

5.0 MANAGEMENT AND APPLICATIONS SERVICES

5.1 MANAGEMENT AND APPLICATIONS-MANDATORY SERVICES

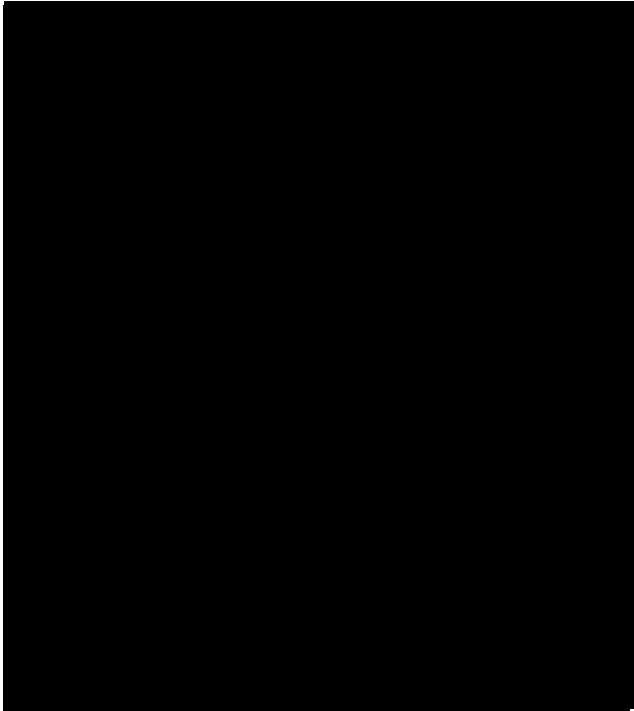
5.1.1 Managed Network Services (MNS) (L.34.1.5.1, M.2.1.4)

Qwest's Networkx Managed Network Services provides a comprehensive, integrated package of products and services that offers complete solutions for managing data, voice, and video networks.

Qwest provides a full-featured Managed Network Services (MNS) offering. Qwest's comprehensive MNS suite provides design, engineering, implementation, Operating System configuration management, fault management, real-time reporting, 24x7x365 monitoring, and total Agency coverage for Simple Network Management Protocol (SNMP) certified Service Enabling Devices (SEDs). Qwest's MNS is protocol and transport agnostic and is available to work in conjunction with all transport network types such as Intrusion Prevention System (IPS), Asynchronous Transfer Mode Service (ATMS), Frame Relay Service (FRS), Private Line Service (PLS), Premises-based IP Virtual Private Network Services (PBIP-VPNS), Network-Based IP VPN Services (NBIP-VPNS), Voice-over-IP (VoIP) Telecommunications Services (VOIPTS), Synchronous Optical Network Services (SONETS), and other services as needed where MNS-certified SEDs and/or Government Furnished Property (GFP) equipments are deployed. Qwest can also provide MNS across multiple carriers. [REDACTED]

[REDACTED] Qwest is committed to delivering reliability, rapid response, and quality restoration with built-in redundancy for all systems and platforms.

Qwest provides skilled MNS engineers to manage the health of the network, including design and engineering, implementation, and network management and maintenance components. Qwest MNS currently supports both domestic and international installations, including commercial and Government customers at the local, state, and federal levels.



5.1.1.1 Technical Approach to MNS Delivery (L.34.1.5.1, M.2.1.4 (b))

Qwest provides a comprehensive, integrated package of services that offers complete solutions for managing SNMP-enabled data, voice, and video networks. Qwest's MNS is backed by a highly skilled team of experts spanning end-to-end functions. MNS provides Agencies with a true Single Point of Contact (SPOC) for all technology management issues concerning an Agency's network. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Qwest's technical approach is based on established industry principles and standards such as the Open Systems Interconnect model; International Telecommunications Standardization Sector; Telecommunications Management Network; and Fault-Management, Configuration Management Accounting, Performance, and Security. Qwest relies on the Network

Reliability and Interoperability Council (NRIC) for best practices in planning and network management activities.

