5.2.8 Teleworking Services (TWS) (L.34.1.5.4, M.2.1.4)

Qwest's Networx TWS is interoperable with a multitude of channels, allowing for seamless delivery to Government Agencies.

Qwest's TeleWorking Services (TWS) offering enables Agency employees to work remotely. The service includes a range of capabilities up to and including a fully managed service with customizable features. TWS offers a feature-rich virtual assistant designed to enhance an Agency's ability to manage alternative work arrangements for authorized remote workers. TWS is a "bandwidth-neutral" solution that allows remote workers to connect back to their secured Local Area Networks (LANs) and/or Internet via any available bandwidth option (dial-up, wireless fidelity (WiFi), broadband, etc.) from a single client interface. It includes a full range of telecommunication and security services necessary to support full teleworker productivity. Additionally, Qwest's TWS offering includes a full range of managed O&M and security services, secure remote access to applications, and collaboration tools.

Figure 5.2.8-1 provides an easy reference to correlate narrative requirements to Qwest's proposal response.

Figure 5.2.8-1. Responses to Narrative Mandatory Service Requirements

Req_ID	RFP Section	[redacted]
33752	C.2.12.1.1.3	[redacted]
33753	C.2.12.1.1.4 (1)	[redacted]
33755	C.2.12.1.1.4 (2) (a)	[redacted]
33757	C.2.12.1.1.4 (2) (b)	[redacted]
33758	C.2.12.1.1.4 (3)	[redacted]
33760	C.2.12.1.1.4 (4) (a)	[redacted]
33761	C.2.12.1.1.4 (4) (b)	[redacted]
33762	C.2.12.1.1.4 (4) (c)	[redacted]
33763	C.2.12.1.1.4 (4) (d)	[redacted]

Req_ID	RFP Section	[redacted]
33764	C.2.12.1.1.4 (4) (e)	[redacted]
33765	C.2.12.1.1.4 (5)	[redacted]
33772	C.2.12.1.1.4 (6)	[redacted]
33777	C.2.12.1.1.4 (10)	[redacted]
33788	C.2.12.1.2.1 (6)	[redacted]
33797	C.2.12.1.2.1 (8)	[redacted]
33810	C.2.12.1.3.1 (1)	[redacted]
33811	C.2.12.1.3.1 (2)	[redacted]
33812	C.2.12.1.3.1 (3)	[redacted]
33813	C.2.12.1.3.1 (4)	[redacted]
33814	C.2.12.1.3.1 (5)	[redacted]

5.2.8.1 Reserved (L.34.1.5.4 (a))

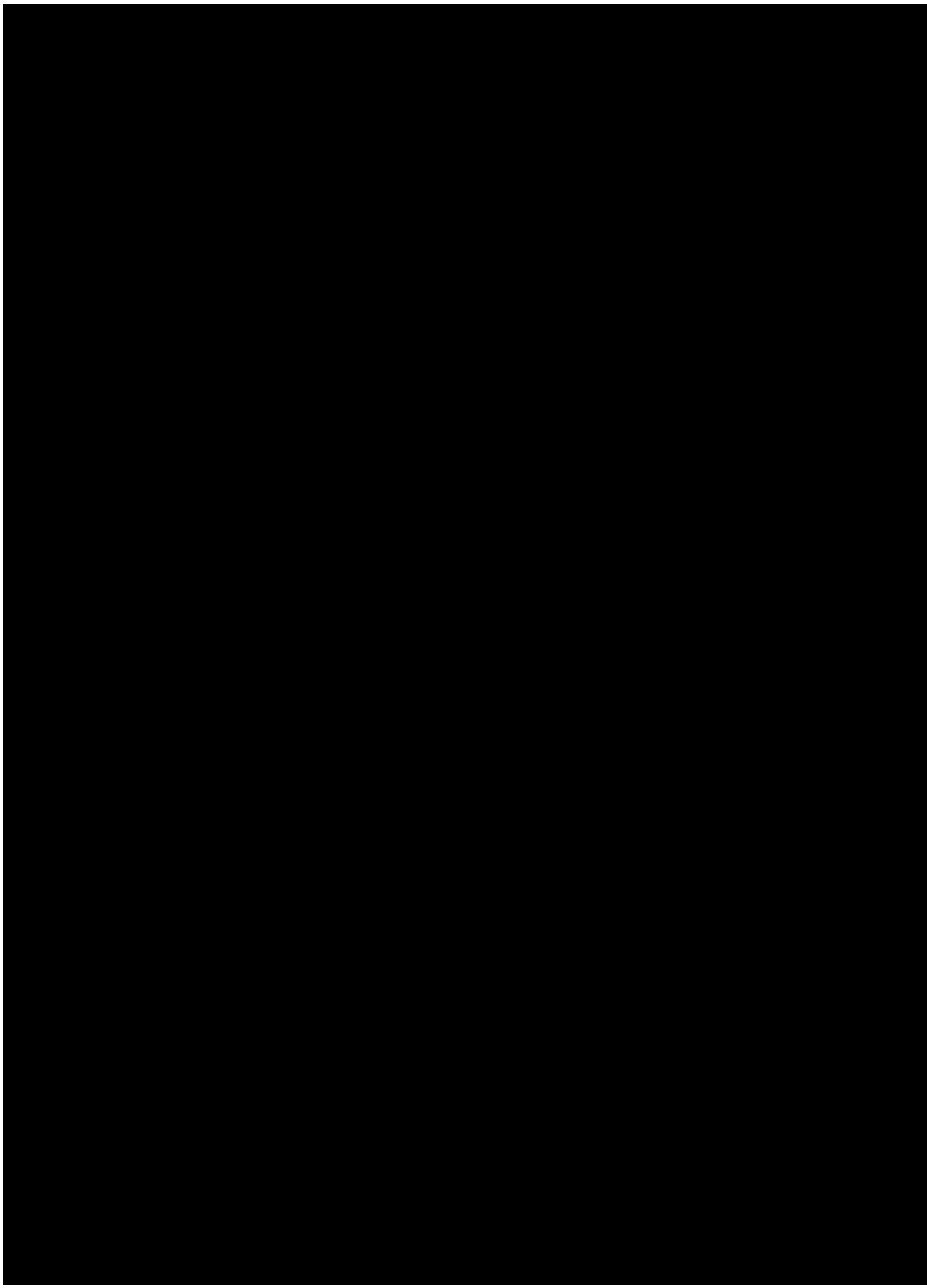
5.2.8.2 Reserved (L.34.1.5.4 (b))

5.2.8.3 Satisfaction of Teleworking Service Requirements (L.34.1.5.4 (c))

Qwest uses a Mobility client/server application to deliver TWS to Agencies. The Qwest Mobility client can be used as either an Internet-only access client or as a Virtual Private Network (VPN) access client to securely connect the user to the Agency's Intranet over any supported Internet access type.

