3.3 SECURITY MANAGEMENT (L.34.2.3.3; M.2.11; COMP_REQ_ID 10176)

In today's environment, security and risk management have become very critical to the well-being of our nation. The Qwest Team has been and will continue to be an industry leader in working with the Government to meet this national priority. We have implemented a hierarchy of auditable controls and management tools in the areas of personnel, systems, and facility security, each of which are governed by comprehensive security policies, standards, and guidelines.

Qwest's integrated Networx Security Team is providing a Networx Security Plan that meets the requirements specified in Sections C.2.1.11, C.3.3.2, C.3.3.2.2.1, C.3.3.2.2.5, and C.3.3.2.4.2.1. The Networx Security Plan is delivered as Appendix 2 of the Qwest Networx Enterprise proposal.

3.3.1 Understanding of the Requirement

Qwest understands GSA's need to ensure the security of the networks, data, Operations Support Systems (OSS), physical environment, and personnel engaged in satisfying the requirements of the Networx program, while also strengthening the overall information security posture against a variety of threats for Agencies using Networx services. We share the GSA's high-priority concerns for protecting the nation's critical infrastructure and services and are both well-experienced and well-positioned to meet this need. In addition, Qwest understands that managing today's security risk levels requires a broad view across a variety of technologies. Qwest provides a strong set of security-related offerings tuned to each Agency's information technology environment and security needs. By building on our pre-existing leadership and experience in the areas of risk management, information security, disaster preparedness, and operational knowledge, we will assure the confidentiality, integrity, and availability of Networx-related data and communications.

All members of the Qwest Team understand their roles in meeting Agency needs for minimizing risks and responding rapidly to both events and new vulnerabilities. Our network operations groups, along with key team member organizations, meet the challenge of providing a secure environment, whether their areas of responsibility cover product and service offerings to Agencies, internal corporate infrastructure and systems, or the administrative components that enable sound management, all as a part of our Spirit of Service™. Security is a core competency and an integral part of the Qwest business.

Qwest's experience has shown that in light of today's ever-changing climate of threats and vulnerabilities, a sound security position is best maintained by adopting a holistic view of risk management across the Qwest enterprise and our service offerings. This enterprise-wide approach to risk management, and specifically to security practices, calls for centralized authority and policymaking combined with clear lines of communication, well-defined expectations, and close collaboration among all those with a stake in making the Qwest and Agency environments secure. [redacted] this model exists at Qwest today, enabling our rapid identification of new threats and vulnerabilities, while also creating an action-oriented approach to remediating risks and managing security events.

[redacted]

3.3.1.1 Responses to Narrative Requirements Table

3.3.1.1.1 General Narrative Requirements

Section 3.3.1.1.1, General Narrative Requirements, and Section 3.3.1.1.2, Specific Narrative Requirements, identify RFP requirements and associated proposal response locations.

comp_ req_id	C Section	[redacted]
10176	C.3.3.2.2.1	[redacted]
10178	C.3.3.2.2.1	[redacted]
10179	C.3.3.2.2.1	[redacted]

comp_ req_id	C Section	[redacted]
10181	C.3.3.2.2.1	[redacted]
10202	C.3.3.2.2.4	[redacted]
10203	C.3.3.2.2.4	[redacted]
10206	C.3.3.2.2.4	[redacted]
10207	C.3.3.2.2.4	[redacted]
10208	C.3.3.2.2.4	[redacted]
10209	C.3.3.2.2.4	[redacted]
10210	C.3.3.2.2.4	[redacted]
10211	C.3.3.2.2.5	[redacted]
10213	C.3.3.2.2.5	[redacted]
10214	C.3.3.2.2.5	[redacted]
10215	C.3.3.2.2.5	[redacted]
10216	C.3.3.2.2.5	[redacted]
10218	C.3.3.2.2.5	[redacted]
10220	C.3.3.2.2.5	[redacted]
10221	C.3.3.2.2.5	[redacted]
10222	C.3.3.2.2.5	[redacted]
10223	C.3.3.2.2.6	[redacted]
10224	C.3.3.2.2.6	[redacted]
10225	C.3.3.2.2.6	[redacted]
10240	C.3.3.2.2.7	[redacted]
10241	C.3.3.2.2.7	[redacted]
10242	C.3.3.2.7	[redacted]
10248	C.3.3.2.2.9	[redacted]
10249	C.3.3.2.2.9	[redacted]
10250	C.3.3.2.2.9	[redacted]
10251	C.3.3.2.2.9	[redacted]
10252	C.3.3.2.2.9	[redacted]
10253	C.3.3.2.2.9	[redacted]

comp_ req_id	C Section	[redacted]
10259	C.3.3.2.2.11	[redacted]
10260	C.3.3.2.2.11	[redacted]
10261	C.3.3.2.2.11	[redacted]
10262	C.3.3.2.2.12	[redacted]
10266	C.3.3.2.2.13	[redacted]
10267	C.3.3.2.2.13	[redacted]
10268	C.3.3.2.2.13	[redacted]