5.1.1.1.1 Approach to MNS Delivery (L.34.1.5.1 (a))

Qwest’s approach to service delivery includes the following foundation: geographically diverse Network Operation Centers (NOCs), state-of-the-art management tools, robust device management capabilities, security compliance, well established processes and procedures, and a highly skilled team.

Geographically Diverse NOCs: [REDACTED]

[REDACTED]

Qwest’s MNS includes 24x7x365 monitoring and notification. When the Element Management System detects a network fault, the NOC staff will be notified and will take timely remediation steps. [REDACTED]

[REDACTED]

Highly Skilled Team: The Qwest Team has both depth and breadth in designing, monitoring, managing, and troubleshooting networks. Qwest engineering and service support resources have extensive certifications and training to remain in the forefront of technology. Qwest engineers hold

extensive certifications, [REDACTED]
[REDACTED]

State-of-the-Art Management Tools: Qwest uses a suite of network management tools, as shown in **Figure 5.1.1-2**, to assure network performance that consistently meets Agency expectations.

Figure 5.1.1-2. Qwest MNS Tools



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

Qwest's Alarm and Trouble Ticketing Service uses industry-standard alarm thresholds. [REDACTED] If a threshold is violated, [REDACTED] trouble ticket will propagate to the

5.1.1.1.2 Benefits of MNS Technical Approach (L.34.1.5.1 (b))

From our years of experience managing emerging technologies, Qwest recognizes the value of preventing problems through lab testing, interoperability testing, configuration management, methods, and procedures.

Figure 5.1.1-4 summarizes the benefits of Qwest’s MNS. Qwest delivers MNS efficiently and confidently with considerable experience, skills, and proven processes to assure full Agency satisfaction.

Figure 5.1.1-4 Qwest MNS Features. *Qwest delivers MNS efficiently and confidently with considerable experience, skills, and proven processes to assure full Agency satisfaction.*

Features	[REDACTED]	[REDACTED]
Assigned Subject Matter Experts (SME) for Each Agency	[REDACTED]	[REDACTED]
Skilled Staff with Engineering Discipline and Bench Strength	[REDACTED]	[REDACTED]
Extensive Agency Experience	[REDACTED]	[REDACTED]
Solution Extensibility	[REDACTED]	[REDACTED]
Proactive Approach to Low-Level Performance Degradation Detection	[REDACTED]	[REDACTED]
Management of Multi-Carrier Networks	[REDACTED]	[REDACTED]
Qwest Control Network Portal	[REDACTED]	[REDACTED]

***Total Customer Agency** is a legal document signed by the customer giving Qwest the ability to work on the Agency’s behalf to resolve troubles with other

suppliers. It basically gives Qwest the authority of the Agency in resolving troubles.

Federal Enterprise Architecture (FEA) goals and the benefits of the Qwest MNS service are summarized in **Figure 5.1.1-5**.

Figure 5.1.1-5. Qwest’s MNS Solutions Meet FEA Objectives

FEA Goals	[REDACTED]
Improve Utilization of Government Information Resources	[REDACTED]
Enhance Cost Savings and Avoidance	[REDACTED]
Increase Cross-Agency and Inter-Government Collaboration	[REDACTED]

5.1.1.1.3 Solutions to MNS Problems (L.34.1.5.1 (c))

Qwest’s approach to MNS was developed with the knowledge that Agencies will have diverse environments that need to be managed under a unified framework. Successful MNS implementations must address the following three categories of problems shown in [REDACTED]

Figure 5.1.1-6. Qwest’s Solution to Potential Problems

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

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

5.1.1.2 Satisfaction of MNS Performance Requirements (L.34.1.5.2, M.2.1.4 (c))

Qwest meets the thresholds for all Key Performance Indicators (KPIs) with our MNS solution. The following sections further describe how Qwest monitors, measures, and validates performance against the Acceptable Quality Levels (AQLs) required for MNS.

5.1.1.2.1 MNS Quality of Service (L.34.1.5.2 (a))

Qwest’s performance is fully compliant with the Government’s requirement. **Figure 5.1.1-7** summarizes our support for MNS performance requirements.

