3.13 OPERATIONAL SUPPORT SYSTEMS (L.34.2.3.13) (M.3.10)

The Government requires a contractor with a reliable set of systems and processes that will fully support the management and fulfillment of day-to-day Networx operations. Qwest's Networx Control Portal will allow GSA and the Agencies insight into our dependable Operational Support Systems (OSS) via Web-based secure access.

3.13.1 Understanding of the Requirement

Qwest will support the Networx program with a comprehensive and secure Operational Support System (OSS) that performs a wide range of integrated functions including billing, service ordering, customer support, service management, inventory management, training and program management. Our Networx OSS, described in detail throughout the Management Volume of this proposal, supports the full range of requirements. [redacted]

Simplicity of access has been a development design principle of Qwest Control Networx Portal which is the front door to our integrated OSS.

Qwest has successfully implemented the customer focused strategy by establishing innovative Web-based interfaces to our legacy systems. This approach allows Qwest to maintain a superior level of service through utilization of legacy systems, while simultaneously presenting customers with intuitive, user-friendly Web interfaces to access the information they require.

The integration of Qwest legacy systems is well-understood, time tested and documented as a result of years of investing in architecture enhancements and technology upgrades. The synergistic relationship between legacy systems and customer portals enables integrated visibility into our OSS.

Qwest continues to make significant investments in customer-driven portals for automation of front end processes, which the Qwest Control Networx Portal best illustrates. Qwest Control Networx Portal enables Government users to manage telecommunications services end-to-end through a simple and easy to use interface. Through the Qwest Control Networx Portal [redacted] users can: derive price quotes; order products and services; view provisioning steps; review, accept or dispute billing; view network management statistics; initiate and manage trouble tickets and complaints; view and query inventory; and format and request standard and ad hoc reporting against the Networx database, fully meeting all the OSS requirements of the Networx RFP. Qwest is attuned to the Government users' specific needs, supporting their business requirements by upgrading and improving the OSS through processes that include [redacted]

Qwest OSS consists of [redacted] systems that support commercial and Government customers today. [redacted]

The Qwest Control Networx Portal provides access to the back-end OSS. All Networx products and services can be ordered via the Portal [redacted]

The Qwest Control Networx Portal is ideally suited to accept and acknowledge all orders, present invoices, accept and track bill disputes, report on inventory data, provide robust reporting from database elements, proactively monitor Government networks, and report and track trouble tickets and complaints according to the requirements of the Networx contract. The simple yet comprehensive nature of the Qwest Control Networx Portal means that Government users have a one-stop shop for their telecommunications management requirements, saving time and maximizing productivity for the Government.

3.13.1.1 Responses to Narrative Requirements Table

3.13.1.1.1 General Narrative Requirements

Section 3.13.1.1.1, General Narrative Requirements, and Section 3.13.1.1.2, Specific Narrative Requirements, identify RFP requirements and associated proposal response locations.

Comp_ req_id	RFP Section	RFP Requirement	Proposal Response
107	C.3.9.2.1	The contractor shall ensure security requirements are met for all automated operational support systems, and shall support Government certification and accreditation of the system via services such as Managed Tier Security Service, Customer Specific Design and Engineering Services, or other services the Government may order to achieve this. The security requirements are defined in Section C.3.3.2, Security Management, and include, at a minimum, security controls for low impact systems as defined in NIST SP 800-53, Annex 1.	Section 3.13.4.1.1
106	C.3.9.2.1	The contractor shall descr be its methods for securing these systems as part of the overall Security Plan.	Section 3.13.4.1.2 Appendix 2
100	C.3.9.2.1	Each system shall meet the requirements addressed elsewhere in this contract such as security management, fault management, and trouble handling.	Section 3.13.4.1.3 Appendix 2
84	C.3.9.2.3	The contractor shall deliver an OSS Change Management Plan.	Section 3.13.5.1.1 Appendix 6
83	C.3.9.2.3	1. The OSS change management requirements shall include, at a minimum, how the contractor will conduct the following: 1.1 Informing the Government when OSS design changes are planned and when maintenance changes are required 1.2 Managing and controlling OSS changes 1.3 Incorporating Government review and approval by the Government into the contractor's change management process 1.4 Government training, if required by the changes 1.5 Retesting with the Government to ensure functionality of any impacted interface.	Section 3.13.5.1.2 Appendix 5 Appendix 6

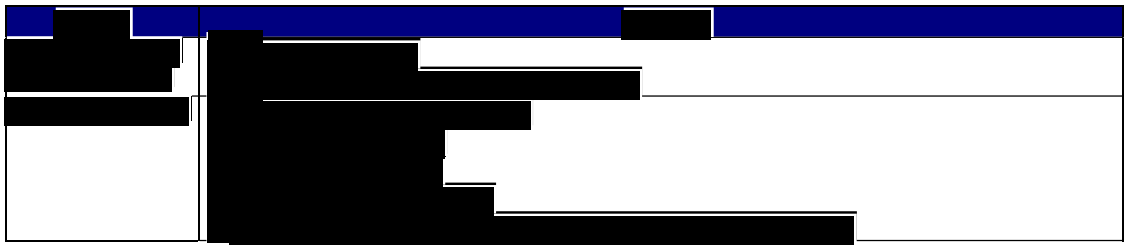
3.13.1.1.2 Specific Narrative Requirements