3.3.1.1.2 Specific Narrative Requirements

comp_req_id	C Section	RFP Requirement	[redacted]
10177	C.3.3.2.2.1	(3) The contractor's Security Plan shall include a description of the approach, scope, and methodology of Networx services security risk analyses that shall be undertaken by the contractor throughout the life of the contract.	[redacted]
10180	C.3.3.2.2.1	(6) The contractor shall descr be in the Security Plan the management, technical and operational controls as defined in NIST SP 800-18, that will be employed to ensure the integrity, confidentiality, and availability of Government information and data that is transported and/or stored by Networx services, Networx OSS, databases, or handled manually at contractor's facilities.	[redacted]
10212	C.3.3.2.2.5	(2) The contractor shall protect against unauthorized access to these databases, OSS, and information processing systems by entry from external communications devices.	[redacted]

3.3.2 Security Planning (M.3.11 (d))

3.3.2.1 Security Requirements (comp_req_id 10178, 10218)

Qwest has a longstanding, robust security program with a proven history of providing industry-leading security services to protect Qwest's infrastructure, including information assurance processes applicable to the databases, OSS, and information processing systems upon which Networx services will depend. Qwest is committed to protecting Agencies against threats, attacks, or failures to systems, in accordance with best commercial practices. Qwest will ensure that, throughout the life of the contract, all

Networx OSS and service components software have current security updates and patches for all known vulnerabilities. Qwest employs a mature, process-based risk assessment approach to ensure logical and physical security controls are in place and are appropriate for our computer centers, network operations centers, secure operations centers, cyber centers, and other Qwest facilities. Qwest's security-related services ensure the integrity, confidentiality, and availability of information assets, and support Qwest resources and our wide range of customers and geographical locations. Qwest's security policies are in compliance with all security control classes specified in NIST SP 800-53/Annex 1, as they relate to both the Qwest Networx infrastructure and OSS.

The Qwest integrated Networx Security Team has leveraged our experience in preparing a Networx Security Plan that meets the requirements specified in Sections C.2.1.11, C.3.3.2, and C.3.3.2.4.2.1. This Networx Security Plan is compliant with OMB Circular A-130, NRIC Recommendations VI-1A-05 through VI-1A-10, and Telcordia standards. In addition, the Networx Security Plan also addresses Qwest's compliance with Public Law 104-191, Health Insurance Portability and Accountability Act (HIPPA) of 1996, as required in the Networx Enterprise RFP and FIPS PUB 200. The Networx Security Plan is delivered as Appendix 2 to the Qwest Networx Enterprise proposal.

As described in Section 3.3, Qwest takes a lead role in developing standards, working with vendors, and implementing new, innovative approaches to improve our products. This includes security services, along with support of ongoing programs to manage the ever-changing security landscape.

3.3.2.2 Security Management Organization and Planning (comp_req_id 10179, comp_req_id 10181)

The Qwest integrated Networx Security Team management structure, along with the organizational information, is provided in this Section, in addition to details provided in the Networx Security Plan. Qwest meets the requirements specified in Section C.3.3.2.2.1 of the Networx Enterprise RFP.

Qwest's Networx Security Manager, along with our CPO Networx Security Team, will interface and coordinate with the Government on security matters in a number of ways, including hosting face-to-face meetings and technology summits with Agency security professionals. These approaches will foster enhanced understanding of Qwest's security policies and practices, and provide an opportunity to receive feedback on the effectiveness of Qwest's Networx security activities. Qwest understands that effective communication can be the differentiator between success and failure for the Networx program. Qwest’s approach to communicating security-related matters to Agencies includes utilization of the Networx Website to post relevant security policies and procedures and reports to all Networx stakeholders [redacted] that will be developed and maintained by the Qwest Networx Security Manager. This has proven to be an effective communication tool for other Qwest programs, to educate employees, agents, contractors and Agency users on specific procedures relevant to a specific activity.