Figure 5.1.1-7. Key Performance Indicators and Performance Standards

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	[REDACTED]
Availability (Network End-to-End)	Routine	99.9%	≥ 99.9%	[REDACTED]
Time to Restore (TTR)	Without Dispatch	4 hours	≤ 4 hours	[REDACTED]
	With Dispatch	8 hours	≤ 8 hours	[REDACTED]

The KPIs and Performance Standards are within our current intervals for TTR and Availability. [REDACTED]

[REDACTED]

The experience of the NOC staff in working with other carriers and network elements and repairing SEDs, along with the knowledge gained from managing the Agency’s Network, allows us to reduce the confusion and enhance accountability regardless of the problem.

5.1.1.2.2 Approach for Monitoring and Measuring MNS (L.34.1.5.2 (b))

Implementation Management and Maintenance: Qwest will provide fully integrated management and maintenance for Agencies including access, transport, SEDs, and security management. In the following sub-sections, we described our integrated approach.

Continuous Network Monitoring: Qwest MNS engineers and systems monitor Agency networks 24x7x365 to ensure optimum performance and to quickly detect, isolate, and repair faults using SNMP and device Management Information Base (MIB) data. This information will be available to the Agency as actionable trouble tickets, reports, etc. or as raw trap and polling information. [REDACTED]

[REDACTED] All of this data is correlated, filtered, and analyzed automatically. [REDACTED]

The first step in monitoring Agencies' networks is to collect or capture the management data stored in the devices. The stored data/values are then used in the following ways:

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Filtering and Correlation: MNS uses filters to look at a single source of Network Management Information (NMI), such as a router, switch, server, or application agent. Filtering rules are applied to check for thresholds, amounts of change, or other factors. [REDACTED]

[REDACTED]

Configuration Management: Configuration Management encompasses the provisioning process and the configuration fault management process. These processes ensure configuration integrity for the Agency. [REDACTED]

[REDACTED]

Qwest will also manage all IP address and schemas across the Agency's network [REDACTED]

[REDACTED]

Qwest will make changes to the configuration on an Agency device as specified by the Agency. The changed configuration will be developed by Qwest based on information provided by the Agency.

Configuration Fault Management: Qwest protects Agencies against configuration corruption and unwanted/unauthorized configuration changes by routinely backing up device configurations. On a daily basis, [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