This Qwest remote access service is a flexible suite of business-class, global remote Internet access and VPN solutions that provide mobile professionals and teleworkers with encrypted VPN access to the corporate LAN using a variety of transport methods.

[redacted]



Qwest provides options to seamlessly integrate Qwest's one-click smart client for VPN communication with an Agency's own VPN gateway and existing VPN authentication methods or to use the service for mobile employee Internet access only.

5.2.8.3.1 Satisfaction of Teleworking Service Capabilities Requirements (L34.1.5.4 (c), C.2.12.1.1.4)

Qwest fully complies with all mandatory stipulated and narrative capabilities requirements for TWS. The following text is intended to provide the technical description required per L.34.1.5.4 (c) and does not limit or caveat Qwest's compliance in any way.

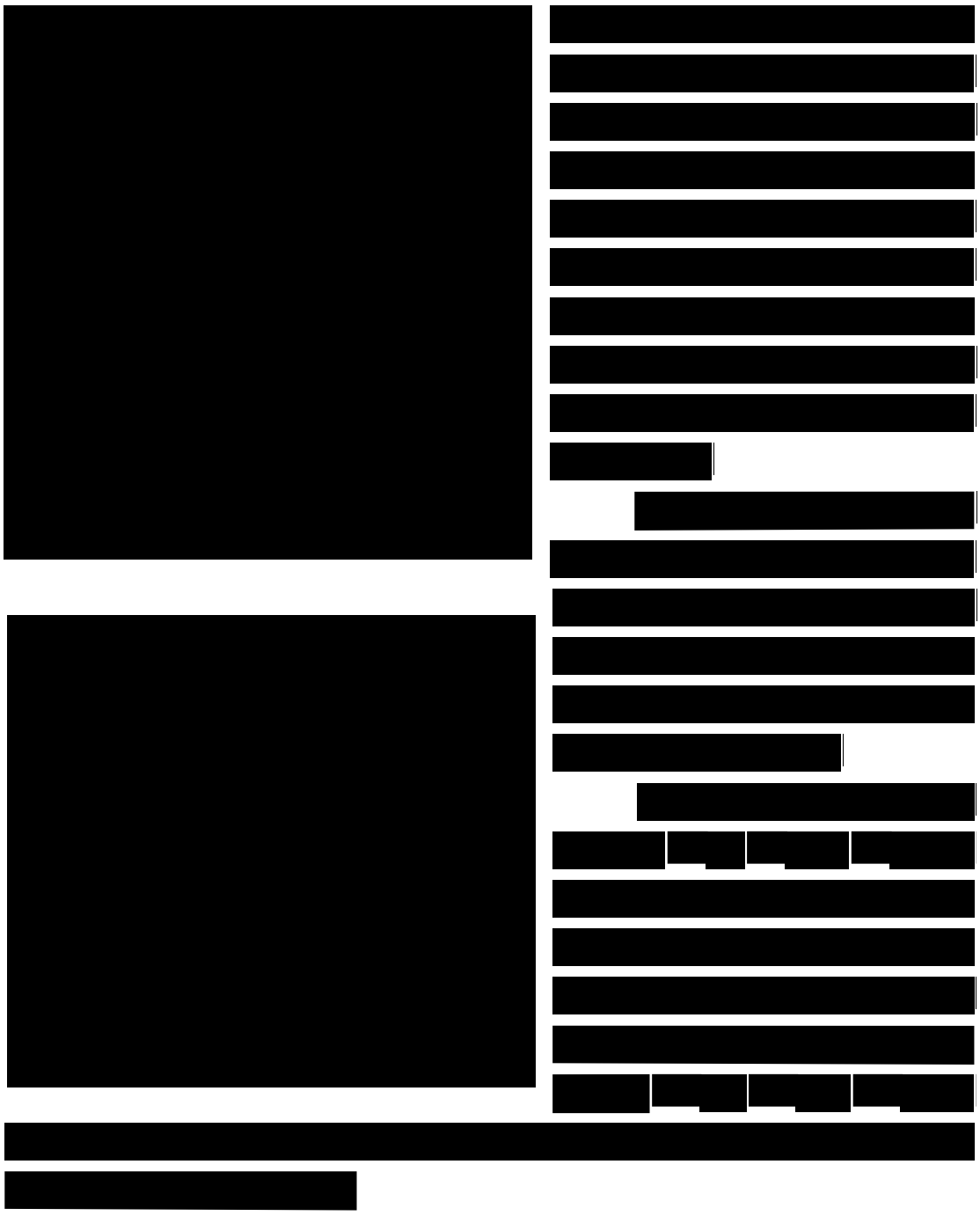
Qwest Mobility Client Overview

When used as an Internet-only access client or for VPN access over the Internet, Qwest Mobility supports a common directory and connect-button user interface for use with the following Internet access types:

- Dial-up analog or ISDN telephone line (Qwest global dial access numbers; integration of Agency own dial-up phone book)
- IEEE 802.11b/g Wi-Fi locations (Qwest Wi-Fi locations; non-Qwest Wi-Fi locations; private WLAN)
- An existing non-Qwest Internet access connection (e.g., home broadband, non-Qwest hotel broadband or other)

When used as a VPN access client, Qwest Mobility provides a VPN login user interface that is compatible with a wide variety of VPN solutions [redacted]

For Agencies that support multiple types of VPN gateways, the Qwest Mobility client enables the integration of mixed types of VPN gateways, all using a single VPN user interface, thus reducing Help Desk costs. [redacted]



[redacted]

The Qwest TWS service includes comprehensive engineering and Help Desk support that offers the teleworker two tiers of service:

Tier 1 *– Basic*: Qwest provides the basic connectivity and related components necessary to establish teleworker capabilities for the subscriber. With this service, Qwest provides a functional group within the Qwest Customer Support Office (CSO) to oversee the installation, configuration, and provisioning of a wide variety of transport services that are offered under the Networx contract. Under this option, the teleworker's supporting Agency would provide technical support for the teleworker's software and applications.

[redacted]

The Qwest approach to service delivery combines highly-trained program management and Help Desk support personnel—geographically diverse and best-in-class automated customer care centers—and underlying network and security services to enable remote communications to Agency applications from the teleworkers' remote work locations. depicts the components that comprise Qwest's service delivery approach. The following describes the components of the Qwest service delivery architecture:

Highly Trained Program Management and Help Desk Support Personnel: The TWS user receives the benefit of having highly-trained individuals who are experienced and adept at responding to networking and applications queries of any type affecting their operating environment.

