2 (b))

Qwest monitors and measures the Key Performance Indicators (KPIs) and AQLs using automated processes that pull data from the root source, summarize it, and display it using Web tools. 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, which include the eight mandatory services (IPS, Network Based Internet Protocol VPNS (NBIP-VPNS), Premises-Based IP VPNS (PBIP-VPNS), Layer 2 Virtual Private Network Service (L2VPNS), CIPS, Content Delivery Network Services (CDNS), Voice Over Internet Protocol Transport Services (VOIPTS), and Internet Protocol Telephony Service (IPTelS)), are provided over the same IP services infrastructure. [redacted]



[redacted]

If an Agency orders a service in which the technical performance requirements are specified on an SDP-to-SDP basis (including performance requirements specified on an end-to-end and/or Agency premises-to-Agency premises performance requirement basis) and where Qwest requires the use of SEDs to meet the requirements and/or requires access to, or use of, the Agency's CPE or software to meet the requirements, then Qwest understands that the ordering Agency may (1) elect to not order such SEDs and/or (2) elect to not permit Qwest access to, or any use of, the Agency's customer-premises equipment or software for such purposes.

Qwest further understands that in these situation(s) and unless otherwise agreed to by Qwest and the user Agency, Qwest, when directed by the user Agency or by General Services Administration (GSA), will monitor, measure, and report the performance of the service for KPI/AQL and for SLA purposes either (1) on an SDP-to-SDP basis, by defining the SDP for performance metric measurement purposes for affected location(s) as being located at the connecting POP(s) of the location(s), or (2) on a POP-to-POP basis. If directed to use the latter method by the Agency, Qwest will comply with the following:

1. For all IP-based network services, the applicable POP-to-POP performance requirements to be used will be those defined in Section C.2.4.1 (IPS).
2. For all other services, the service-specific SDP-to-SDP performance metrics will be applied on a POP-to-POP basis unless a stipulated POP-to-POP performance metric already applies for the associated service(s).

In summary, three options are available:

1. Standard SDP-to-SDP approach
2. Auxiliary SED for SDP-to-SDP monitoring

3. POP-to-POP as defined in Amendment 8

Use of Statistical Sampling in lieu of Direct KPI Measurements

[redacted]

The Use of Government Furnished Property

If an Agency orders a Transport/IP/optical service in which they are employing a device, Qwest will provide KPI monitoring and measurement of the delivered service in three ways:

A. Request that the Agency provide SNMP capability to the device for the Qwest NOC

B. Request that the Agency buy a monitoring SED from Qwest

C. Coordinate with the Agency per Amendment 8 change for the following:

- Qwest understands that the ordering Agency may (1) elect to not order such SEDs and/or (2) elect to not permit Qwest access to, or any use of, the Agency's CPE or software for such purposes.
- Qwest further understands that in these situation(s) and unless otherwise agreed to by Qwest and the user Agency, Qwest, when directed by the user Agency or by GSA, will monitor, measure, and report the performance of the service for KPI/AQL and for SLA purposes either (1) on an SDP-to-SDP basis, by defining the SDP for performance metric measurement purposes for affected location(s) as being located at the connecting POP(s) of the location(s), or (2) on a POP-to-POP basis.

[redacted]

[redacted]

For all services that Qwest offers, we use the [redacted] a trouble ticketing system that is an industry-leading off-the-shelf commercial application that we have customized to make more effective for our needs. From this system, we collect many useful metrics that we use internally to evaluate and improve our processes, including Time to Restore (TTR). The calculation for TTR uses the same business rules as the Government requires for its services.

The Qwest Infrastructure Group monitors IP Network utilization. The group also reports statistics to the Data Network Planning and Design group. This information also is distributed to internal databases and is available to customers through the Qwest Control Networx Portal. This portal provides Agencies with performance statistics to verify that Agency-specified AQLs are met. [redacted]. Qwest employs [redacted]™ monitoring agents to produce the real-time performance reports.

For CIPS, all of the required AQLs are assessed on an individual site basis or on a site-pair basis where applicable. This data is used to ensure that all Agency Data Network AQLs are systematically supported by the network. Additionally, key network infrastructure interfaces (e.g., aggregation 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's VoIP network leverages both active and passive methods for ensuring media and signaling quality. In conjunction with our robust OC-192 network (which provides the backbone services for the Qwest VoIP network), full network analysis is performed via media loopback schemes (compliant with current Internet Engineering Task Force (IETF) draft functionality) with planned support for Real-Time Control Protocol (RTCP) as defined in RFC3550 [redacted]

4.1.12.2.3 CIPS Performance Improvements (L.34.1.4.2 (c))

Qwest proposes to meet required KPIs and AQLs for CIPS. 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 will leverage our vast CIPS product portfolio, which includes a variety of SED providers and specific CIPS solutions. Through a special combination of vendor solutions and talented engineering capabilities, Qwest will serve an Agency's business needs.