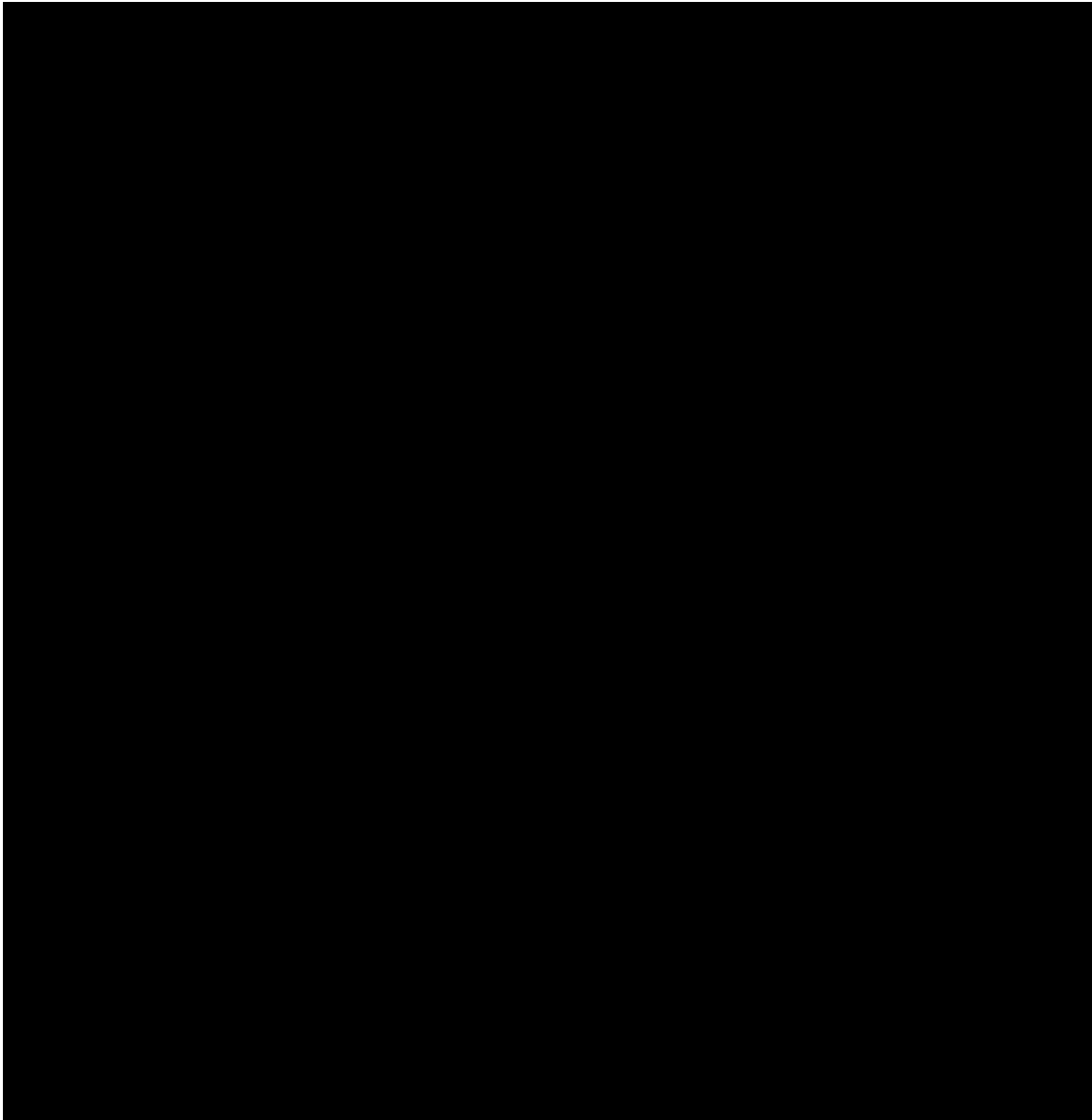
[REDACTED]

[REDACTED] Qwest will identify and alert MNS engineers of any configuration changes. Once a new configuration is validated, it will replace the previously stored configuration.

Qwest will restore previous device configuration states as required. If the current configuration is lost due to hardware failure, we will restore the previous configuration. We always store a copy of the “last known good configuration” for a device.

If a network issue is caused by requested configuration provisioning activities, Qwest will restore the previous configuration to the device. MNS engineers will work with the Agency to analyze the consequences of a requested configuration change.

[REDACTED] details the process used for configuration fault management.



Online Reporting: Qwest provides a full suite of reporting capabilities to Agencies using industry-leading reporting platforms. Network reports are automated and available via the Qwest Control Network Portal. Qwest MNS engineers also use these reports to evaluate the performance of Agency networks. Reports are organized from a high level view of a network down to the smallest component, thus providing the varied level of detail required by the Agency.

Standard Reports: Qwest will provide real-time access to Network

[REDACTED]

[REDACTED] In addition to this information, Qwest will also provide the following standard reports to all Agencies:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Standard Router/Switch Reports

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Qwest MNS supports industry-standard SNMP devices. This “open” design allows the Agency maximum flexibility when implementing Qwest MNS. Qwest MNS will comply with the specific standards and recommendations identified in the Agency Task Order. Additionally, Qwest

MNS will comply with all appropriate standards for any underlying Network access and transport service.

Network Profiling: The inventory database, topology maps, and drawings are available online and are updated each time there is a change in the network. Changes include adding, moving, or removing a device from MNS; the addition or removal of a connection or protocol (interface or sub-interface); and changes in device or connection information, such as IP addressing, bandwidth, filtering, and traffic prioritization schemes. [REDACTED]

[REDACTED]

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

5.1.1.2.3 Verification of MNS (L.34.1.5.2 (c))

Data Integrity Analysis: Qwest has procedures in place to ensure that the source data and the repository of source data are protected through restricted access and redundant databases. [REDACTED]

[REDACTED]

[REDACTED]

Root Cause Assessment: Any time a breach of any of the performance levels Qwest measures occurs, Qwest will review and determine

the root cause for the issue and document the findings in a Reason For Outage report. [REDACTED]

[REDACTED] Utilizing our proven carrier grade tools and engineering capabilities, Qwest ensures that performance is restored and proactive preventative actions are taken.

