

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 Networkx operations. The Qwest Control Networkx Portal will provide GSA and Agencies insight into our proven and highly integrated Operational Support Systems (OSS) via Web-based, secure access.

3.13.1 Understanding of the Requirement

Qwest will support the Networkx 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 Networkx OSS, described in detail throughout the Management Volume of this proposal, supports the full range of requirements.

[REDACTED]

[REDACTED]

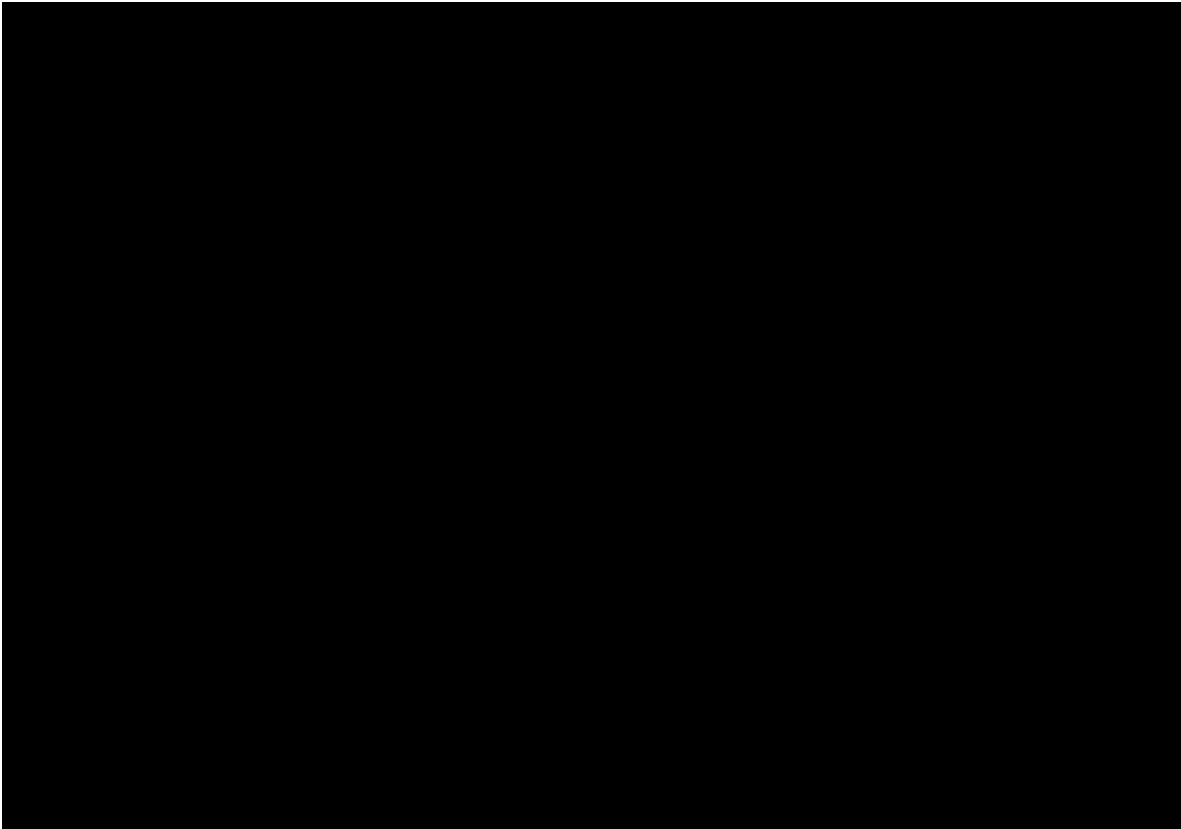
[REDACTED]

[REDACTED]

[REDACTED] Simplicity of access has been a development design principle of Qwest Control Networkx Portal, which is the front door to our integrated OSS [REDACTED]

[REDACTED]

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 use of legacy systems, while simultaneously presenting customers with intuitive,



user-friendly Web interfaces to access the information they require. [REDACTED]



Qwest continues to make significant investments in customer-driven portals for automation of front end processes, which the Qwest Control Network Portal best illustrates. Qwest Control Network Portal enables Government users to manage telecommunications services end-to-end through a simple and easy-to-use interface. Through the Qwest Control Network Portal [REDACTED], Agencies can perform a variety of functions, including: 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 Agencies' specific needs, supporting their mission requirements by upgrading and improving the OSS through processes that include [REDACTED]

[REDACTED]

[REDACTED]

Qwest's OSS features [REDACTED] systems that support Government and commercial customers today. [REDACTED]

[REDACTED]

[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]

[REDACTED]

[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 Agency 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 Agencies have a one-stop shop for their telecommunications management requirements, saving time and maximizing productivity.