Comp_req_id	RFP Section	RFP Requirement	Proposal Response
98	C.3.9.2.2	The contractor shall provide an OSS Verification Test Plan, in accordance with Section E, Inspection and Acceptance at contract award.	Section 3.13.3.1.1 Appendix 5
1134	E.2	The contractor shall develop and execute a Networx Services Verification Test Plan to verify that the services delivered under the contract meet the requirements of Section E.4, Verification and Acceptance Testing of Networx Services, and shall develop and execute an OSS Verification Test Plan to verify that its OSS meets the requirements of Section E.3, Verification Testing of the Contractor's Operational Support Systems.	Section 3.13.3.3 Appendix 5
1132	E.2.1	The contractor shall prepare an OSS Verification Test Plan in accordance with the requirements of Section C.3.9, Operational Support Systems, and Section E.3, OSS Verification Testing of the Contractor's Operational Support Systems.	Section 3.13.3.1.2 Appendix 5
8056	E.2.1	The contractor shall update the OSS Verification Test Plan when a new service is offered or when an OSS is changed.	Section 3.13.3.1.3 Appendix 6
1127	E.3	'The test cases that the contractor shall execute acceptably include those listed in Table E.3.1.	Section 3.13.3.1.4
1126	E.3	The contractor shall demonstrate acceptable performance using one of the following electronic media: Internet secure access, electronic mail, or electronic file transfer.	Section 3.13.3.1.5 Appendix 59

3.13.2 System Capabilities including Delivery Methods (M.3.10(c))

The Qwest Control Networx Portal provides a broad range of online tools that enable the Agency user to manage their Qwest services. [redacted] These features within the Portal will be ready at NTP including order management, repair, reporting, Managed Network Services/ Managed Security Services, portal administration, inventory, and billing. These features have already been released into the production environment.

[redacted]



3.13.2.1 Qwest Control Networx Portal: A Complete Qwest System

The Qwest Control Networx Portal provides the convenience of allowing Government staff to view the service life cycle from quoting through acceptance and continuing through service performance management [redacted] The Portal provides quotes and is the vehicle for submitting service orders into our ordering system. Confirmed service orders are provisioned via our network provisioning systems. After provisioning is completed and the customer accepts the service, invoicing is performed by our billing system. Network Management, including alarming and remote polling, is accomplished using our network management system. All Qwest trouble and complaint reporting is captured and resolved using our

trouble ticketing system.

In addition to all of these functional systems, the Networx inventory system replicates and stores Networx-specific data for easy access and reporting, including inventory information using the Qwest reporting tool, is where users can run standard reports or can create ad hoc reports through custom queries of inventory. The Qwest reporting tool is also used for correlation of Service Order Completion Notices (SOCN) to both the inventory and billing, providing the Government an easy method to validate services ordered against inventory and billing. Flexible reporting makes the service and performance management process simple, efficient and enables higher productivity levels among Government staff.

OSS Architecture and Integration

[redacted]

ordering, provisioning, inventory, billing, reporting, etc. [redacted]

[redacted]

[redacted]

[redacted]

Portal users are created at an “Enterprise” level which equates to an Agency. This assignment serves as the first domain restriction of the content to which they have authorized access. A GSA Administrator-level user can also be created to provide a contract-wide portal content access capability. Portal users may also be assigned roles and role levels (Basic, Advanced, and Administrative) for functional capabilities such as billing, ordering, inventory, etc. that will drive what “tabs” are made available to the user in the interface. [redacted]

[redacted]

[redacted]

Service, Pricing, and CLIN Definitions

[redacted]. The services are constructed to fit the structure and features required by the Networx RFP [redacted]. For instance, ATM service will require a loop, PVC and port. [redacted]

[redacted]

[redacted]

[redacted]

The accuracy and completeness of reporting on the services and associated SLAs is ensured by the data integrity inherent to the constructs and systems leveraged to provide the Networx OSS [redacted]

[redacted]

3.13.2.2 Delivery Methods

Agencies can pull reports from the Qwest Control Networx Portal in virtually any format, depending on their business requirements. Qwest has a comprehensive set of tools and applications for the delivery of data, including Internet Secure Access, SMTP, FTP, e-mail, CD-ROM, U.S. Postal Service, Facsimile. The reports can be provided in the following formats to include: CSV, ASCII Text Tab Delimited, ASCII text fixed record, XML, or other formats as mutually agreed between the Government and Qwest. Additionally, Qwest's robust ad hoc reporting allows the user to discover trends using filters, sorting and grouping of queried data to produce custom formatted data available via any of these delivery methods. Multiple data formats for real-time reports and user-defined queries for ad hoc reports make the Qwest Control Networx Portal flexible and easy to use.

3.13.3 Verification Testing (L.34.2.3.13.1) (M.3.10(d))

3.13.3.1 OSS Verification Test Plan Approach

Qwest's OSS verification testing approach complies with all Networx requirements as stated in the RFP. The narrative requirements are detailed in the following sections. More information on Qwest's approach can be found in Appendix 5, Operational Support Systems Verification Test Plan.