Resolution: Once an alarm has broken an established performance threshold, system initiated tests will be performed to identify where the trouble ticket should be routed (e.g., SED support, Network Support, etc.). [REDACTED]

[REDACTED] Once prioritized, the trouble ticket is sent to an engineer for resolution action. Once we execute on the resolution path and corrective action is completed and performance measures have stabilized and returned to service levels acceptable to the Agency, then the trouble ticket will be closed.

5.1.1.2.4 MNS Performance Level Improvements (L.34.1.5.2 (d))

5.1.1.2.5 Additional MNS Performance Metrics (L.34.1.5.2 (e))

5.1.1.3 Satisfaction of MNS Specifications (L.34.1.5.3, M.2.1.4 (d))

Qwest's MNS solution is designed to take advantage of the various efficiencies created by the development and implementation of a uniform service delivery approach. Qwest acknowledges that Agencies may require customized elements in the service delivery process to accommodate special considerations of the Agency's network or internal communication needs. The following sections detail Qwest's technical approach to meeting MNS requirements, including our demonstrated ability to offer MNS.

In reference to standards, Qwest MNS service will comply with all applicable standards, as current MNS offerings have been operating across multiple carriers and technologies [REDACTED] providing a comprehensive view on the networks operations.

In reference to connectivity, Qwest MNS will be available on all underlying Network offerings, as service is currently provided on all of the listed Network offerings in the retail marketplace.

5.1.1.3.1 MNS Service Requirements (L.34.1.5.3 (a))

Qwest’s MNS provides a broad range of design, engineering, implementation, monitoring, proactive troubleshooting, and reporting capabilities, including the software tools used to enable the MNS NOC to monitor multi-carrier access, transport components, and CPE. Qwest has provided this service to commercial, state, local, and Federal Government customers [REDACTED]. Qwest currently manages customer networks located around the world [REDACTED]. The networks managed are multi-carrier, multi-technology, and multi-topology.

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

[REDACTED] This is carrier-grade network management for the Agency.

5.1.1.3.1.1 Satisfaction of MNS Capability Requirements (L.34.1.5.3 (a), C.2.9.1.1.4)

Figure 5.1.1-9 identifies all the MNS-required capabilities and Qwest’s Technical approach. Qwest fully complies with all mandatory stipulated and narrative capabilities requirements for MNS. The text in Figure 5.1.1-9

provides the technical description required per L.34.1.5.3(a) and does not limit or caveat Qwest’s compliance in any way.

Figure 5.1.1-9 MNS Technical Capabilities and Qwest’s Approach

ID	Capability	[REDACTED]
<i>Design & Engineering</i>	<p>1. The contractor shall provide design and engineering services that fully satisfy Agency requirements. Design and engineering services include a review of the current network traffic, performance, transport, hardware and software components, and an overall evaluation of network topology, configuration, addressing, bandwidth, availability, scalability, reliability, and disaster recovery requirements. The contractor shall document the design and engineering services. The contractor shall also review the design and engineering services that have been implemented to ensure that ongoing Agency needs are satisfied.</p>	<p>[REDACTED]</p>
	<p>2. The contractor shall incorporate the Agency’s security requirements into the design to ensure that all factors influencing data and circuit integrity are captured. This may include the integration of a security package or individual Networkx security services.</p>	<p>[REDACTED]</p>
	<p>3. The contractor shall identify network components and determine protocols, redundancy, traffic filtering, and traffic prioritization requirements. The contractor shall also recommend the appropriate CIRs, PVC levels, and network access speeds, as required.</p>	<p>[REDACTED]</p>