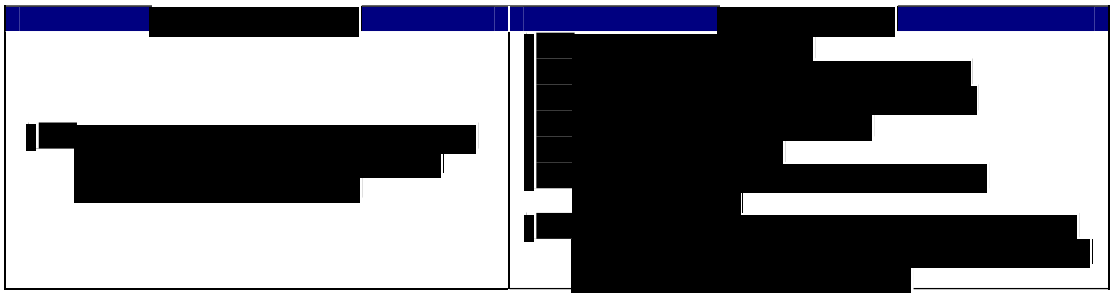
The Qwest Help Desk will be the Agency's primary point of contact for post-sales questions about the use of the services (to be defined service by service) and will act as a resource to direct users to other Qwest resources who can help resolve the user's issue. The Qwest Help Desk will continue to be the user's primary point of contact for portal navigation and education; administration and account management; site functionality trouble resolution; inventory verification; PC configuration issues; and basic trouble shooting, execution of fall-out procedures, and table/system updates. The Qwest Help Desk will provide Agencies with a consistent level of resolution, irrespective of the access channels: fax, telephone, postal service, click-to-chat, or email. Additionally, the Qwest Help Desk will be TDD-accessible.

[redacted]

Qwest offers a best-in-class automated Customer Support Office (CSO) enabling support through various mechanisms, including the Qwest Control Networx Portal, Interactive Voice Response (IVR), email, fax, postal service, and Click-to-Chat. Qwest's centers are TDD-capable and are configured with robust physical and network infrastructures.

The Qwest team uses move, add, and change features from Qwest's automated technology to minimize the time needed to resolve a teleworker's service installation and setup.

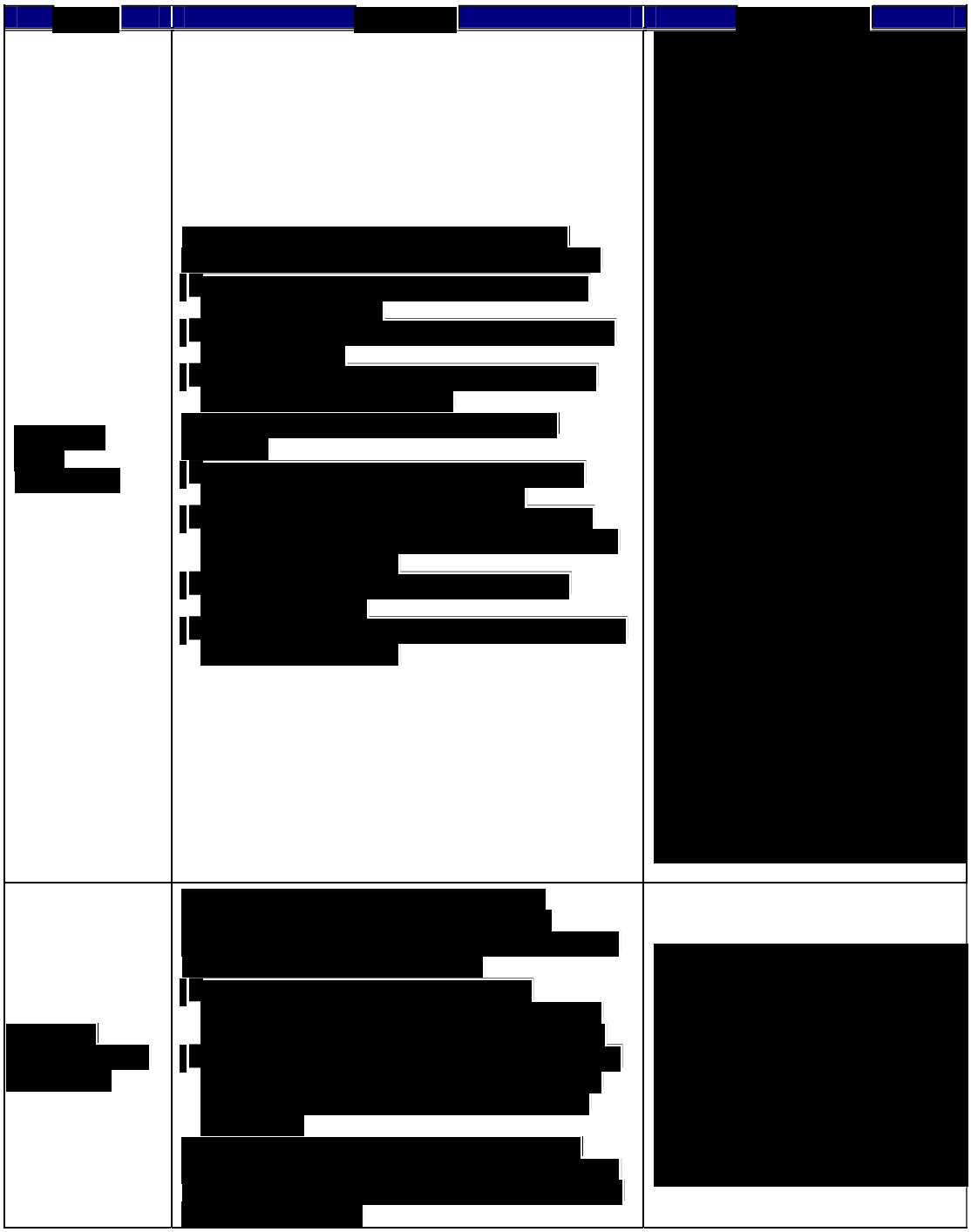
Network and Security Services: TWS will provide network and security services critical to the teleworker's data and communications security. [redacted]