Qwest understands the importance of internal security management, partnering with the Government and leveraging strategic business relationships, to provide superior security management for Networx.

The Qwest Networx Security Manager will work with the Qwest Subcontracts Manager to ensure that appropriate controls are implemented to manage subcontractor security compliance. The Qwest Networx Security

Manager will develop, document, and communicate security standards for Qwest business alliances, suppliers, and vendors. [redacted] The Qwest Networx CPO will also have a dedicated Networx Disaster Recovery (DR) Liaison Officer, who will be in direct communications with DR counterparts at Qwest's business alliances, suppliers and vendors.

[redacted]

[redacted] These areas work in partnership with a variety of operational groups, business units, and key service providers to ensure appropriate implementation of security measures, including ongoing compliance management. [redacted]

[redacted]

[redacted]

At Qwest, we have proven capabilities in managing risk [redacted]. While risk management is composed of a variety of expertise areas, recent world events have shown that combining these skill sets into a cohesive team allows us to assess threats and respond to events rapidly, with the right expertise, even as events unfold.

[redacted] This approach provides strong security management for Networx. [redacted]

The cyber threat for Agencies has grown, along with the need for demonstrated security practices to comply with obligations such as the

Federal Information Security Management Act (FISMA) and the Department of Defense Information Technology Security Certification and Accreditation Process (DITSCAP). To counter this threat, Qwest has evolved our security functions to ensure close organizational alignment and collaboration between more traditional industrial security programs and our technology-related functions.

[redacted] has proven capabilities in designing and delivering specific security services to customers. Feedback from our customers, our highly experienced staff, and external auditors and consultants has shown that this team approach to security fosters a stronger recognition of risks and a more rapid response to threats. Our track record in maintaining a secure networking environment and corporate infrastructure proves the value of this approach.

[redacted] provides policy making within their areas of expertise, and defines processes, practices, and procedures for executing their management and operational controls as described below in Section 3.3.3. While specific tools and systems are employed by each function, [redacted] From an Agency's perspective, this program enables Qwest to recognize and respond to issues quickly, in a consistent manner, and it fosters a climate of compliance that ensures all our team members treat security as a part of their jobs.

The Networx Security Plan is delivered as Appendix 2 and details the process that will be utilized by the Qwest integrated Networx Security Team to communicate with and educate the entire Qwest Networx team on the Networx security program.

Qwest's approach to communicating security policies, practices, and procedures [redacted]. These communications and training programs are provided to the Networx PMO, and Agency users, as well as to Qwest's employees, suppliers, subcontractors and vendors. These communication practices will ensure understanding of the policies and procedures relevant to each Networx stakeholder. [redacted]

The Qwest Networx Security Plan details the processes that will be used by the Qwest integrated Networx Security Team (including subcontractors, suppliers, and vendors). The [redacted] will be used to communicate with and educate the entire Qwest Networx team on the Networx security policies, practices, procedures, and general security awareness. [redacted]

3.3.2.3 Security Policies, Practices, Tools, and Systems (comp_req_id 10249, comp_req_id 10248, comp_req_id 10253, comp_req_id 10251, comp_req_id 10250, comp_req_id 10225, comp_req_id 10203, comp_req_id 10211, comp_req_id 10218, comp_req_id 10223)

[redacted]

Physical Security

[redacted]

Additionally, the Qwest integrated Networx Security Team is well versed in the NISPOM requirements for accreditation of secure facilities, and has proposed an experienced security professional to be the Networx Security Manager. Upon contract award, this individual, in concert with the Qwest Networx CPO and GSA Networx PMO, will determine what required accreditations for secure facilities (i.e., DoD Secret or above) are needed to perform classified tasks for Networx, as defined by the DD254s. In addition to being well versed in the physical security area to support secure facilities and protect classified information, [redacted]

[redacted] to ensure they meet the minimum requirements per NISPOM and other Government clearance/access regulations.

Qwest supports a robust program of physical security measures to protect Agency hardware and software from theft or other human threats that may impact the availability of Networx services or compromise Government information or data. [redacted]

The Qwest integrated Networx Security Team will work with the Qwest Networx CPO to ensure Qwest physical security controls are commensurate with the critical nature of work being performed and/or the sensitive nature of Agency information being handled.