ID	Capability	
	<p>4. The contractor shall provide complete project management including design, implementation, installation, access coordination, provisioning, equipment configuration, hardware testing, and service activation. The contractor shall coordinate installation activities with the Agency in order to minimize the impact on the current networking environment.</p>	<p>[REDACTED]</p>
<p>Implementation, Management & Maintenance</p>	<p>1. The contractor shall provide integrated management of services to the extent needed by the Agency—that includes managing services that are delivered to the Agency by other contractors.</p>	<p>[REDACTED]</p>
	<p>2. The contractor shall develop, implement, and manage comprehensive solutions constructed from components of the Network services and their enhancements in order to meet Agency-specific requirements. The solutions shall include but not be limited to:</p> <p>a. Access solutions that use a combination of different services, such as Wireline and Wireless Access Services, for specific Agency locations, and also Satellite Access Arrangements at particular locations to meet Agency performance metrics for availability and disaster recovery</p>	<p>[REDACTED]</p>
	<p>2.b. Transport solutions that distribute traffic over multiple contractor backbone networks to provide redundancy and carrier diversity, and vary the traffic allocation dynamically based on Agency-specified performance requirements</p>	<p>[REDACTED]</p>

ID	Capability	
	2.c. Customer premises solutions that provide Agency-specific interfaces, software, and equipment to meet Agency requirements	[REDACTED]
	2.d. Security Solutions as required by the Agency	[REDACTED]
	3. The contractor shall supply and manage the hardware, firmware, and related software required by the Agency. Components include but are not limited to routers and switches, ATM devices, CSUs/DSUs, hubs, ISDN adapters, and modems.	[REDACTED]
	4. The contractor shall manage the network in real-time on a 24x7x365 basis. The contractor shall support remote management capabilities from its operations center, including but not limited to equipment configuration, testing, monitoring, troubleshooting, fault/problem resolution, and maintenance. The contractor shall proactively monitor utilization and packet loss and errors, probing in intervals of at least fifteen minutes to ensure proper equipment/network operation and performance.	[REDACTED]
	5. The contractor shall support SNMP data feeds that provide the Agency with managed equipment information, as applicable.	[REDACTED]

ID	Capability	[REDACTED]
	6. The contractor shall perform configuration changes that include but are not limited to the following: <ul style="list-style-type: none"> a. Adding a protocol b. Adding, moving or removing CPE c. Changing addressing, filtering, and traffic prioritization schemes d. Modifying PVCs e. Optimizing network routes f. Updating equipment software and/or configuration, including but not limited to firewall and VPN security devices g. Upgrading or downgrading bandwidth 	[REDACTED]
	7. The contractor shall provide IP Address Management as applicable. The contractor shall supply registered IP addresses to the Agency as required and assist in the translation of non-registered private IP addresses into public addresses for routing purposes.	[REDACTED]
	8. The contractor shall monitor and control access to equipment under its control including limiting access to authorized personnel and implementing passwords and user permissions as directed and approved by the Agency.	[REDACTED]
	9. The contractor shall regularly perform off-site equipment configuration backups in order to ensure the availability of recent configuration data for restoration purposes. The contractor shall provide the Agency secure access to backup logs as needed.	[REDACTED]
	10. The contractor shall perform the necessary hardware and software upgrades, updates, patch deployments, and bug fixes as soon as they become available. The contractor shall implement updates in coordination and mutual agreement with the Agency and test new releases to resolve any security concerns, ensure compatibility with the Agency environment, minimize service disruptions, and maintain equipment functionality.	[REDACTED]

ID	Capability	[REDACTED]
	11. The contractor shall proactively detect problems, respond to alerts, and promptly report situations that adversely affect throughput to the impacted Agency. The contractor shall provide notification of alarms, network troubles, and service interruptions via email, pager, telephone, or as directed by the Agency.	[REDACTED]
	12. The contractor shall provide the Agency with real-time access to the following: <ul style="list-style-type: none"> a. Installation schedule detailing the progress of activities such as the implementation of equipment, access and transport circuits, ports, and PVCs, as applicable. This allows Agencies to track the provisioning process through completion at any time. Near real-time access to the installation schedule is acceptable b. Network statistics and performance information including equipment data, availability, throughput and delay statistics, Class of Service settings, and application-level performance information, as applicable c. Trouble reporting and ticket tracking tools d. Security logs 	[REDACTED]

5.1.1.3.1.2 Satisfaction of MNS Feature Requirements (L.34.1.5.3 (a), C.2.9.1.2)

Figure 5.1.1-10 identifies all the MNS-required features and Qwest’s Technical approach. Qwest fully complies with all mandatory stipulated and narrative feature requirements for MNS. The text in Figure 5.1.1-10 provides the technical description required per L.34.1.5.3(a) and does not limit or caveat Qwest’s compliance in any way.