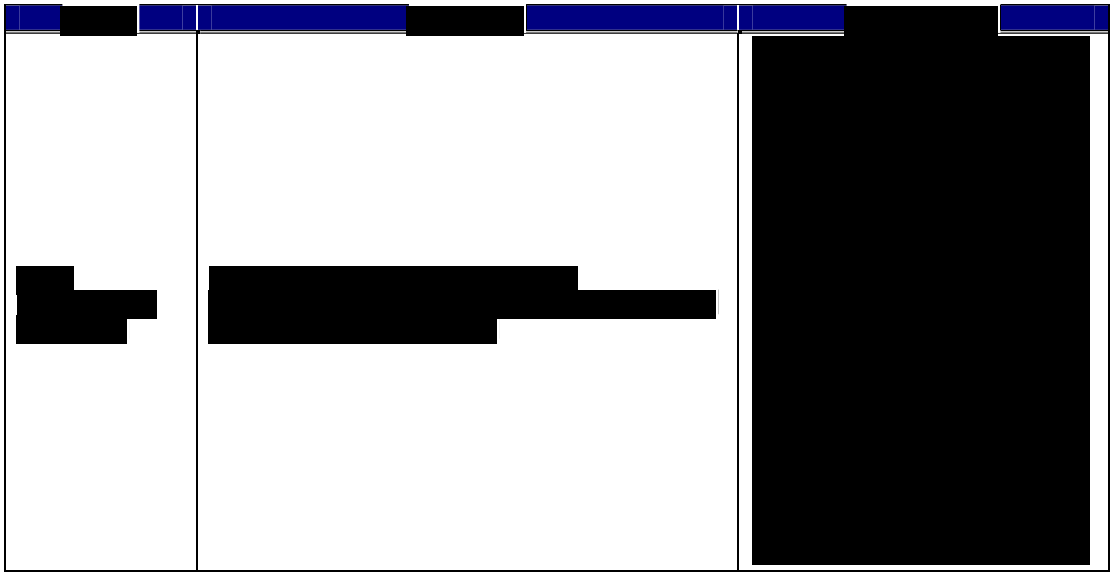


Qwest Mobility Security Policy Management

Security and policy enforcement are important aspects of the service and are being used today with great success by customers. As a Qwest Mobility customization option, this service currently supports two optional methods of policy enforcement: [redacted]

[redacted]





Qwest's pre-sales engineering will assist the Agency in developing an optimal solution to ensure a cost-effective and secure TWS capability using underlying security and communications services such as, Network-Based IP VPN services, ISDN, Broadband, or Private Line services. Qwest's provisioning and operations groups will ensure that the solution is installed and maintained to meet the Government's requirements.

5.2.8.3.1.1 Communications from Teleworker Location to Agency (Req_ID 33752), (C.2.12.1.1.3)

Qwest provides options to seamlessly integrate a one-click smart client for VPN communication with the Agency-owned VPN gateway and authentication methods. Section 5.2.8.3 and Figure 5.2.8-4 show how Qwest provides seamless communications from a teleworker's location to an Agency's Intranet (corporate LAN). Figure 5.2.8-6 shows that within the Qwest Mobility client, the teleworkers choose from among the list of available connections (e.g., paid Ethernet, dial-up) and then, for all access types, the teleworker clicks the same Connect button. For Qwest Mobility directory

searches, the teleworker clicks the Directory button and, for all access types, can search the directory by location (country, state, city), in addition to other types of directory searches, such as by dial-up access number, access type, and location type (e.g., hotel).

5.2.8.3.1.2 Data and Voice Connectivity (Req_ID 33753), (C.2.12.1.1.4 (1))

[redacted]

5.2.8.3.1.3 Tier 1 Basic Subscriber Capabilities (Req_ID 33755), (C.2.12.1.1.4 (2) (a))

With a single click on the “download client” button, the Qwest Control Networx Portal enables the Agency mobile workforce and teleworkers to download and automatically install the Qwest Mobility client software. [redacted]

5.2.8.3.1.4 Tier 2 Enhanced Custom Service (Req_ID 33757), (C.2.12.1.1.4 (2) (b))

[redacted]

[redacted]

5.2.8.3.1.5 Authentication and Encryption Capabilities (Req_ID 33758), (C.2.12.1.1.4 (3))

The service enables Agency mobile or remote employees to utilize a single account at thousands of dial-up and wireless broadband Internet access locations via Agency user Internet access accounts, hosted either by Qwest RADIUS servers or Agency-owned RADIUS servers. These wireless broadband locations and dial-up access numbers are integrated within the Qwest Mobility client directory and are updated automatically.

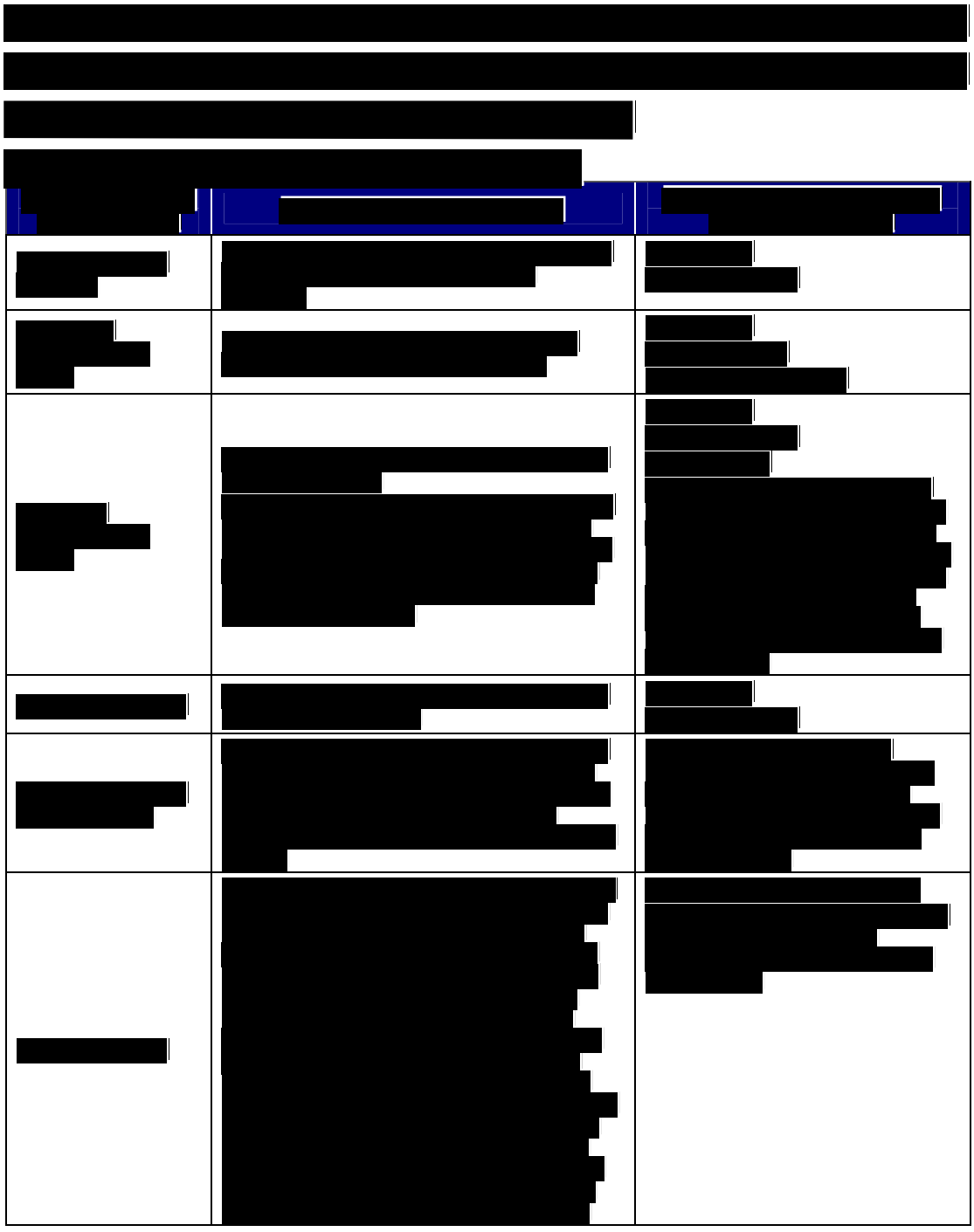
[redacted]

Depending on Agency security requirements, the service gives Agencies the option of selecting between three credentials identification protocols: Challenge/Handshake Authentication Protocol (CHAP), MS-CHAP V1, or Password Authentication Protocol (PAP) for authentication of all users of Qwest's global dial-up network.