Qwest understands the importance of providing Agencies with high quality services through an OSS infrastructure that is tested and proven to meet Agencies' needs. Qwest understands the order and billing challenges

of FTS 2001 and has developed an OSS Verification Test Plan for the purpose of validating our compliant systems before accepting Agency orders.

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	[REDACTED]
10898	C.3.9.2.1	[REDACTED]
10899	C.3.9.2.1	[REDACTED]
10905	C.3.9.2.1	[REDACTED]
10919	C.3.9.2.3	[REDACTED]
10920	C.3.9.2.3	[REDACTED]

3.13.1.1.2 Specific Narrative Requirements

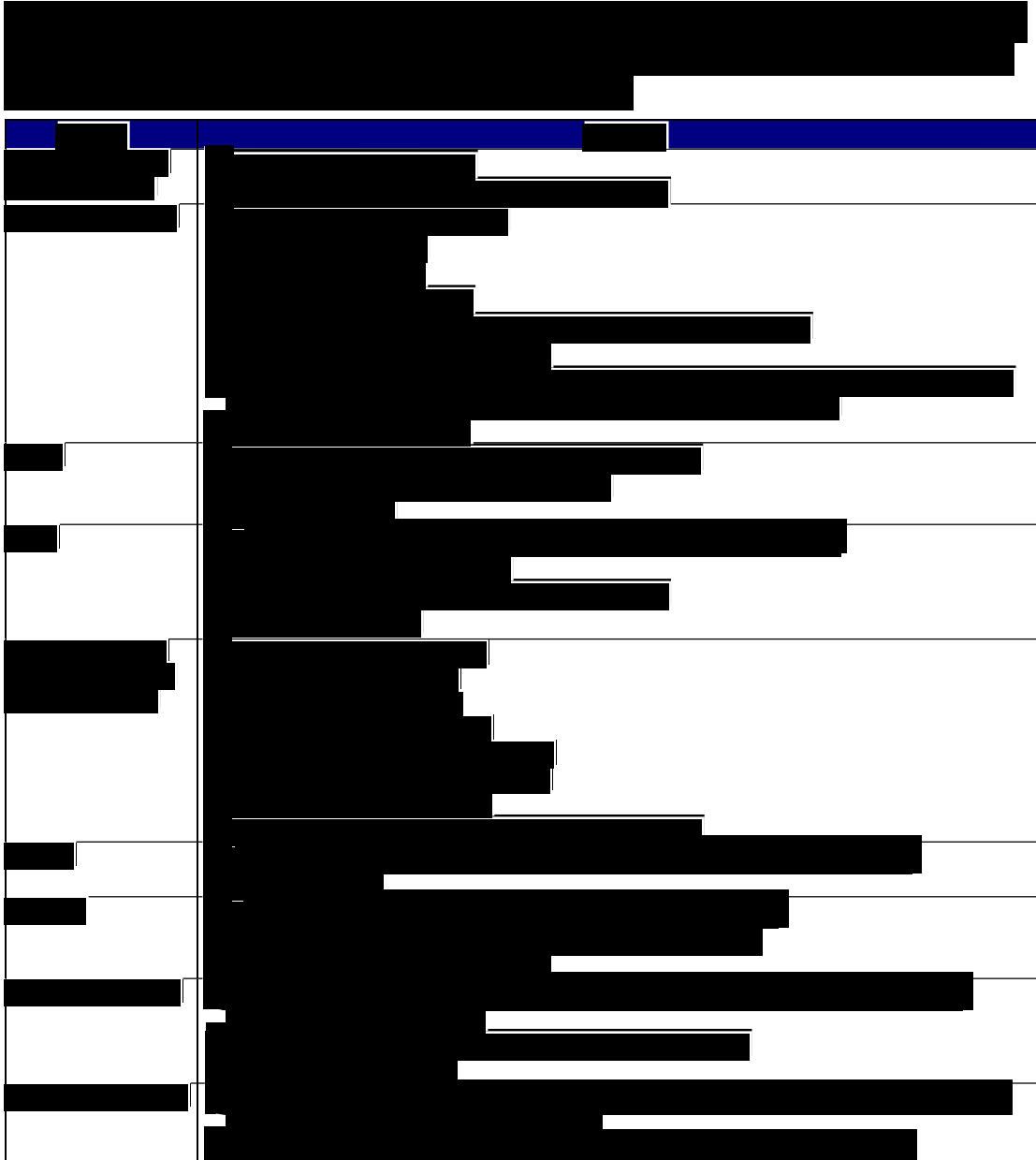
Comp_req_id	RFP Section	[REDACTED]
10906	C.3.9.2.2	[REDACTED]
11017	E.2	[REDACTED]
11019	E.2.1	[REDACTED]
11020	E.2.1	[REDACTED]
11025	E.3	[REDACTED]
11026	E.3	[REDACTED]