Fraud Control and Investigations

[redacted]

Qwest maintains a strong safety and environmental protection program as part of enterprise Risk Management, and adheres to all applicable regulations and processes appropriate to specific facilities and locations in compliance with Federal, state and local regulations, including, for example, fire code regulations.

Disaster Preparedness

[redacted]

[redacted] Additional details regarding the approach Qwest takes to network management for preventing service interruptions and minimizing their impacts in the rare event of an occurrence are detailed in Section 3.2, Network Management and in Section 3.4, Disaster Recovery.

Information Security

In contrast to the more traditional security functions described above, the [redacted] organization is devoted to protecting the confidentiality, integrity, and availability of information assets, and supporting resources of Qwest and its customers [redacted]

Qwest understands the need to follow Government requirements, and to meet or exceed the expectations set by them. We employ widely-accepted guidance as the framework for our security programs. [redacted]

Qwest's security program is in place to protect our infrastructure, including databases, OSS, and information processing systems upon which

Networx services will depend. Qwest already employs and will continue to adhere to the important principles and practices that comprise this program. Qwest uses widely-recognized standards such as the ISO 17799, NIST SP 800, FIPS documents, and other applicable standards as underlying guidance and the framework for our Networx security programs. [redacted] management of FIPS 201 compatible two-factor security measures, such as tokens and digital certificates; and compliance assurance activities for systems access to key components of the OSS. The Qwest Networx Security Plan as delivered in Appendix 2 provides additional details on these programs.

Our Networx Security Plan also details Qwest's approach to new technology testing and certification processes used to ensure security is integrated into new or changed infrastructure components for Networx services and OSS.

As Qwest Operations receives software update inputs or requests for new products for the Qwest infrastructure, they will work with the Qwest Networx CPO and the Qwest integrated Networx Security Team as part of the software and new product evaluation process, and make appropriate recommendations to the GSA Networx PMO.

Proactive Approach to Security

Qwest supports a proactive set of planning and management controls including security-related policy making, evaluations and risk assessments, in order to make security practices a priority as new products, services, and other infrastructure components are contemplated.

[redacted]

[redacted] Please see Section 3.3.3.4.3, below, for details on event management and Agency notification. [redacted] They ensure that protective controls are in place and current across the Qwest infrastructure for vulnerability management as described below in Section 3.3.3.4.2[redacted]. This team works closely with Qwest Operations to ensure that all security-related events with a potential to impact Agencies are identified, handled, and communicated in a timely manner.

While Qwest Government Services, Inc. (QGSI) Security provides dedicated support to Agencies for both industrial and cyber security areas, the organization is closely aligned, as shown in Figure 3.3.2-1, with Qwest's integrated Risk Management organization to ensure a strong focus on security practices and close collaboration with corporate functions to leverage all Qwest expertise in support of programs such as Networx. This team will provide dedicated support, security guidance, and oversight to Networx via the Qwest Networx Security Manager in the Qwest CPO.

Information on security-related events with a potential to impact Agencies will be managed by the Qwest Networx Security Manager to ensure a clear focus and timely response. The Networx Security Manager has the responsibility of working with the Government's Networx Program Management Office (PMO) to ensure compliance with all applicable policies, publications, standards, and Executive Orders contained in the Networx Enterprise contract.

Qwest's Networx Security Manager, [redacted] will be the authorized interface within Qwest to our suppliers, vendors, subcontractors and Agencies on all Networx security matters. Working with the integrated Networx Program Team, he will have oversight on all activities impacting security. [redacted] is a seasoned security professional [redacted] with more than 12 years of security experience supporting various Government entities. The Networx Security Manager also has a clear path of communication and reporting to the Qwest Networx CPO.

The Qwest CPO has a dedicated Networx Disaster Recovery Liaison Officer as described in Section 3.4, Disaster Recovery, as well as a dedicated Information Security Engineer. Together, this team will be well-positioned to take full advantage of all the capabilities of Qwest's Risk Management professionals to provide to Networx longstanding, state-of-the-art security practices.

In addition to the Qwest functions described above, [redacted] Networx Managed Security Services, as identified within the Networx Enterprise RFP. [redacted]

[redacted] By adding this team of professionals experienced in delivering customer-specific security services to our proven enterprise risk management program, Qwest brings a comprehensive approach to security for Networx.