[redacted]

Our Qwest Mobility client seamlessly integrates with a variety of AAA credential authentication methods, including User ID and Fixed Password, SecurID, and Safeword.

[redacted]



[redacted]

5.2.8.3.1.7 Management Utilities (Req_ID 33761), (C.2.12.1.1.4 (4) (b))

Qwest Mobility Administrative Access Overview

The service includes a secure, client configuration and management Web-based administrative portal called the Qwest Control Networx Portal. Through this Portal, Agency-authorized personnel can gain highly granular central configuration, management, and security policy enforcement of the Qwest Mobility client, the optional integrated VPN client, Agency personal firewall, or other software configurations. This software can be pushed out to specific groups of mobile, remote users in a manner specified and controlled by the Agency. This enables Agencies to hide remote system configuration complexities from users, reducing Agency support costs while ensuring machine compliance with the Agency security policy.

Authorized Agency personnel can use the Qwest Control Networx Portal to manage administrative requirements. [redacted]

[redacted]

5.2.8.3.1.8 Class of Service Capabilities (Req_ID 33762), (C.2.12.1.1.4 (4) (c))

Teleworkers using the TWS have access to multiple Classes of Service associated with the underlying transport services being used for the remote communication. [redacted]

5.2.8.3.1.9 Transmission of Multiple Protocols (Req_ID 33763), (C.2.12.1.1.4 (4) (d))

Qwest Mobility is an IP-centric service that enables transmission of any communication application data and application protocol that is normally seen in IP-based corporate Intranets or the Internet (e.g., Web server access, email, collaboration applications, and network folder access). [redacted]

5.2.8.3.1.10 Transmission of Multiple Protocols (Req_ID 33764), (C.2.12.1.1.4 (4) (e))

Qwest's TWS has the ability to provide multiple domains in which Qwest will provision the network to allow end-user authentication on the dial-up network and/or on alternate access supplier networks; this process is seamless to the end user. Each TWS end user will be assigned by Qwest a

Dynamic IP address for each unique authentication request on the dial network and/or Qwest supplier networks.

5.2.8.3.1.11 Delivery to Different Endpoint Devices (Req_ID 33765), (C.2.12.1.1.4 (5))

Qwest will provide the capability to deliver TWS to a variety of end-point devices using underlying network IP services, such as IP VPN, ISDN, Broadband, or Private Line. [redacted]

5.2.8.3.1.12 Training for Connection Maintenance (Req_ID 33772), (C.2.12.1.1.4 (6))

Qwest will provide a Qwest Mobility user guide and training for the teleworker on how to establish and maintain TWS connections. This training will be Web-based [redacted]

The service includes a user guide that explains how the teleworker can register in the portal, download the Qwest Mobility client, and access the directory (and all administrator-defined software, VPN client, and settings), as well as how to connect to the Internet and the Agency's VPN or Intranet via the various supported Internet access types. [redacted]

5.2.8.3.1.13 Compatibility with Agency Teleworker Applications and Client Software (Req_ID 33777), (C.2.12.1.1.4 (10))

Qwest TWS is backed by a highly trained team of Qwest pre-sales experts in application services. The Qwest team will work with the Agency to ensure the solution will support the teleworker applications and client software. Qwest Mobility is an IP-centric service that enables transmission of any IP-based communication application data and application protocol, such as MS Outlook/Exchange and IBM Lotus Notes, that is normally used in IP-

based corporate Intranets or the Internet. [redacted]

5.2.8.3.1.14 Managed Moves, Adds, and Changes Supports (Req_ID 33788), (C.2.12.1.2.1 (6))

The Qwest solution for moves, adds, and changes for TWS is supported by [redacted]. The service includes a 24x7x365 toll-free technical support number for any issue that may arise. Qwest's support personnel are dedicated exclusively to Remote Access end users. End users are supported around the clock to resolve any technical or service problem they may encounter (e.g., client software installation issues, unable to connect, can connect but not authenticate, unable to browse, experiences severe latency, or is disconnected abnormally).

[redacted]

5.2.8.3.1.15 Video Conferencing (Optional) (Req_ID 33797), (C.2.12.1.2.1 (8))

[redacted]

5.2.8.3.2 Satisfaction of Teleworking Service Features Requirements (L.34.1.5.4 (c), C.2.12.1.2.1)

[redacted]

[redacted]

Additionally, ***Figure 5.2.8-14*** summarizes the proposed Qwest service offering features that are available.

Qwest fully complies with all mandatory stipulated and narrative features requirements for TWS. The text in Figure 5.2.8-14 is intended to provide the technical description required per L.34.1.5.4(c) and does not limit or caveat Qwest's compliance in any way.

Figure 5.2.8-14. Qwest Technical Approach to TWS Service Features

ID/Name of Feature	Description	[redacted]
1. Anti-Virus Management	The contractor shall provide the capability to protect the TWS Agency and subscriber from a virus. Minimum capabilities include detection, notification, and removal of a virus.	[redacted]

ID/Name of Feature	Description	[redacted]
		[redacted]
2. Follow-Me Service [Optional]	The contractor shall provide the capability to route inbound calls (at a minimum, to three alternate numbers) with options for sequential or parallel routing to destination phone numbers (i.e., ring simultaneous phone numbers) or to voice mail. The subscriber will be able to manage a "find me list" and select any combination of different phone numbers in a user-defined search order to ensure delivery of important calls.	[redacted]
3. Instant Messaging [Optional]	The contractor shall provide Instant Messaging capabilities. Minimum requirements include providing: 1. Enable file transfer 2. Text chat 3. Presence information 4. Contact lists ("buddy and group lists") 5. User authorization	[redacted]
4. Intrusion Detection and Prevention	The contractor shall provide monitoring, attack recognition, and response to network security threats.	[redacted]

ID/Name of Feature	Description	[redacted]
5. Managed Firewall	The contractor shall provide a managed firewall service to protect the Agency network endpoint(s) from unauthorized inbound Internet-based intrusion.	[redacted]
6. Managed Moves, Adds, and Changes Support	The contractor shall provide management support and act as a single point of contact for Agency moves, adds, and changes with respect to TWS.	[redacted]
7. Teleworker Firewall	The contractor shall protect teleworkers' endpoint from unauthorized inbound Internet-based intrusion with anti-virus protection and filtering capabilities. The firewall is premises-based and located at the teleworker TWS endpoint.	[redacted]
8. Video Conferencing [Optional]	The contractor shall enable TWS subscribers to utilize point-to-point and multipoint desktop video conference capability.	[redacted]
9. Voice Mail [Optional]	The contractor shall provide a voice mail box, including voice messaging transmission, reception, and 24/7 storage except for periodic scheduled maintenance. The contractor shall provide the following minimum requirements: 1. At least thirty minutes of storage time (or 15 messages) 2. Ability to remotely access voice mail services	[redacted]