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

The Qwest Control Networkx Portal provides a broad range of online tools that enable Agency users to manage their Qwest services. [REDACTED]

[REDACTED]

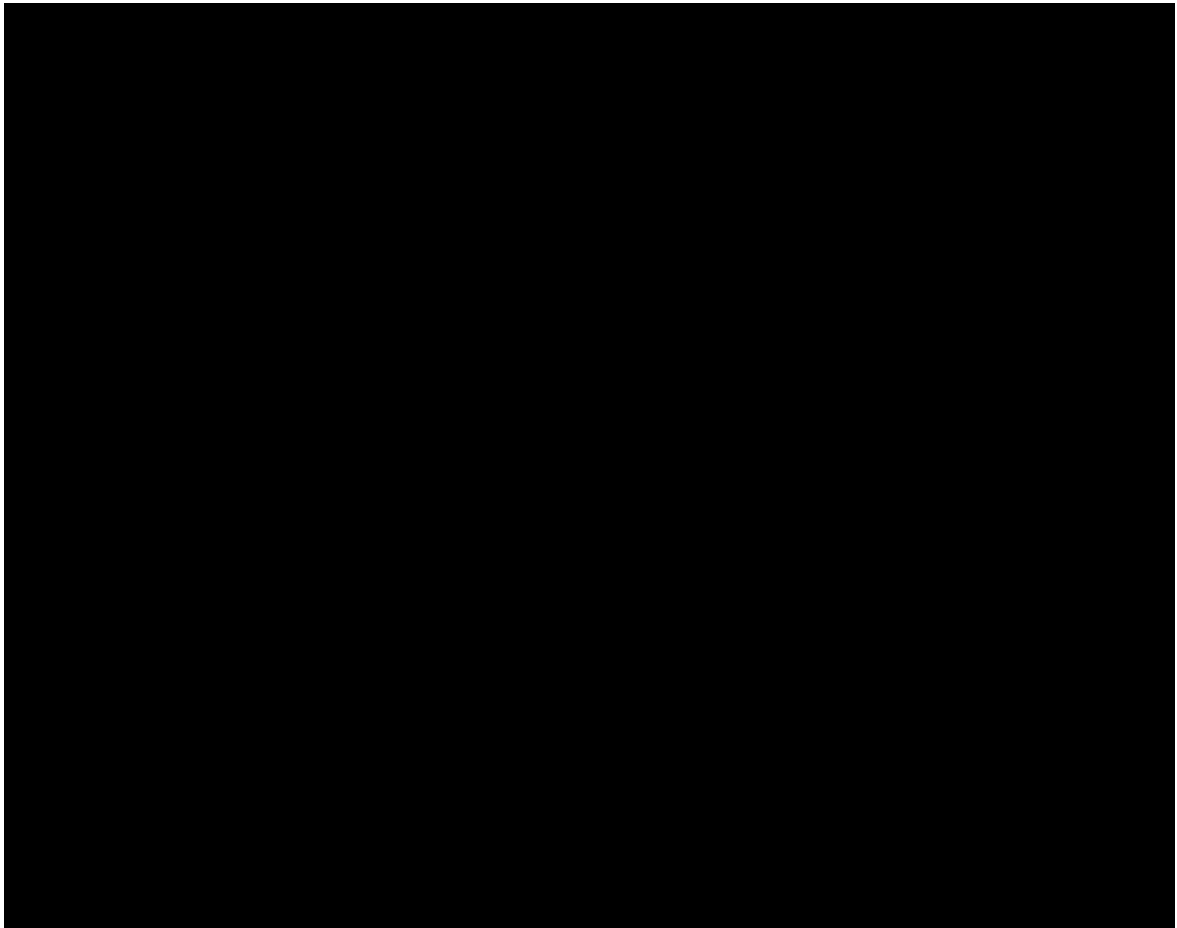
█. These features within the Portal will be ready at Notice To Proceed (NTP), including order management, repair, reporting, Managed Network Services/ Managed Security Services, Portal administration, inventory, and billing. These features have already been released into the production environment.