3.13.3.1.1 OSS Verification Test Plan (comp_req_id 98)

Qwest will complete the OSS Verification Testing process according to the OSS Verification Test Plan (See Appendix 5) within 60 calendar days of Notice to Proceed (NTP) or within 60 calendar days after Government approval of the test plan, whichever is later as required in Section C.3.9.2.2 and in accordance with Section E of the RFP. Please see Appendix 5, OSS Verification Test Plan.

3.13.3.1.2 Accordance with C.3.9 Requirements (comp_req_id 1132)

Refer to Appendix 5, OSS Verification Test Plan, for correlation to the Requirements of Section C.3.9, Operational Support Systems and Section E.3, OSS Verification Testing.

3.13.3.1.3 OSS Verification Test Plan Update (comp_req_id 8056)

Qwest will update our OSS Verification Test Plan when new services are offered or when an OSS is changed in accordance to RFP Section E.2.1.

3.13.3.1.4 Test Cases (comp_req_id 1127)

Refer to Appendix 5, OSS Verification Test Plan, Attachments 1-6, for evaluation criteria. A complete description of each of the six Government specified test cases and how they apply to all services offered by Qwest is provided. These six test cases include Test Case #1, Ordering Testing, which will test all services. All the test cases listed in Table E.3.1 will be acceptably executed by Qwest.

3.13.3.1.5 Standard Test Procedures (comp_req_id 1126)

Qwest will communicate and demonstrate acceptable performance for all verification testing results, including data in all GSA requested records as identified in Section J.12, via Internet secure access, electronic mail, or electronic file transfer, as required by GSA.

3.13.3.2 OSS Verification Test Plan Requirements

Qwest's OSS verification testing approach complies with all Networx requirements as stated in the RFP. How Qwest meets Networx requirements is detailed in the following sections. More information on Qwest's approach can be found in Appendix 5, Operational Support Systems Verification Test Plan.

3.13.3.2.1 Completeness and Consistency of Plan (L.34.2.3.13.1(a))

Following best commercial practices, the Qwest Networx OSS is subject to testing in accordance with defined criteria for completeness and consistency. The acceptance criteria define the necessary outcomes for successful testing evaluation.

Completeness, defined by verification testing, takes into account specific requirements of the Networx program and internal Qwest systems. Completeness is achieved by demonstrating the ability to process a full range of orders (i.e. all service and all order types) from order receipt to ordering invoicing and adjustments. In doing so the test will invoke all applicable Qwest OSSs. OSS Verification Testing defines what is to be tested in a contextual basis by defining objectives, requirements, functional specifications, validations and acceptance criteria.

[redacted]

Completeness and consistency are reflected in the many types of testing Qwest performs. [redacted]

3.13.3.2.*2* Testing Approach (L.34.2.3.13.1(b))

Qwest's testing approach supports completion of testing within 60 calendar days from the NTP or the date GSA approves its OSS Verification Test Plan (whichever is later). [redacted] Qwest will support the Government and ordering Agency in