4.1.12.2.4 Additional CIPS Performance Metrics (L.34.1.4.2 (d))

[redacted]

4.1.12.3 Satisfaction of CIPS Specifications (L.34.1.4.3)

Qwest will meet all CIPS requirements using our IP network and VoIP infrastructure. The following sections describe how Qwest satisfies the service specifications in the Request for Proposal (RFP).

4.1.12.3.1 Satisfaction of CIPS Requirements (L.34.1.4.3 (a))

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

4.1.12.3.1.1 Satisfaction of CIPS Capabilities Requirements (L.34.1.4.2(a); 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 PSTN for both originating and terminating traffic. Access to an Agency's intranet (based on NBIP-VPNS, PBIP-VPNS, L2VPNS, ATMS, or 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, as shown in ***Figure 4.1.12-9***. Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for CIPS. The text in the following table is intended to provide the technical description required per L.34.1.4.2(a) and does not limit or caveat Qwest's compliance in any way.

Figure 4.1.12-9. 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	Agency determines prioritization of applications	[redacted]

ID #	Name of Capability	[redacted]
		[redacted]
5	Gateways	[redacted]
6	Network Capacity	[redacted]
7	Dynamic IP Addressing	[redacted]
8	Secure Website	[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	[redacted]

ID #	Name of Capability	[redacted]
	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 5082; 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. Qwest's CIPS solution is equipped to support QoS-based, Agency-controlled network services specializing in real-time application performance across converged networks. Both predetermined and customizable QoS templates are available to address Agency business needs.

To enable the convergence of Agency applications with required performance, Qwest provides [redacted]

[redacted]

Qwest's CoS uses industry-standard techniques including the CBWFQ methodology. Qwest will work with Agencies to engineer their CoS design to ensure that the service meets application requirements.

[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 PE on the access line towards the Agency 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]

Agencies have the option to apply Unique QoS policies on each port, as follows:

[redacted]

Gateways for Protocol Conversion, CIPS interface and External Networks (Req_ID 5078; 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. [redacted]

[redacted] 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 the Layer 3 services, but no interworking at the protocol level is required.

Qwest utilizes [redacted] gateways to interface with the PSTN network. Qwest employs [redacted] gateways for conversion between IP voice traffic and TDM voice traffic and [redacted] gateways to interface with the SS7 network. Qwest utilizes [redacted] systems at the IP-to-IP network boundaries to manage traffic and convert protocols.

Network Capacity to Deliver CIPS (Req_ID 5076; C.2.7.11.1.4(6))

Qwest's OC-192 core network will ensure adequate network capacity to deliver CIPS service for all Agencies. Qwest built its network to provide high availability to our customers. Qwest's performance measures and engineering practices are designed to provide robustness of the access and backbone networks, ensure resiliency, and prepare for growth. Our design procedures, network modeling, and circuit route checks provide a high level of customer service.

These practices include application of network design rules, network capacity modeling for failure scenarios, and circuit route check to ensure redundant and diverse routing. In addition, the design of our network unifies technologies under a common service platform where all NEs are designed with resiliency and growth in mind.

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 4.1.12.4.2 and 4.1.12.5 for further information regarding the availability of adequate network capacity.

Utilization Statistics (Req_ID 5072; C.2.7.11.1.4 (8)(b))

Statistics will be available through the Qwest Control Networx Portal. [redacted]

Active Directory Compatibility (Req_ID 5058; C.2.7.11.1.4 (13))

Qwest's CIPS is currently compatible with Agency provided AD services using Lightweight Directory Access Protocol to interface with the Networx Qwest Control portal. The office administration tool within the portal enables this capability and provides compatibility with Agency-provided Active Directory services. Updates made to the Agency provided Active Directory are supported by linked updates in the office administration tool.