The table is almost entirely redacted with black boxes. It features a single blue header row at the top. The table structure is defined by a grid of black lines, but the content within the cells is obscured.

3.13.2.1 Qwest Control Network Portal: A Complete Qwest System

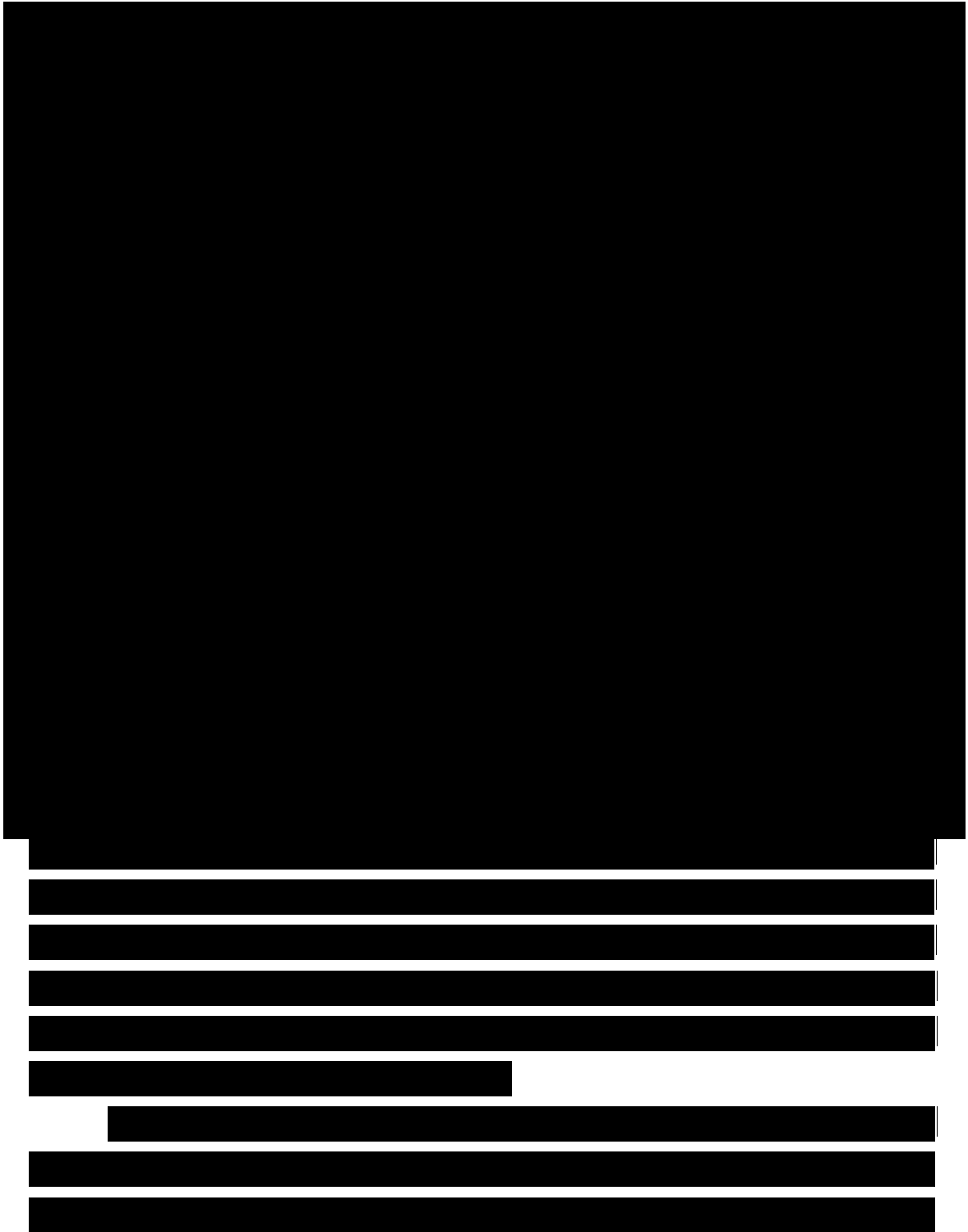
The Qwest Control Network Portal provides the convenience of allowing Government staff to view the service lifecycle, from quoting through acceptance and continuing through service performance management [REDACTED]. The Portal provides quotes and is the vehicle for submitting service orders into our ordering system. Confirmed service orders are provisioned via our network provisioning systems. After provisioning is completed and the Agency 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. The Qwest reporting tool is where users can run standard reports or can create ad hoc reports through custom queries of the inventory database. The Qwest reporting tool is also used for correlation of SOCN to both the inventory and the invoice. This provides the Agency an easy method to validate services ordered against the inventory database and the invoice. Flexible reporting makes the service and performance management process simple, efficient, and enables higher productivity levels among Agency staff.