[redacted] Qwest Networx Security Team provides integrated full-service communications security solutions that meet or exceeds the requirements of Agencies. Given our extensive work with Agencies in managing security practices and obtaining certification and accreditations, the Qwest Networx Security Team has the experience necessary to adapt and grow with the Networx contract, enabling GSA and Agencies to take advantage of the emerging security technologies that will provide a comprehensive security solution for Government communication challenges.

Specifically, Qwest will be proactive in ensuring that security is considered as a part of any new deployments or changes to services and OSS, as described in the Qwest Security Plan, Section 5.0 of Appendix 2. Qwest will ensure that security is considered and is built into the following: new Networx services, deployments and enhancements; new OSS deployments and enhancements; and Networx services and OSS configuration changes.

Through our highly integrated risk management program and key team members, Qwest has the policies, processes, practices, procedures, tools, systems, and reports to assist Agencies in meeting both current and future security challenges. Qwest supports continuous improvement in our programs and learning for our professionals, by supporting key professional certifications and engaging in industry standards and best practices forums. Qwest security professionals carry a diverse set of certifications based on their roles, including: Certified Information Security Manager (CISM), Certified

Information Systems Security Professional (CISSP), Certified Information Systems Auditor (CISA), Certified Business Continuity Planner (CBCP), Certified Fraud Examiner (CFE), Certified Protection Professional (CPP), Global Information Assurance Certification (GIAC) program certifications, and a wide variety of vendor-specific credentials. In all, Qwest engages with [redacted] standards and best practices forums, many of which develop security practices and standards as new technologies emerge.

Notably, Qwest is involved in the following security-related bodies: [redacted] to develop best practices in a variety of security areas focused on the telecommunications industry; standards setting groups [redacted] effort; [redacted] to address security best practices in this important, emerging telecommunications area. We also work with a variety of other industry working groups, commercial organizations, and Government-sponsored organizations and research teams to foster a more secure telecommunications environment, [redacted]

3.3.3 Security Management Capabilities

3.3.3.1 Controls (comp_req_id 10180, comp_req_id 10177, comp_req_id 10242)

In addition to the information provided in this Section regarding Qwest's security planning and management, operational and technical controls, the Qwest Networx Security Plan meets the requirements specified in Section C.3.3.2.2.1. In addition to the information provided in Sections

3.3.3.2 through 3.3.3.4 regarding our proactive security program and approach to risk assessment, our Networx Security Plan will include details on the specific risk analysis approach, scope, and methodology that will be employed throughout the life of the Networx contract. This includes our approaches for continuous security improvement through innovation. The Networx Security Plan is included as Appendix 2 to the Qwest Networx Enterprise proposal.

Qwest's approach to ensuring the effectiveness of our management, operational, and technical security controls includes a broad set of regular audit and assessment activities, and formal compliance management processes, as defined in NIST SP 800-14 pertaining to ensuring the integrity, confidentiality, and availability of Government information and data. Formal compliance reviews are conducted by both internal and external parties, to ensure all findings of such assessment activities are addressed in a timely manner.

On an ongoing basis, the integrated Networx Security Team will conduct security risk analyses, reviews, assessments and/or evaluations of Qwest's Networx services. [redacted] The objective of these reviews is to provide verification that the controls selected and/or installed provide a level of protection commensurate with the acceptable level of risk for Qwest's Networx services.

Without these proven processes, the security of Qwest's Networx services may degrade over time as technology changes, systems evolve, or people and procedures change. This ongoing review process provides assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

In addition to these ongoing assessment activities, Qwest engages in ongoing Research and Development (R&D) in security-related products, functions, and services. Dedicated security engineers perform these directed R&D projects [redacted]. Qwest also supports extensive work in industry forums and standards-setting groups [redacted]. Together, these activities ensure both the effectiveness and innovative nature of Qwest's security program.

Qwest provides and maintains real-time operational procedures and capabilities for detecting and monitoring suspected abuse or intrusions to the network. Alarms are set off for those events that require immediate attention by the GSA PMO, affected Agency or site, and/or Qwest staff. Sections 3.3.3.2.3 and 3.3.3.4.1 provide details on Qwest's approach and capabilities.