Agency Firewall Compatibility (Req_ID 5055; C.2.7.11.1.4 (14))

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

Security Practices (Req_ID 5054; C.2.7.11.1.4 (15))

Qwest will ensure 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] Vulnerability scanning and penetration testing is standard for new element or code deployment. [redacted]

Qwest Hosted VoIP services are protected via defense in depth. ACLs, rate limits, and firewall rules throughout our network restrict access to the individual NEs used in Qwest Hosted VoIP. [redacted]

Regular Audit and Update of Security Practices (Req_ID 5053; C.2.7.11.1.4 (15))

Qwest will ensure security practices and policies are updated and audited regularly. Qwest performs ongoing audit scans on production NEs. For audits, we have a mature process that includes [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 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 bidirectional 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]

Safeguards to Prevent Denial of Service Attacks (Req_ID 5052; 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.

Specific protections against cyber attacks include:

a) [redacted]

[redacted]

Safeguards to Mitigate Illegitimate CIPS Use (Req_ID 5051; C.2.7.11.1.4 (15)(b))

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

Most of the safeguards for DDoS will also act as safeguards to block attempts to illegitimately use CIPS, but the [redacted] main safeguards are:

[redacted]

Prevent Invasion of Privacy (Req_ID 5050; 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 that unauthorized third parties cannot eavesdrop on the packet payloads through the use of [redacted] to further protect the CIPS payloads.

The Qwest network [redacted]

Encryption and Secure Tunneling at SBU Level (Req_ID 5049; C.2.7.11.1.4 (15)(d))

Encryption and secure tunneling (VPN), at the SBU through NSI levels available under section C.2.10 Security Services and C.2.7.2 Premised 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.

4.1.12.3.1.2 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.

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

Qwest CIPS UNI types and their associated SEDs are shown below in ***Figure 4.1.12-10***. Qwest may substitute these SEDs over the course of the Networx program with SEDs of comparable functional and performance capabilities. Qwest fully complies with all mandatory stipulated and narrative features, capabilities, and interface requirements for CIPS. The text in the following table is intended to provide the technical description required per L.34.1.4.2(a) and does not limit or caveat Qwest's compliance in any way.

Figure 4.1.12-10. Qwest Provided CIPS Interfaces at the SDP

UNI Type	Interface Type and Standard	Payload Data Rate or Bandwidth	Signaling Type	[redacted]
1	All 802.3 cable and Connector types	10/ 100/ 1000 Mbps	IPv4 (v6 when and where available commercially from the contractor) 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]

4.1.12.3.2 Proposed Enhancements to CIPS (L.34.1.4.3 (b))

[redacted]

4.1.12.3.3 Network Modifications Required for CIPS Delivery (L.34.1.4.3(c))

Qwest's network requires no additional modifications to satisfy CIPS requirements.

4.1.12.3.4 Experience with CIPS Delivery (L.34.1.4.3 (d))

Qwest is a proven provider for both voice and data/IP services and has long been a leader in IP network technology. Its 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 its long distance traffic over IP [redacted]) since 2001. 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 2001 and currently running more than 4 billion minutes per month on our VoIP platform

[redacted]

- 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 network consisting [redacted] DMS-250s, [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 20 years. Qwest expertly manages IPS narrowband, broadband, satellite, Integrated Services Digital Network (ISDN), and Wireless Fidelity (WiFi) access services, delivered by industry-leading alliances such as Covad for nationwide Digital Subscriber Line (DSL) service and [redacted] 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]

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, state government, and educational institutions. Qwest dedicated IP access services customers include [redacted] one of the largest domestic consumer dial-up providers, as well [redacted]

4.1.12.4 Robust Delivery of CIPS (L.34.1.4.4)

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.

4.1.12.4.1 Support for Government CIPS Traffic (L.34.1.4.4 (a))

Qwest will use its robust, state-of-the-art IP Networking platform and VoIP platform to provide CIPS services. The Government traffic model indicates about 5,300 VoIP telephone numbers, less than 200 DS0 – DS-1 IP/MPLS ports, and less than 150 DS-3 IP/MPLS ports will be deployed over the next 10 years. This represents an incremental increase [redacted] to the Qwest IP and VoIP networks. Qwest will easily absorb the projected traffic onto our existing service infrastructure.

4.1.12.4.2 CIPS Measures and Engineering Practices (L.34.1.4.4 (b))

The speed and size of Agencies' telecommunications systems can grow easily and transparently on the Qwest network. Qwest has a history of adapting rapidly to meet customer requirements. [redacted] As their traffic requirements grew, Qwest used the practices described here to incrementally transition the customer to a 10Gbps wavelength network. CIPS explicitly requires that network resiliency and growth be addressed both from an IP transport infrastructure standpoint and from the support of voice- and video-oriented capabilities. The following paragraphs first address our approach for engineering and planning for our core network and then discuss our voice-oriented strategy.