OSS Architecture and Integration

[Redacted content]



[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted content]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

[Redacted text block]

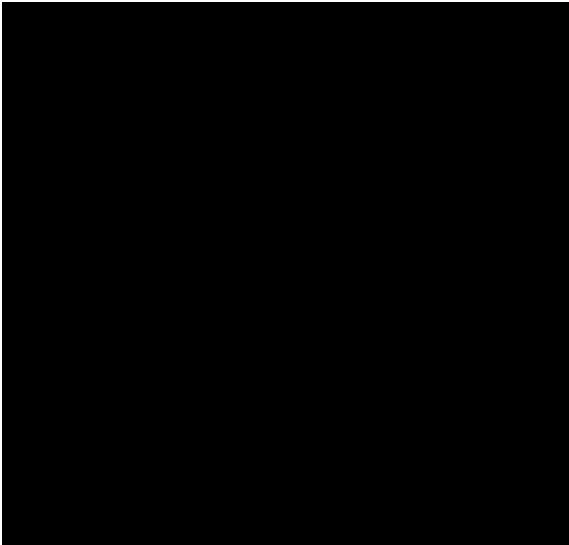
[Redacted text block]

[Redacted content]

[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 Network 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, email, CD-ROM, U.S. Postal Service, and Facsimile. The reports can be provided in the following formats: 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 Network 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 Network 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 10906, 11019)

Qwest has provided a draft OSS Verification Test Plan, Appendix 5, in accordance with Section C.3.9 Requirements and Section E, Inspection and Acceptance. Qwest will update and finalize the OSS Verification Test Plan within 10 business days of receipt of Government comments. In accordance with Section E of the RFP, Qwest will complete its OSS verification test process within 60 calendar days of NTP, or 60 calendar days after Government approval of the test plan, whichever is later.

3.13.3.1.2 OSS Verification Test Plan Update (comp_req_id 11020)

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

3.13.3.1.3 Test Cases (comp_req_id 11025)

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

Qwest will execute acceptably the tests prescribed by the Network RFP using:

1. Qwest test data
2. Government provided test data in standard format (using historical data)
3. Government provided on-site, randomly-created test data

3.13.3.1.4 Standard Test Procedures (comp_req_id 11026)

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. See also Appendix 5.

3.13.3.2 OSS Verification Test Plan Requirements

The following sections detailed how Qwest meets Network requirements. More information on Qwest's approach can be found in Qwest's OSS Verification Test Plan. Qwest has developed and will execute the 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. Certification and Accreditation testing may run in parallel with the OSS 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 Network 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 Network 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 on 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]

[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]

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]

[REDACTED]

[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.