3.3.3.2 Management Controls (M.3.11(a), comp_req_id 10213, comp_req_id 10222, comp_req_id 10259, comp_req_id 10260, comp_req_id 10261, comp_req_id 10225)

Qwest understands and agrees to the Government's definition of "Information Systems" in C.3.3.2.2.5, and will employ appropriate security controls as called for by Networx requirements in protecting such systems. Specifically, Information Systems will include but not be limited to the OSS, audio and video teleconferencing, reservations systems, repositories of Agency network configurations, repositories of users' identification and authorization information, and Call Detail Records (CDRs). At the request of the Government, Qwest will provide evidence within 60 days (for example, test results, evaluations, and audits) that security controls, as specified in our Networx Security Plan, are implemented for Networx services and OSS. .

Qwest will assess and test our Networx services and OSS-related security controls and their operating effectiveness per all applicable NIST standards, including NIST SP 800-53 and FIPS-200 specifications, and we will provide the Government all relevant assessment results and audit reports. The types of evidence to be provided to the Government include audit reports, scanning data, and additional applicable test results. Qwest will approach security as specified in our Information Security Framework, referencing NIST SP 800-53, FIPS-200 and all other applicable NIST guidance, as well as contemporary industry best practices. The delivery mechanism for evidence can be either electronic (encrypted for transmission), paper, or both. Qwest will supply initial assessment reports within 60 days of a Government request. The timeline for subsequent reports will be consistent with Government expectations as arranged through the Qwest Networx Security Manager working with the Networx PMO. Evidence reported will reflect the current operating environment. Updates to the environment will be reflected in updates to assessment reports, as applicable.

Our comprehensive approach to security management and practices provides a proactive program that focuses on risk assessment to prevent security events, resolve network vulnerabilities, and to minimize the impact if an event does occur. As described in Sections 3.3.3.4.2 and 3.3.3.4.3, Qwest currently employs formalized processes to both prevent and manage security events, including potential breaches of our network, OSS, and databases. While the preventative practices focus on detailed vulnerability management, the event management processes also include specific post-event gap analysis and review activities, to identify any additions or changes that can prevent a subsequent event. The Qwest integrated Networx Security Team will work with the Qwest Networx CPO to identify all security-related and network vulnerabilities pertaining to the Networx infrastructure, and take the necessary actions to mitigate the threat, and, if possible, eliminate it. Specifically, the Team has the requisite skills required to, upon request, advise Agencies how to best deter security breaches when using Qwest Networx services.

Qwest has rigorous security policies, standards, and processes that are enforced by Qwest Risk Management on authority granted by the Qwest Board of Directors, to effectively manage security risks associated with mission-critical information systems such as those supporting Networx. [redacted]

The Networx Security Plan details the methods Qwest employs to improve our overall Networx security posture over the life of the contract.

Qwest organizations, as described above in Section 3.3.2.2, systematically identify and manage security risks using formal risk assessment and compliance assurance processes to provide ongoing review of the state of controls versus documented policy. Updates to controls, including ongoing risk assessment and vulnerability management to stay abreast of the ever-changing security climate, are managed through initiatives [redacted]. Updates to controls are made in collaboration with specific operations and business unit groups, including product development where new controls [redacted]. In addition to these formal assessment and risk management activities, Qwest also fosters a strong collaborative model across all areas with a stake in security practices, as shown in Figure 3.3.1-1. For instance, in addition to specific enforcement activities [redacted]

[redacted] across the wide variety of technology environments we manage as a telecommunications provider.

Qwest will also conduct security assessments and vulnerability analysis on the infrastructure of our Networx subcontractors. Working with the CPO Subcontract Manager, the Qwest Networx Security Manager will ensure a process-based risk assessment approach and ensure physical security controls are in place with Qwest's subcontractors, who have access to Government information. Qwest will ensure that subcontractors provide verification of their security controls on a periodic basis, and report the results to the Qwest Networx Security Manager, who in turn will include it in Qwest's [redacted] risk assessment. Preparing subcontracts that include security requirements in support of Risk Assessments enables Qwest to confirm that subcontractors comply with all Federal, corporate, and legal requirements. The Qwest Subcontracts Manager has the primary responsibility for administering subcontracts, and will work closely with the Qwest Networx Security Manager to monitor security compliance. Risk assessments require a clearly defined scope of specific services provided, along with detailed information sharing from Agencies. Qwest will prepare a risk assessment report to communicate actions taken by Qwest, subcontractors, and suppliers to maintain Agencies' security environment at an acceptable level of risk

Qwest has strategic vendor relationships and participates in industry forums to keep up with security practices and stay at the forefront of developing new processes, tools, and technologies in our products and underlying support structure. Qwest will ensure that all Networx OSS and service components software have current security updates and patches for all known vulnerabilities throughout the life of the contract. As Qwest

Operations receives software update inputs or requests for new products for the Qwest infrastructure, the integrated Networx Security Team reviews network security enhancements, equipment vendor notifications, and software products with the Qwest Networx CPO and GSA Networx PMO. Qwest is committed to an open discussion with the Government in order to identify benefits and/or risks to the Qwest Networx infrastructure before deployment of these new processes and technologies.