Qwest built its network to provide high availability to our customers. Qwest's performance measures and engineering practices are designed to

provide robustness of the access and backbone networks, ensure resiliency, and prepare for growth. Our design procedures, network modeling, and circuit route checks provide a high level of customer service. In addition, Qwest's centralized engineering team applies a consistent capacity management model to all data services.

These practices include application of network design rules, network capacity modeling for failure scenarios, and circuit route check to ensure redundant and diverse routing. In addition, the design of our network unifies technologies under a common service platform where all NEs are designed with resiliency and growth in mind.

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. [redacted] Edge aggregation devices are those devices that directly terminate customer circuits. Usage statistics are gathered on every edge aggregation circuit, and reports are generated using these samples for weekly review. [redacted]

[redacted] of the same speed, provisioned over diverse physical facilities provided by the Qwest state-of-the-art nationwide Dense Wavelength Division Multiplexing wavelength network and self-healing SONET backbone. Usage reports are gathered and reviewed for all backbone circuits (defined as those circuits that interconnect core backbone devices), just as they are for the edge aggregation circuits. [redacted]

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

We analyze how the traffic utilization patterns will be affected under abnormal network conditions and then take the appropriate action, such as adding new nodes or links. [redacted] We are able to predict how the failure would affect traffic utilization on the other backbone circuits and identify backbone circuits that need to be upgraded.

When placing an order to have a new backbone link added to the network, the Qwest engineers will circuit-route check the facilities to make sure the new backbone link is distinct from the other backbone links. The new circuit route information will then be entered into the order to be carried out by

the Qwest Provisioning team. Qwest Engineering audits existing backbone circuits several times a year to make sure that the backbone links are diverse.

In addition, simulations are run to determine the traffic distribution in the event of a failure of any router, link, or fiber path in the network. This takes into consideration the fact that multiple long haul circuits may share a single conduit in some sections of the fiber network. The network is designed to be able to handle the full offered load in the event of any single failure, so the physical routing of the new circuit must follow a path that allows it to meet these requirements. The new circuit route information will then be entered into the order to be carried out by the Qwest Provisioning Team.

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

A key element of CIPS involves the support for voice-based services. Qwest VoIP service will scale to meet future Agency capacity requirements through a modular network architecture, consisting of discreet components providing [redacted] services. Each one of these modules can be expanded or supplemented as required.

[redacted]

Qwest has chosen vendor platforms that meet some form of high availability scheme. Depending on the system, there may be a 1+1 or N+1 configuration of hardware to ensure high reliability for voice services. Qwest's goal is to provide Agencies with a network that meets their requirements.

[redacted] Connectivity to the Agency premise can be done via diverse paths in some cases, where facilities are available and the Agency has specific requirements and agreements.

SS7 Signaling is done via an extremely robust network. [redacted] All of the SS7 systems are fully redundant and geographically redundant as well. Voice traffic and signaling traffic is carried over SONET rings for secured transport.

4.1.12.5 CIPS Optimization and Interoperability (L.34.1.4.5)

This section discusses Qwest's approach to optimizing CIPS, the approach to optimizing network architecture, access optimization, and Qwest's vision for CIPS internetworking.

4.1.12.5.1 Optimizing the Engineering of CIPS (L.34.1.4.5 (a))

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.

For example, if analysis results show that AQL can be maintained by link metric adjustments, then Qwest engineers will update the configuration immediately. If additional equipment and/or new backbone links are required, the Qwest engineers will deploy new equipment and design and install new circuits.

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

As Agency traffic demands increase, Qwest will design, engineer, and deploy edge devices at POPs closest to the Agency locations to provide L2/L3 services locally and aggregate customer traffic and backhaul them to larger POPs if the traffic needs to leave the area. [redacted] This type of network arrangement will allow the customer access loops to be shortened, which will lead to lower latency and higher availability as portions of the backhauled access loops will now be replaced by the redundant and diverse high-speed uplinks.

As Networx traffic and traffic from other customers increases, Qwest will add uplinks and backbone links to the network. At certain points, the Qwest engineers will evaluate the percentage of utilization on the links and see if it would make sense to use higher bandwidth links to replace multiple lower bandwidth links and ensure that the new links are resilient and affect a network-wide improvement to overall performance. Qwest takes a proactive stance on network optimization because when the network architecture is optimized, it scales better and becomes much easier to manage.