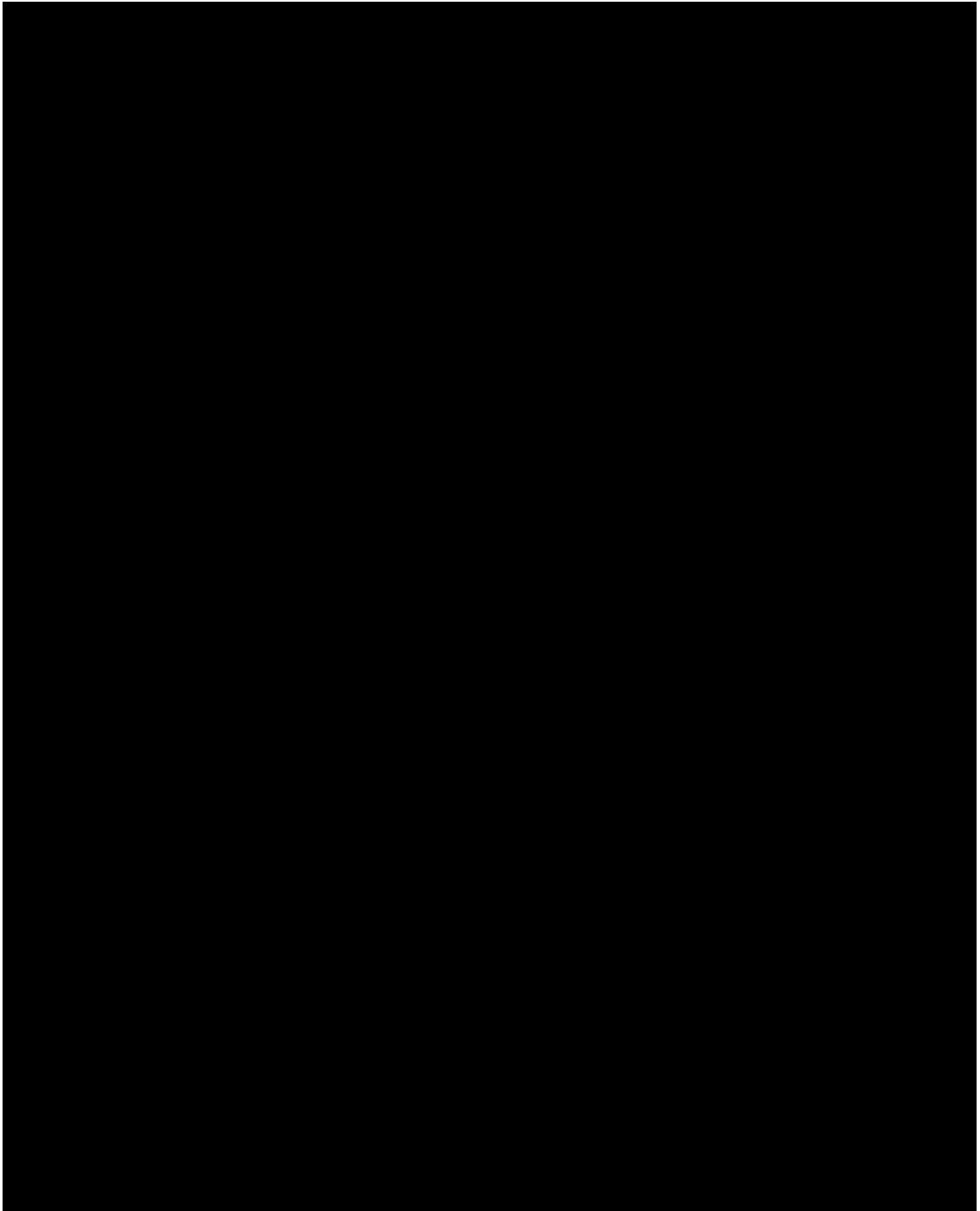
3.13.3.2.3 Effective and Timely Testing (L.34.2.3.13.1(c))

Qwest routinely 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]

[REDACTED]

[REDACTED]

[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 Network ordering, Qwest will execute 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]

[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]

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 Networkx requirements using 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 [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.

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

3.13.3.3 Networkx Services Verification Test Plan (comp_req_id 11017)

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 (see also Appendix 5). The Networkx Service Verification Test Plan that Qwest is developing will be delivered within 60 days of NTP. The Networkx 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 Networkx services and complies with all agreed acceptance testing as noted in Section E.4.

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 Networkx requirements as stated in the RFP. Our response to the narrative requirements is detailed in the following sections. More information on Qwest's approach can be found in Appendix 2, Networkx Security Plan.