Figure 5.1.1-10 MNS Features and Qwest’s Approach

ID#	Feature	
1	Government Furnished Property (GFP) Maintenance	[REDACTED]
2	Agency-Specific Network Operations Center (NOC)	[REDACTED]
3	Network Testing	[REDACTED]

5.1.1.3.1.3 Satisfaction of MNS Interface Requirements (L.34.1.5.3 (a), C.2.9.1.3)

Figure 5.1.1-11 identifies all the MNS-required interface requirements and Qwest’s Technical approach. Qwest fully complies with all mandatory stipulated and narrative interface requirements for MNS. The text in Figure 5.1.1-11 provides the technical description required per L.34.1.5.3(a) and does not limit or caveat Qwest’s compliance in any way.

Figure 5.1.1-11 MNS Interface and Qwest’s Approach

ID#	UNI Interface Type	[REDACTED]
1	C.2.3.1 Frame Relay Service [Optional]	[REDACTED]
2	C.2.3.2 Asynchronous Transfer Mode Service [Optional]	[REDACTED]
3	C.2.5.1 Private Line Services [Optional]	[REDACTED]
4	C.2.4.1 Internet Protocol Service [Optiona]	[REDACTED]
5	C.2.7.2 Premises-Based IP VPN Services [Optional]	[REDACTED]
6	C.2.7.3 Network-Based IP VPN Services [Optional]	[REDACTED]

5.1.1.3.2 Proposed Enhancements for MNS (L.34.1.5.3 (b))

[REDACTED]

5.1.1.3.3 Network Modifications for MNS Delivery (L.34.1.5.3 (c))

[REDACTED]

5.1.1.3.4 Experience Delivering MNS (L.34.1.5.3 (d))

Qwest brings decades of data network management experience—
[REDACTED] providing direct MNS for complex customer
environments—utilizing carrier grade tools, platforms, and expertise. [REDACTED]

[REDACTED]

[REDACTED] Qwest manages the transport, routers, switches, and
firewalls located at a variety of sites, including a corporate data center,
disaster recovery facility, supplier sites, and field offices. The network
architecture is based on a VPN hub-and-spoke design with full backup
capability for the main data center. Qwest MNS maintains the complete
inventory and network maps for the network, full configuration management,
and 24x7x365 in-band monitoring and fault management. In support of these
services, Qwest MNS provides online documentation, real-time reporting, and
comprehensive monthly reporting of network performance.

5.1.1.3.5 MNS Approach (L.34.1.5.3 (e))

MNS is provided by the dedicated Federal NOCs [REDACTED]
[REDACTED] which meet all Networkx security and disaster recovery
requirements. Refer to Figure 5.1.1-9, which includes the disaster recovery
out-of-band access requirements.

Design and Engineering: [REDACTED]

[REDACTED]

[REDACTED]

Implementation: Day 1 Services (Install/Turn Up) – Once complete, the SPOC will assist the Agency in formalizing the required documentation needed for the ordering and provisioning on the required services. Any additional information captured from the discovery meeting will be included in the documents, in addition to contact hierarchy for maintenance issues, device locations, IP, or other network-specific addressing schemes. Once all the documentation has been completed, the SPOC will submit the implementation information to the MNS NOC for order processing. The associated order tracking IDs will then be sent to the SPOC in order to

facilitate the order tracking and subsequent order status monitoring with the designated contact(s) within the Agency. [REDACTED]

[REDACTED]

Management and Maintenance: Subsequent to the SOCN, the MNS NOC will closely monitor the network for fine tuning and modifications that might not have been detected within the previous network management framework. [REDACTED]

[REDACTED]

5.1.1.4 ICB CLIN and Case Numbers

Table 5.1.1.4-1 Table of ICB CLINs and Case Numbers

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

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

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]