ID/Name of Feature	Description	[redacted]
	3. Secure access to voice mail via a password or PIN 4. Automatic notification when a message is received 5. Capability to record custom voice mail greetings 6. Call answering for a busy or "ring, no answer" condition	
10. Voice Service [Optional]	The contractor shall provide inbound and outbound voice calling capabilities with the following minimum capabilities: 1. Call Waiting 2. Caller ID 3. Caller ID Block (permanent or on a per call basis) 4. Three-Way Conference Call	[redacted]
11. Vulnerability Scanning [Optional]	The contractor shall provide real-time network scanning for potential entry points exposed to malicious attack through an automated scanning service that probes Internet-facing devices for vulnerability.	[redacted]

5.2.8.3.3 Satisfaction of Teleworking Service Interface Requirements (L.34.1.5.4 (c)), (C.2.12.1.3.1)

Qwest fully complies with all mandatory stipulated and narrative interface requirements for TWS. The following text is intended to provide the technical description required per L.34.1.5.4(c) and does not limit or caveat Qwest's compliance in any way.

Teleworking Service is an application-layer service that uses underlying network service(s) to transport traffic from the Service Delivery Points (SDPs) for teleworker endpoints such as the Agency data center or teleworker location. Qwest fully complies with mandatory (IP and VPN) and optional (VS and PLS) interfaces for the User-to-Network Interfaces (UNIs)

and SDPs for the respective services listed in the following RFP sections (where applicable):

1. C.2.2 Voice Services [Optional]
2. C.2.4 Internet Services
3. C.2.5.1 Private Line Services [Optional]
4. C.2.6.1 Combined Services [Optional– not proposed]
5. C.2.7 Virtual Private Network Services

5.2.8.3.3.1 Teleworking Services Interface Requirements (Req_ID 33810 to 33814), (C.2.12.1.3.1 (1 to 5))

[redacted] Please see the following subsections for UNI details by service.

1. Voice Services: 4.2.1 of Qwest's response.
2. Internet Protocol Services: 4.1.1.1.3.1 of Qwest's response.
3. Private Line Services: 4.2.5.3.1 of Qwest's response.
4. Combined Services: Qwest is not proposing this optional service.
5. Virtual Private Network Services:
    - NBIP-VPNs: 4.1.2.1.3.1 of Qwest's response.
    - PBIP-VPNs: 4.2.8.2 of Qwest's response.
    - L2IP-VPNs: 4.2.12.3 of Qwest's response.

5.2.8.4 Achieving Quality of Service Goals (L.34.1.5.4 (d))

In order to meet the time to restore requirement for TWS services, Qwest employs highly skilled, customer-focused engineers to respond to any outages. These resources use automated management tools that automatically notify necessary personnel in the event of an outage. The Qwest TWS Help Desk seamlessly interfaces with telecommunications NOCs and security services to ensure conformance to the Key Performance Indicator (KPI) and Acceptable Quality Level (AQL) measurements. ***Figure***

5.2.8-14a highlights Qwest's KPIs and performance thresholds. [redacted]

Figure 5.2.8-14a. Qwest TWS Service Goals.

Key Performance Indicator	Service Level	Performance Standard (Threshold)	Acceptable Quality Level	[redacted]
Time to Restore	Without Dispatch	4 hours	≤ 4 hours	[redacted]
	With Dispatch	8 hours	≤ 8 hours	[redacted]

5.2.8.5 Proposed Service Enhancements (L.34.1.5.4 (e))

[redacted]

[redacted]

5.2.8.6 Qwest Experience On Delivering Teleworking Services (L.34.1.5.4 (f))

[redacted]

5.2.8.7 Approach to Performance Verification (L.34.1.5.4 g)

Qwest deploys systems-monitoring tools to support performance verification for both Qwest's management systems and Qwest's network performance.

Management Systems: The Qwest Help Desk management systems provide reporting that facilitates management verification of performance for the TWS service.

Real-Time Reports: Enable supervisory viewing of personnel status and Help Desk queue information in a simple format. [redacted]

Analytical Historical Reporting: Analytical tools will be used to assess the historical performance of the contact center personnel to assist with long-term planning and contact center optimization. [redacted]

Network: [redacted] Network performance is tracked by [redacted] a series of automated online trend and Pareto charts [redacted]

We design and build Qwest's tools to drill down to Qwest's individual products and show detailed metrics. Within Qwest's scorecards, we show dozens of metrics, with results over several years for each product, to give a complete picture of performance over time.

[redacted]

5.2.8.8 Delivery Impact on Network Architecture (L.34.1.5.4 (h))

Qwest's TWS is in place and operating today. There is no need to modify our network to support Networx requirements.

5.2.8.9 Approach to Satisfying NS/EP Requirements (L.34.1.5.4 (i))

As defined in RFP Section C.5.2.2.1, TWS is not an NS/EP-impacted service. Qwest's overall support of the NS/EP requirements can be found in Section 3.5.1, and our NS/EP plan can be found in Appendix 2 in the technical volume.

5.2.8.10 Approach to Assured Service in the National Capital Region (L.34.1.5.4 (j))

Relevant to TWS, the Qwest Team has Operation Centers [redacted]

Each has redundant connections and provides exceptionally high levels of reliability and availability.

All bridging equipment is front-ended by multiple networks (ISDN and IP), which provide multiple layers of network redundancy. All network traffic is delivered to the facilities over three independent Synchronous Optical Network (SONET) rings.