3.13.4.1.1 Ensure Security Requirements are Met (comp_req_id 10898)

Qwest information systems, data, information processing capabilities, and telecommunications networks are critical to Agency's missions and are important Qwest business assets. Qwest is committed to protecting the security, confidentiality, availability, and integrity of our information, underlying information systems, telecommunications networks, and the data contained within this infrastructure. Qwest 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 that manage users' access to specific systems based on identification and

authorization; managed OSS security services that protects the systems from outside attacks; software configuration and patch management that ensures system applications are protected; and a robust monitoring system for managing the infrastructure. Please see Appendix 2, Networkx 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.

[REDACTED]

[REDACTED] 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 10899)

As part of the Security Plan, Qwest has extensive methods in place to secure OSS, [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]

3.13.4.1.3 Meeting Other Contract Requirements (comp_req_id 10905)

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 resolve security incident calls in order to maintain the Acceptable Quality Level of 99.999 percent availability for the Qwest Control Network 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 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 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 Qwest Control Network 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. Qwest will manage the reliability of our network and that of our team members [REDACTED]. The Government will have [REDACTED] access through

the Qwest Control Network Portal to obtain the latest information regarding network faults. In addition, Qwest uses state-of-the-art communication tracking and development tools [REDACTED] [REDACTED] to ensure network integrity. Qwest's goal is to minimize any downtime, service dispatches, or repair issues. Through our Qwest systems and our Network team members, Qwest's objective is to isolate and resolve issues before they impact service. Our goal is simple - ensuring our network is always at optimal operating levels.

Qwest's trouble-handling is managed through secure systems and processes. Through our network management system's advanced surveillance system, potential troubles will be [REDACTED] identified and most will be resolved prior to any impact to the Government. Alarm thresholds will be set to trigger prior to Agency-apparent services degradation. Qwest will take all necessary corrective action to ensure continued service quality. When Agencies contact the Qwest CSO in response to other troubles they experience, our technicians respond quickly, and engage immediately in a 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 Network Portal provides industry-leading security to ensure integrity and confidentiality of Agency and company information in support of all Network 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 Network Portal gives 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. Only authorized users will 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]

[REDACTED]

Qwest will secure the Qwest Control Network Portal using FISMA Guidance, NIST, 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 [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]		[REDACTED]	[REDACTED]	[REDACTED]

To manage risk effectively, Qwest will implement a Multi-layered Security Model [REDACTED]

[REDACTED] Additional security services and measures support Portal operations, which include: [REDACTED]

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

[REDACTED]

[REDACTED] (see Appendix 2, Networkx Security Plan).

Physical security is the action taken to protect the 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 (NISPO) and the Networkx 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 Agency and corporate networks. Only those personnel with a need to know are permitted access to Qwest and Agency resources. Likewise, Qwest systems that support our services are protected via industry standard security 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 is proactive to ensure the dependability of our OSS, by the execution of risk mitigation plans. These plans detail the methods that prevent security breaches.

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

[Redacted text block]

- Network

[Redacted text block]

- Internet/Intranet

[REDACTED]
[REDACTED]

- Security Evaluations

[REDACTED]
[REDACTED]

- Virus/Intrusions/Vulnerabilities

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

- Operating Systems

[REDACTED]
[REDACTED]
[REDACTED]

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 Network 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 uses standard industry methods to ensure data integrity. [REDACTED]

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

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

[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 Qwest Control Networx Portal data is 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 [REDACTED]

[REDACTED]

[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 10919)

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 10920)

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 Networkx PMO and Qwest CPO. Notice of all changes will be posted on the Qwest Networkx Website and the Qwest Control Networkx 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 that 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 Networkx 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 Networkx 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. In addition, Government training implications and details around Government retesting will be included,

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

[REDACTED]

[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 Networkx Website, www.gsanetworkx.com, as well as announcements on 1-866-GSA-NETWorx (1-866-472-6389) will be used to communicate planned and unplanned changes to all Government users. More detail regarding delivery methods is provided in Appendix 6, OSS Change Management Plan.

The Qwest approach to meeting OSS requirements is the same for optional services as mandatory services.

3.13.6 OSS Summary

Qwest will support the Networkx program with a comprehensive and secure OSS that performs a wide range of functions including billing, service ordering, customer support, service management, inventory management, training, and program management. Our Networkx 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 used to support Agencies and existing contracts. Simplicity of access has been a development design principle of Qwest Control Networkx Portal, which is the front door to our OSS.