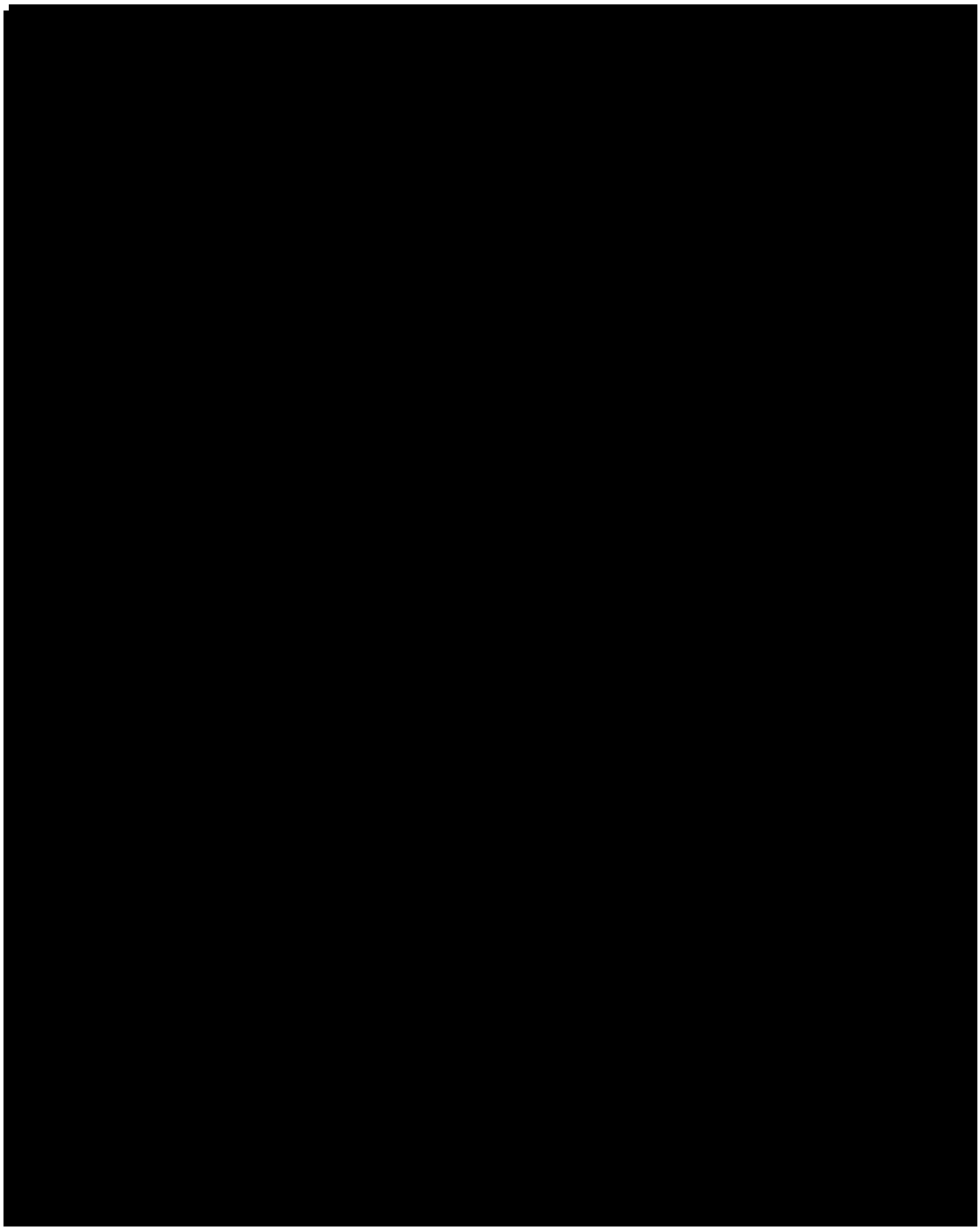
observing or having a representative observe all or any part of the verification testing. The Government may also directly participate in the execution of the tests at this location by electing to execute all or some of the test cases themselves. The Qwest Contract Program Office (CPO) will provide the Government with periodic reporting of testing activities, and can arrange for Government staff to gain access to the testing area. Qwest's encouragement of Government involvement in the testing process, and the transparency with which it reports testing activities is part of our goal of providing excellent customer service.

Please see [redacted] for the initial OSS Verification Testing schedule.

3.13.3.2.3 Effective and Timely Testing (L.34.2.3.13.1(c))

Qwest consistently conducts effective and timely testing for new functionality or services. Before testing begins, test steps are defined according to the OSS Verification Test Plan for each type of order and action executed by the user. The Government will approve the individual tests to be executed and verify the results of the tests performed. Evaluation of each action will receive a pass or fail status as measured by the expected output defined for each action in each test [redacted] Qwest and the Government to complete all testing and review within the 60-day schedule requirement.

Each time a new service or enhanced functionality is built for Networx ordering, Qwest will execute on the OSS Verification Test Plan and report results to the Government prior to release of new service. Qwest will facilitate Government observance if required for each new service or OSS



enhancement. The Qwest CPO will have responsibility for communicating the test results, so that the Government is assured that successful implementation will include stable OSS functionality.

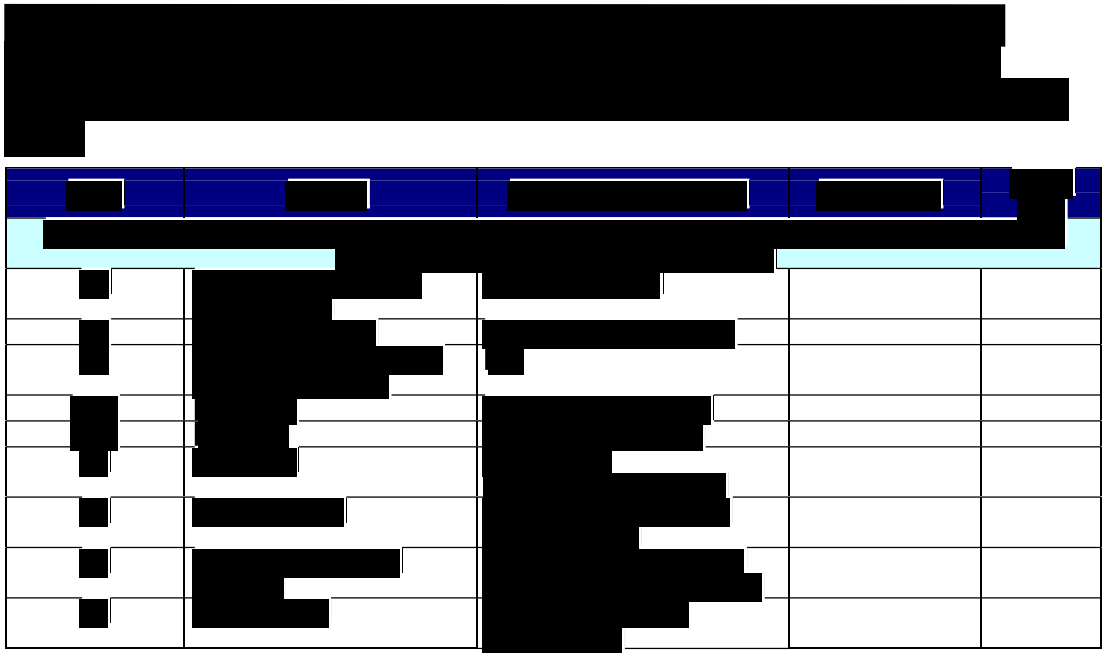
3.13.3.2.4 Data and Interfaces (L.34.2.3.13.1(d))