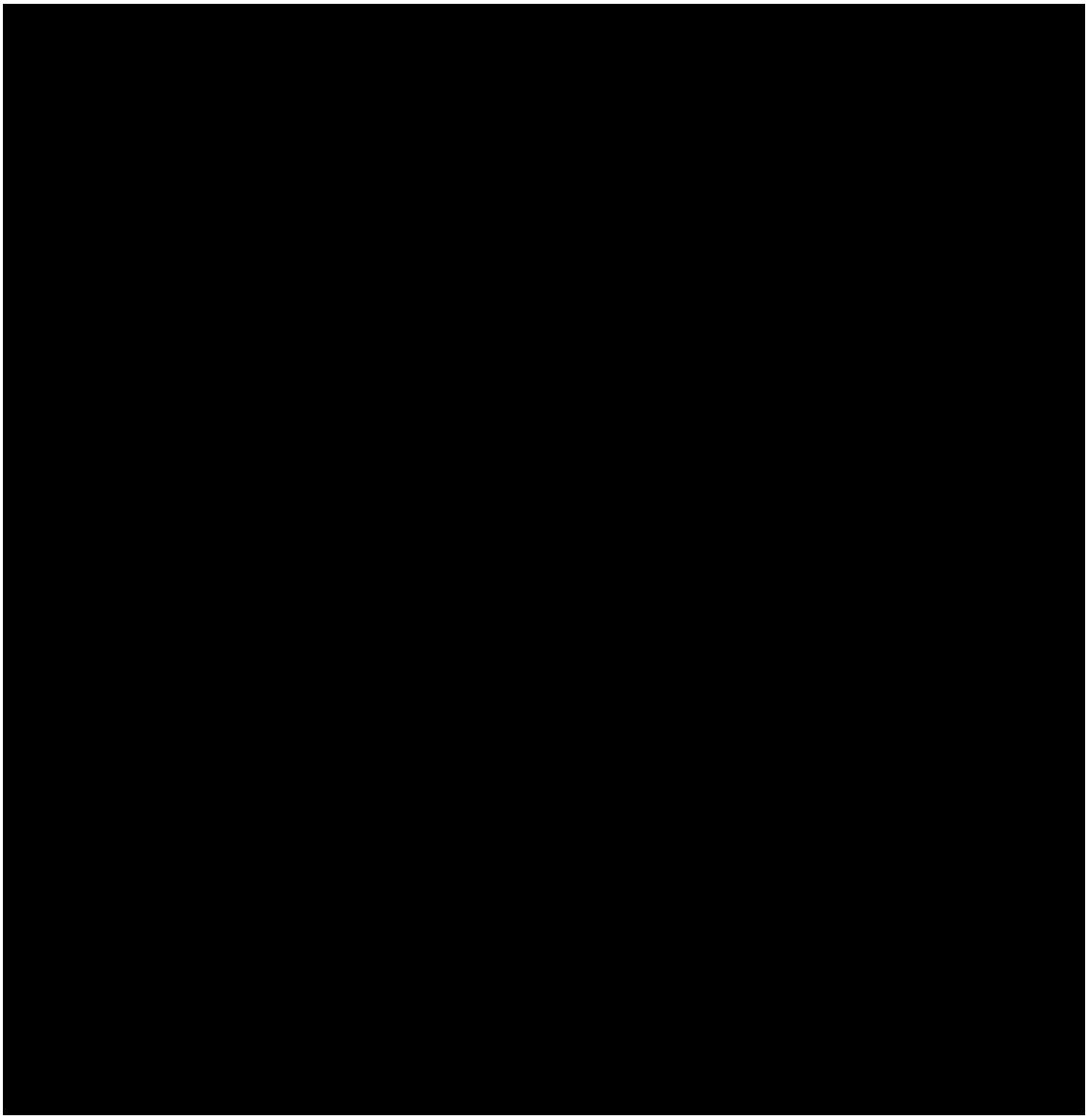
[redacted]

[redacted]

Qwest understands the Government's requirement to assure performance of network services in and around the NCR. To meet this important requirement, Qwest has established Point-of-Presence (POP) diversity in the NCR. [redacted] Each of these gateways provides complete redundancy to access Qwest nationwide and international network capabilities as well as regional voice and data services. Qwest also has a third provisioning POP [redacted] which serves both as an access POP, IP services node, and high-availability collocation and hosting center. Qwest has recently acquired OnFiber, a metro SONET and Ethernet provider with yet another diverse network in the NCR. This gives Qwest [redacted] regional fiber optic networks to use to ensure redundancy and survivability in the greater DC area.

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

[redacted]



Qwest's completely separate regional network connects [redacted] POPs in a route-diverse SONET-protected ring. This configuration enables these [redacted] 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.

[redacted] 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-protected ring 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.

To ensure the flow of voice services into and out of the NCR, Qwest connects to at least two ILEC access tandems. 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.

Qwest's Internet backbone is extremely well connected to other Internet Service Providers (ISPs). Qwest peers with the largest ISPs [redacted] private peering locations are 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. [redacted] As with other data services, Qwest can dual-

home critical peers as well as dual-homing critical Agency connections with complete route diversity to all of Qwest's data networking services to have complete resiliency from facility failures in the NCR.

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

5.2.8.11 Approach to Meeting Section 508 Provisions (L.34.1.5.4 (k))

Qwest's approach to meeting Section 508 criteria includes a range of activities to ensure ***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 products and services are 508 compliant, Qwest continues tests and evaluations with industry and specific assistive technology vendors to assess interoperability with TTY and assistive technology devices.

Qwest has enlisted a toll-free number for 24x7x365 access, 1-866-GSA-NETWorx (1-866-472-6389), to provide Agencies with direct access to our Customer Support Office (CSO), which will also be 508 compliant, enabling access by email, fax, TTY, TDD, 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 Qwest Networx customers.

As part of Qwest's Networx deliverables, [redacted] lists the Voluntary Product Accessibility Templates (VPATs) developed for each offered product and service applicable for Networx services as required.

[redacted]

The VPATs, including the relevant provisions of Subparts B, C, and D listed below in Figure 5.2.8-17, 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