This collaboration between Risk Management and key stakeholders from ensures that initiatives and risk remediation occur team wide in an atmosphere of cooperation, taking advantage of the collaboration of design expertise from the entire organization. We ensure that the best Qwest minds and resources are considering Agency security challenges and needs. With key stakeholders involved in a centrally-orchestrated strategy, Qwest has proven it is possible to drive formal processes, ensure risk awareness with key leaders and stakeholders, provide user awareness training, institute a central Cyber Incident Response Team (CIRT) process, perform business-continuity planning, and build compliance-based security into Qwest networks from the onset. This centrally-orchestrated strategy is also used [redacted] based on clear guidance gleaned from best practices, business priorities, and technical feasibility.

This partnering strategy enables a centralized reporting model, including mechanisms for the design, collection, and publishing of risk-based metrics, and provides a compliance assurance read-out to highlight known risks within technology/process owner groups. The risk-based metrics include results of risk assessment tests, scans, and security assessments compliant with NIST SP 800-30, other applicable NIST standards, and commercially-accepted best practices as applied to Networx-related infrastructure, Networx services, and OSS. [redacted] We monitor compliance with Qwest policies and standards, along with key industry and international standards used as underlying guidance (for example, NIST 800-14, ISO 17799, industry practices, and related publications). Qwest collaborates with our key team members to remediate known risks and improve our posture while adhering to business priorities.

[redacted]

[redacted]

Along with all of these internal communications and compliance management measures, Qwest works with Agencies on protection features and improvements to our products and services. The development of these features often results from the strategic security planning with hardware and software vendors, network suppliers, and subcontractors.

In summary, Qwest follows a systematic risk assessment and evaluation process to identify the threats and vulnerabilities that could impact Qwest, both internally and externally. The risk assessment and validation process covers existing infrastructure and products, which is further emphasized by Qwest's commitment to employing real-time monitoring and methodical technical assessment approaches as our basis for compliance assurance. Established, strong relationships with hardware and software vendors, network suppliers, and subcontractors are also vital for timely vulnerability notification and remediation efforts as part of Qwest's information security vulnerability management program. These remediation efforts include the collection and analysis of data about incidents affecting information systems and networks, in order to highlight root causes, business impacts, and appropriate follow-up actions. This program also tracks risk remediation activities across Qwest, and reveals risk dependencies between systems and risk pinch points.

3.3.3.2.1 Integrity, Confidentiality, and Availability of Information (L.34.2.3.3(a), comp_req_id 10206, comp_req_id 10202, comp_req_id 10207, comp_req_id 10208, comp_req_id 10209)

Qwest understands the Government's requirement for the integrity, confidentiality, and availability of information, and we are highly skilled in meeting such challenges. Securing the Qwest infrastructure to protect our customers' information assets requires the collaboration of [redacted] various Operations organizations, both within Qwest and within our key team member organizations [redacted]. As provided in our description of the Qwest organization and management controls, this collaborative model ensures consistent, strong practices for risk assessment, policy making, threat remediation, and implementation of best security practices across a variety of technology spheres [redacted]. The Qwest Networx Security Manager will draw from these experiences to ensure the Networx program benefits from Qwest's history and the innovations we will bring in security management, as risk management continues to evolve.

Qwest will ensure data integrity for the Networx program by providing Agencies with a security solution that offers unsurpassed next-generation, state-of-the-art controls. This security solution will, in conjunction with policies, standards, guidelines, data classification, records management, and compliance oversight, ensure confidentiality of Agency data. This includes appropriate measures to handle data to the Sensitive But Unclassified (SBU) level, public trust, and where identified by the Government in DD254, to the Top Secret level. Additional details on how Qwest provides for data confidentiality through operational and technical controls are provided in Sections 3.3.3.3 and 3.3.3.4.