[redacted]

3.13.3.2.5 Test Results Reporting Requirements (L.34.2.3.13.1(e))

The Qwest Team has built a comprehensive OSS Verification Test Plan that addresses all Networx requirements utilizing Qwest internal testing standards. Verification tests define the objective, requirements, steps, actions and expected responses for each component test. Test actions are numbered for reference and identify the detailed steps to be performed as part of each

test (see [redacted] The expected responses define acceptable norms against which the results are compared. Additional detailed actions and expected responses will be defined at the time of Notice to Proceed (NTP) for Government approval. Testing results are scheduled to be reported within five business days at the conclusion of each test case for Government review over the following ten business day period. This will allow Qwest to run individual or repeated test cases while Government review is being conducted in parallel and to continue testing to meet the 60 day after NTP OSS Verification Test deliverable.



3.13.3.3 Networx Services Verification Test Plan (comp_req_id 1134)

Qwest is responsible for developing and delivering two verification test plans. The OSS Verification Test Plan is described above and is provided as part of this proposal submission. The Networx Service Verification Test Plan that Qwest is developing will be delivered within 60-days of NTP. The Networx Service Verification Test Plan will meet and comply with all the

requirements of RFP Section E.4 and will apply to all services being offered by Qwest under the contract. Qwest is responsible for the verification testing of Networx services and complies with all agreed acceptance testing as noted in Section E.4. Qwest has developed and will execute an OSS Verification Test Plan to verify that Qwest's OSS meets the requirements of Section E.3, Verification Testing of the Contractor's Operational Support Systems.

3.13.4 Security and Performance (L.34.2.3.13.2) (M.3.10(b))

3.13.4.1 OSS Security Approach

Qwest's OSS security approach complies with all Networx requirements as stated in the RFP. The Qwest response to the narrative requirements is detailed in the following sections. More information on Qwest's approach can be found in Appendix 2, Networx Security Plan.

3.13.4.1.1 Ensure Security Requirements are Met (comp_req_id 107)

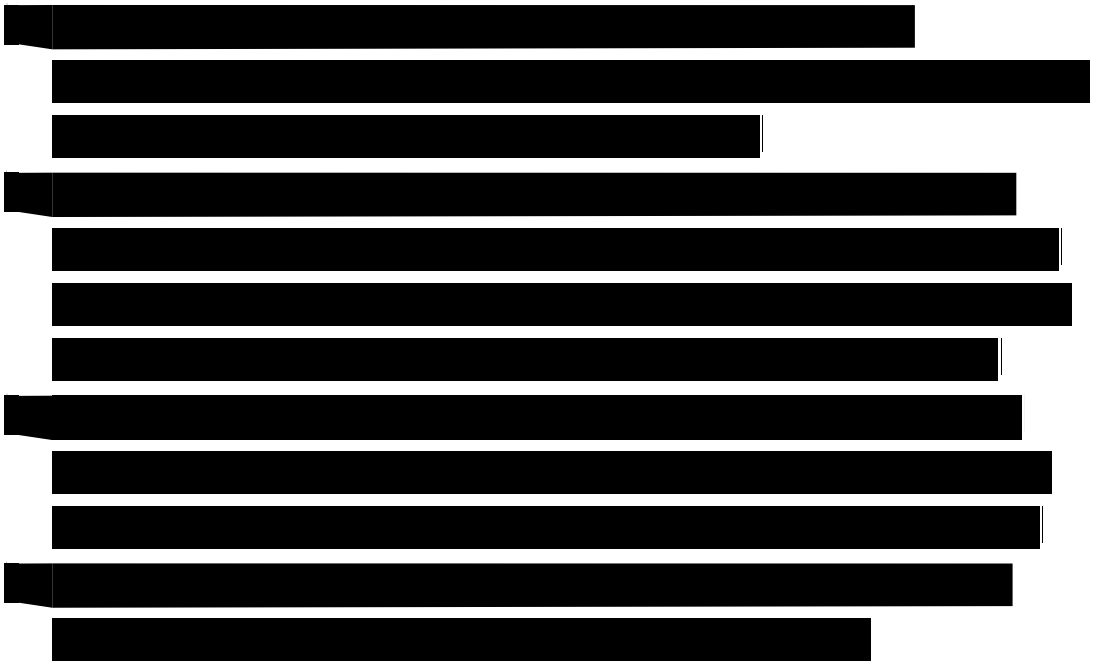
Qwest information systems, data, information processing capabilities and telecommunications networks are critical to our customer's business and are important Qwest business assets. Qwest is committed to protecting the security, confidentiality, availability and integrity of its information, underlying information systems and telecommunications networks and the data contained within this infrastructure and is equally committed to ensuring the Government's security requirements are met. We also protect against anticipated threats or hazards to these assets, including unauthorized access, malicious code attacks and/or inappropriate use or disclosure of information. Qwest has deployed a complete set of controls including access controls which manage users access to specific systems based on identification and authorization, managed OSS security services which protects the systems from outside attacks, software configuration and patch management which ensures system applications are protected, and a robust monitoring system for managing the infrastructure. Please see Appendix 2, Networx Security