4.1.12.5.3 Access Optimization for CIPS (L.34.1.4.5 (c))

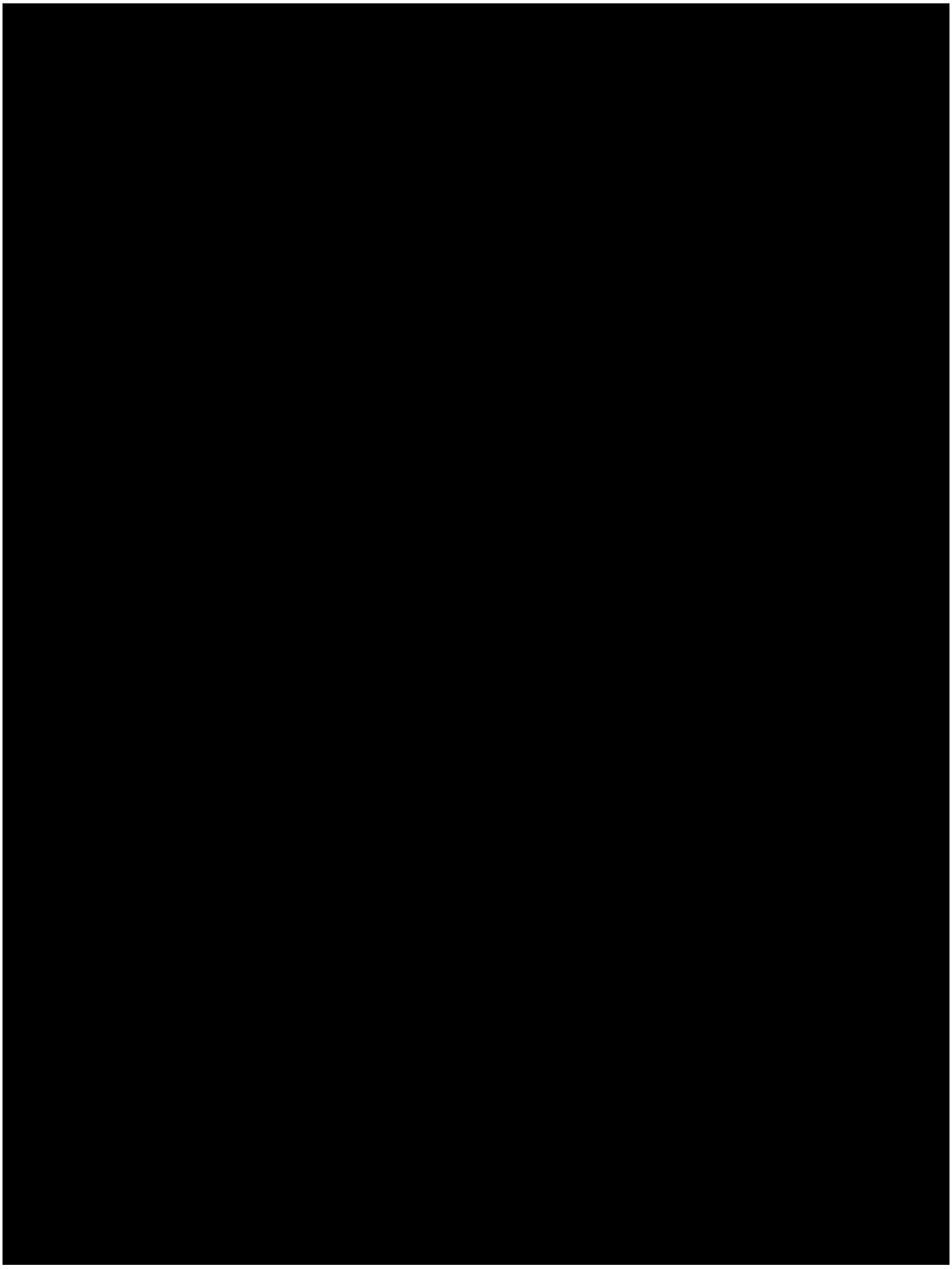
[redacted]

4.1.12.5.4 Vision for CIPS Internetworking (L.34.1.4.5 (d))

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

Qwest's service delivery model supports multiple types of customer requirements. Qwest's approach for network architecture evolution guides our investments and provides the overall direction for our technology evolution and services convergence. 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 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.



[redacted]

[redacted]

[redacted]

In summary, the Qwest backbone has been transformed from primarily serving Internet traffic into a general-purpose packet transport network with TDM-like quality characteristics, capable of serving multiple kinds of application traffic, including Internet, L3 VPNs, L2 VPNs, VoIP, Video over IP, Storage over IP, etc.