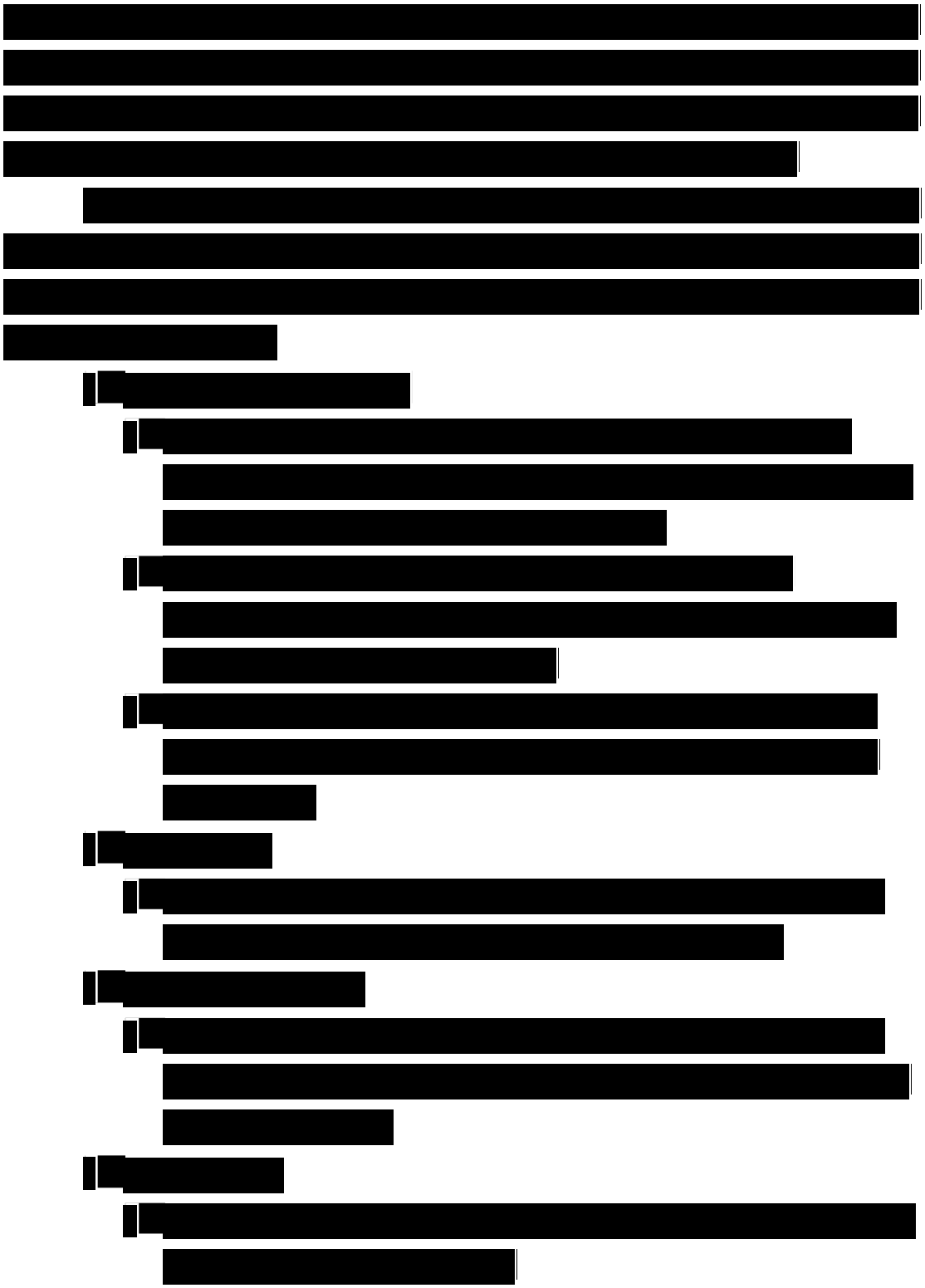
More information about how Qwest will maintain 508 compliance is located in Section 3.5.4, *Approach for Meeting Section 508 Provisions*, of this Technical Volume.

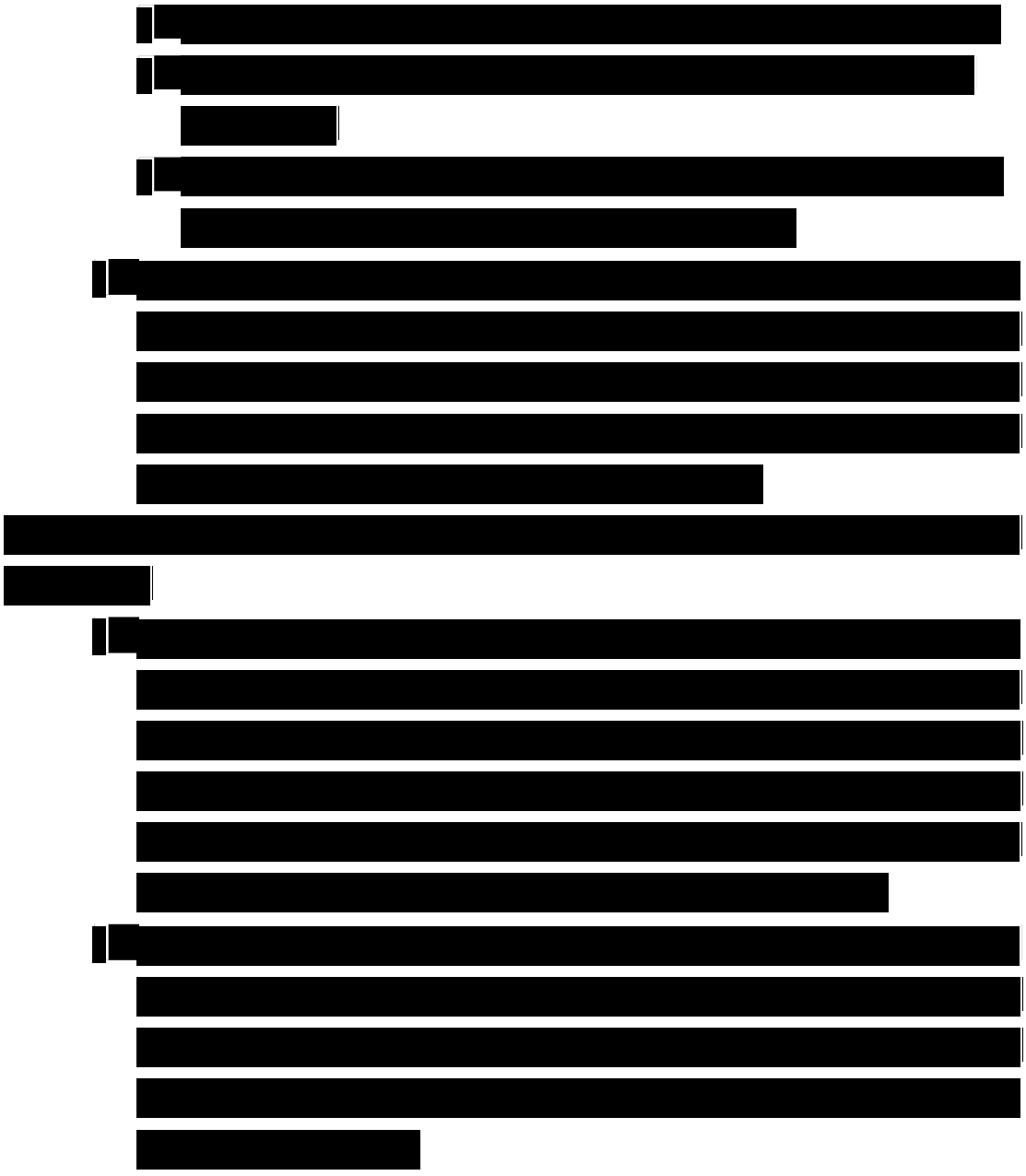
5.2.8.12 Approach to Incorporating Technological Enhancements and Improvements (L.34.1.5.4 (l))

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]





Today, most carriers use only dedicated circuits from ILECs and CLECs. The procedures for ordering, provisioning, and performing trouble resolution and repair are well-known and understood. However, the proliferation of new access methods, such as connecting to ILEC ATM and FR networks, shared Ethernet delivery, and xDSL for access, brings new

complexities to all of these processes. For example, in general, dedicated circuits either run clean or have errors that are generally automatically detected by carrier network equipment, with alarms and trouble tickets automatically generated. In the case of a Layer 2 access (for example, FR or Ethernet), there may be no traditional circuit problems, but congestion or problems in the local data network may occur. [redacted]