Plan, for a description of the security controls that Qwest uses to ensure security requirements are met for all automated operational support systems. Specifically, Qwest will meet the requirements of Section C.3.9.2.1, Step 1 – Security and Performance, ID numbers 1 through 3.

The Qwest Team will work with Government Agencies to support certification and accreditation of the system via services such as Managed Tiered Security, Customer Specific Design and Engineering Services, or other services the Government may order. Qwest will fully conform to the requirements of Section C.3.3.2, Security Management, and include, at a minimum, security controls for low impact systems as defined in NIST SP 800-53, Annex 1.

3.13.4.1.2 Securing Methods in Security Plan (comp_req_id 106)

As part of the overall Security Plan, Qwest has extensive methods in place to secure OSS, including:



In addition to the methods stated above for securing OSS, Qwest provides more detail in Appendix 2, Networx Security Plan, of our proposal.

3.13.4.1.3 Meeting Other Contract Requirements (comp_req_id 100)

Qwest will meet the requirements for security management, fault management, and trouble handling in compliance with the Networx RFP. Qwest's Security Management is detailed in Appendix 2, the Networx Security Plan. Additionally Qwest has a robust security incident and resolution process. Qwest will provide 24x7x365 call coverage to receive, report, and assist with security incident calls in order to maintain the Acceptable Quality Level of 99.999 percent availability for the Portal and its

features (as described in Figure 3.13.2-1 above). Qwest provides the ability of defined users to report security incidents via the toll-free phone line to the Secure Network Operations Center (NOC) on a 24x7x365 basis. In addition the Portal has the capability to report, track, and manage security incidents. This capability fully covers the Agency business hours defined as Monday through Friday, 7:00 AM-7:00 PM. Procedures for security incident support and resolution will be consistent with requirements specified by the Agency and the Incident Response Plan. Qwest understands that resolving some security incidents will require action on the part of the Agency; therefore, no timeframe parameters are specified. Qwest will report all detected security incidents within 15 minutes via email and will post information on the Networx Portal. Qwest's NOC will cooperate with the Agency to mutually agree to a timeframe for resolution of each security incident, depending on the nature of the incident. Any delays or hindrance in resolution will be escalated and reported to the Agency COTR, security manager, or designated POC in accordance with the Qwest escalation process. The Qwest Secure NOC continuously monitors for service degradation and network component alarms which includes monitoring for security incidents.

Fault management is performed by Qwest's Network Management organization and is focused on network reliability and performance to reduce the occurrence, frequency, severity, and duration of fault events. Qwest [redacted] our network, using state-of-the-art tools and operational processes that make us a leading provider of telecommunications and data services. The Government will have [redacted] access through the Qwest Control Networx Portal to obtain the latest information regarding network faults. Qwest will manage all service reliability in [redacted], with customer controlled access through the Portal for application use. In addition, Qwest uses state-of-the-art communication tracking and development tools for

[redacted] to ensure network integrity. Qwest's goal is to minimize any downtime, service dispatches, or repair issues. Through our Qwest systems and our Networx team members, Qwest's objective is to isolate and resolve issues before they impact service. Our goal is simple: Qwest will work toward ensuring our network is always at optimal operating levels.

Qwest trouble handling is managed through secure systems and processes. Troubles will be [redacted] and resolved prior to any impact to the Government through our network management system's advanced surveillance system. Alarm thresholds will be set to trigger prior to customer-apparent services degradation. Qwest will take all necessary corrective action to ensure continued service quality. For other troubles, promptly contacting the Qwest CSO will enable our technicians to quickly respond, engage, and commence the troubleshooting process. Agencies will receive timely status on the progress and corrective action taken to resolve a trouble. For complex issues, Qwest's established process will engage the required technical expertise for prompt trouble resolution, up to and including [redacted] industry subject matter experts.

3.13.4.2 OSS Security Minimum Requirements

Qwest addresses OSS security requirements in the following subsections.

3.13.4.*2*.1 Description of Methods (L.34.2.3.13.2(a))

The Qwest Control Networx Portal provides industry-leading security to ensure integrity and confidentiality of customer and company information in support of all Networx services. Qwest will provide users access to a secure, online, Internet-accessible electronic system that meets the performance requirements of Section C.3.9, Operational Support Systems. The Qwest Control Networx Portal gives the GSA and Agencies access to all aspects of

their network deployment and ongoing management, security controls, particularly in user authentication, authorization, and data integrity. These access controls ensure that only authorized users are able to access the system. Once authorized, users will only be able to access areas of portal functionality related to their Agency and to the functions for which they are approved.

Qwest ensures that systems can be audited for historical views of who has accessed any Qwest system. Qwest can obtain reports of who is authorized and user logs.

Qwest will use access controls to manage user access to Qwest systems. Qwest will verify as part of the OSS test that users can see only their data. Users can be granted or restricted access based on Agency Hierarchy Code (AHC), function group (i.e. user can see ordering, but not billing) and service (user can order Frame Relay but is restricted from ordering Cell Phones). Qwest will set user access based on the Government's direction.

Qwest has robust backup and recovery capabilities whereby primary systems have redundant and geographically diverse systems in place. [redacted]

Qwest will secure the Networx Portal using FISMA Guidance, NIST, and FIPS standards and applicable Federal Standards. Qwest will conduct risk assessment in accordance with NIST 800 series standards and Qwest best practices to evaluate and assess the threat environment in terms of security impact and Security Objectives of the Portal and its applications. From this assessment Qwest will implement on the Portal the appropriate management, operational and technical controls, and the counter measures to meet the threat environment in accordance with the Security Outline 1 through 5 in [redacted]

Figure 3.13.4-1. Security Outline for Securing the Networx Portal. *Qwest* [redacted]

To effectively manage risk, Qwest will implement a Multi-layered Security Model (See [redacted]). Additional security services and measures support portal operations [redacted] (see Appendix 2, Security Plan).

Physical security is the action taken to protect Networx Portal information technology resources (e.g., access, facilities, installations, personnel, equipment, electronic media, documents) from damage, loss, theft, or unauthorized physical or passive access. Qwest will ensure physical security is in accordance with National Industrial Security Program Operating Manual (NISPOM) and the Networx RFP.

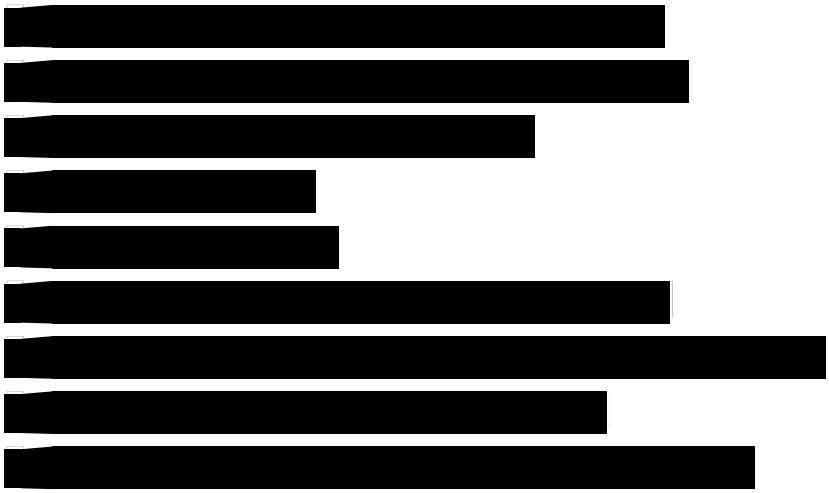
Qwest, [redacted], will execute the Security Test and Evaluation (ST&E) Plan, validate the management, operational, and technical controls and procedures implemented on the Portal, and submit ST&E findings to the Designated Approval Authority (DAA) for Certification and Accreditation Authorization in accordance with NIACAP requirements to obtain an Authority to Operate (ATO) from the DAA.

Additional security practices include implementing trend-setting controls specifically in the areas of personnel, systems, and facility security, which are guided by comprehensive security policies and standards. Qwest

has also implemented broad business continuity and disaster recovery measures and controls to ensure the availability of customer and corporate networks. Only those personnel with a need to know are permitted access to Qwest and customer resources. Likewise, Qwest systems that support our services are protected via superior practices, which include access, authorization and auditing controls. Qwest's network elements are protected by logical and physical security measures, all of which are controlled and auditable. Additionally, Qwest proactively works to ensure dependable OSS systems through risk mitigation planning, thereby preventing security breaches before they happen.

The Qwest Team's approach to risk derives its strength from project management processes and methodologies that are based on mature and well-documented corporate standards:

- Standards for Information Resources



- Network

[redacted]

- Security Evaluations

  [redacted]

- Virus/Intrusions/Vulnerabilities

  [redacted]

- Operating Systems

  [redacted]

Qwest data protection and backup and recovery plans are standard procedures of the Qwest Hardware and Application Software Change Management Plan. Fall back plans, [redacted] affecting the OSS, are also performed. Overall, Qwest's security and performance measures, which include audit processes, access controls, data protection, and backup and recovery of the OSS, combine to ensure reliable and comprehensive data protection and performance.

3.13.4.2.2 Data Integrity (L.34.2.3.13.2(b))

Qwest recognizes the importance of assuring data integrity for all stakeholders. To ensure data integrity, Qwest Control Networx Portal data fields are validated at the time of data entry according to individual

parameters and attributes defined during the software development process. On a system and database level, Qwest utilizes commonly accepted industry methods to ensure data integrity. These methods include:

[redacted]

[redacted]

Ultimately, data integrity is measured by Qwest's timely delivery of complete and accurate data records to GSA in the formats required in Section J.12 of the Networx RFP. Qwest's implementation of industry-standard data integrity methods ensures that the Qwest Control Networx Portal data are consistent and meaningful. Data integrity within the OSS allows Agency users to focus on the management of all services rather than the interpretation of data, thereby streamlining operations.

3.13.5 Change Control (L.34.2.3.13.3) (M.3.10(a))

3.13.5.1 Change Control Approach

Qwest's approach to provide and maintain OSS Change Control follows a process that includes [redacted] This is followed by an [redacted] This procedure is initiated and monitored by the CPO throughout the process. Please see the Appendix 6, OSS Change Management Plan for detailed steps and procedures.

3.13.5.1.1 Change Management Plan (comp_req_id 84)

Please see Appendix 6, OSS Change Management Plan, which meets the requirements of C.3.9.2.3.

3.13.5.1.2 Change Management Requirements (comp_req_id 83)

Qwest complies with all change management requirements as stated in the Networx RFP C.3.9.2.3 as follows:

- RFP requirement 1.1, informing the Government when OSS design changes are planned and when maintenance changes are required.

Qwest will inform the Government of planned changes via the GSA Networx PMO and Qwest CPO monthly status reports and meetings, and unplanned changes via conference calls between the GSA Networx PMO and Qwest CPO. Notice of all changes will be posted on the Qwest Networx website and the Qwest Control Networx Portal. Please see Section 3.13.5.2.3, which details Qwest's communications practices.

- RFP requirement 1.2, managing and controlling OSS change. Qwest has created a Change Management Plan which controls how changes are made to the OSS. [redacted]
- RFP requirement 1.3, incorporating Government review and approval into the contractor's change management process. Qwest has created a Change Control Board (CCB) [redacted] Please see Section 3.13.5.2.1 and Appendix 6 for details.
- RFP requirement 1.4, Government training. Qwest will provide training to the Government, if required, for changes to the OSS. All training will be coordinated by the Qwest Networx Training Manager. Please see Appendix 6, OSS Change Management Plan Section 4.6 for additional details.
- RFP requirement 1.5, Retesting with the Government to ensure functionality of any impacted interface. Qwest will comply with all retesting requirements and will make certain that the Government can ensure functionality of any impacted interface against the Networx requirements. Specifically, Qwest will involve the Government in retesting when OSS changes are planned and when maintenance changes are required. Qwest will manage and control OSS changes, and incorporate

Government review and approval by the Government. In addition, Government training implications and details around Government retesting will be included.

3.13.5.2 Change Control Minimum Requirements

Qwest addresses and will adhere to change control requirements as described in the following subsection.

3.13.5.2.1 Government Review (L.34.2.3.13.3(a))

Qwest recognizes that comprehensive change requests and requirements are critical to successful system enhancements or changes, and that for GSA to derive a successful result, they must be a partner and team member, playing a supporting role in addition to the customer role throughout the change process. As such, it is important for Qwest and GSA to work together to produce accurate scope, requirements, milestones and deliverables thus providing GSA with review and approval involvement.

The Qwest CPO and GSA PMO will validate, track and discuss changes on a monthly basis at GSA PMO meetings or more frequently as required; the Change Management Plan (Appendix 6, Sections 3.0 and 4.0) and OSS Verification Test Plan (Appendix 5, Section 1.0) provide more detail.

3.13.5.2.2 Functionality of Interfaces (L.34.2.3.13.3(b))

As shown previously in Figure 3.13.3-1, Qwest utilizes a number of tests, [redacted] to ensure functionality of interfaces. These tests are performed by Qwest on all system enhancements or changes to Qwest's OSS in parallel with development teams, prior to [redacted] as defined in the OSS Verification Test Plan.

3.13.5.2.3 Methods of Communicating Changes (L.34.2.3.13.3(c))

Qwest will inform the Government of planned changes via the Networx PMO and CPO monthly status reports and meetings. In all instances Qwest

will meet the requirement for 30 calendar days notice prior to any planned maintenance performed on the OSS.

[redacted]The Qwest OSS is actively monitored 24x7x365 and processes and procedures are in place to minimize disruption to the OSS infrastructure. Events affecting the OSS will be monitored and communicated to the GSA PMO via the Qwest CPO as soon as the event is recognized. Qwest's Networx Web site, www.gsanetworx.com, will also be used to communicate planned and unplanned changes to all Government users, as well as, announcements on 1-866-GSA-NETWorx (1-866-472-6389). More detail regarding delivery methods is provided in Appendix 6, OSS Change Management Plan.

3.13.6 OSS Summary

Qwest will support the Networx program with a comprehensive and secure Operational Support System (OSS) that performs a wide range of functions including billing, service ordering, customer support, service management, inventory management, training and program management. Our Networx OSS, described in detail throughout the Management Volume of this proposal, supports the full range of RFP requirements. Our approach offers the advantages of building on our existing Federal Portal, currently being utilized to support Federal customers and existing contracts. Simplicity of access has been a development design principle of Qwest Control Networx Portal which is the front door to our OSS.