Qwest strongly supports the needs of Agencies to employ their own content-level controls such as encryption, and we will support transmissions of this content in a transparent and effective manner. Qwest will provide protection from modification of information for the Networx program by providing a total security solution.

Qwest understands the need to ensure strong access control measures are in place to manage identification, authentication, and authorization for those personnel involved in providing Networx services. Qwest will identify and authenticate Qwest personnel and Government personnel who are authorized to place orders or to access network management information. [redacted] Qwest's integrated Networx Security Team, in conjunction with the Qwest Networx CPO and the GSA Networx PMO, will identify all personnel with a need to access Networx systems and data to ensure that they are given the necessary access credentials to perform their required Networx duties. These processes and procedures protect Government information from unauthorized modification.

In addition to the internal interaction of the various Qwest organizations detailed here, Qwest is also involved with various Government and industry organizations [redacted] to help Qwest stay abreast of the latest security best practices. Qwest takes an active role in establishing these best practices and in sharing our experiences to promote a stronger telecommunications security posture for the nation's critical infrastructure. In this manner, Qwest will ensure the Networx program will remain at the forefront of new security technologies, practices, and processes needed to maintain the highest level of integrity, confidentiality, and availability across such diverse environments.

3.3.3.2.2 Security Needs of Heterogeneous User Community (L.34.2.3.3 (b))

Qwest fully understands the dynamics of a heterogeneous user community that may have many different security needs and requirements as so often face Agencies today. To meet the security needs of the Networx community, [redacted] security solution that provides end-to-end security controls that are layered, starting with the Qwest backbone transport, Frame Relay, MPLS cloud, and IP network, and then moving outward to edge services that include Managed Tiered Security Services.

Qwest takes a lead role in developing standards, working with vendors, and implementing new, innovative approaches to improve our products, including security services. [redacted]

Qwest security policies and organizational practices, along with best industry security standards, provide a seamless Agency interface to the Qwest Network in support of a wide ranging set of users, equipment types, and requirements as called for in the Networx environment.

3.3.3.2.3 Waste, Fraud, and Abuse (L.34.2.3.3(c), comp_req_id 10268, comp_req_id 10267, comp_req_id 10266, comp_req_id 10262, comp_req_id 10242)

[redacted] Qwest currently employs

a state-of-the-art fraud detection system, which will be utilized on the Networx program along with a series of other prevention and detection controls to quickly identify and resolve potential fraud and/or abuse situations. In addition, Qwest will act as a consultant to Agencies, supporting their efforts to minimize fraud, and to identify, and potentially prosecute, fraud perpetrators.

[redacted] Qwest segregates international, Caribbean, toll-free, domestic, and unbilled toll usage In addition to real-time calling analysis, Qwest reviews daily calls and minutes that establish an Agency historical profile. Qwest will investigate, research, and resolve "annoyance calls" as reported by the Government irrespective of circumstances. Qwest will investigate incidents of programmed systems and network computers found to be programmed in error. This will occur whether it is Qwest or the Government that suspects fraud. Qwest will perform calling pattern analysis prior to and after billing at all times, including when Qwest or the Government suspects fraud. Additionally, when there is a significant variation in the normalized traffic for the Agency, Qwest will:

- Perform message and calling pattern analyses prior to and after billing
- Investigate annoyance calls
- Investigate incidents of programmed system and network computers programmed in error
- Work with Agencies to advise and resolve issues resulting from fraudulent activities.

Qwest will provide fraud detection services, including call pattern analysis capabilities to identify fraud or abuse, to the Government on products and services that are interconnected with the Qwest network[redacted]

[redacted] Specifically, Qwest's fraud detection systems will:

- Continually receive and analyze call detail records
- Provide near real-time view and trending/pattern analysis
- Offer flexible thresholds and scoring allowing for swift changes based on industry trends
- Be developed and supported in-house
- Be customizable to provide a unique identification code for Government calling which will allow specialized fraud analysis along with immediate recognition of Government billing entity
- Perform pattern and trending analysis:
  - Specific to International, Caribbean, toll free, domestic, and unbilled toll by billing entity (e.g., telephone number, trunk group including VoIP, 8xx number, etc.)
  - Notify Government through an established alerting process for suspected fraud or possible usage anomalies

Qwest fraud detection services also include fraud consultation for any issue or question, call annoyance research, prevention measures to reduce fraud exposure, and common safeguards within Agency premise equipment (e.g., international restrictions and lockdown of features/functionality that permit unauthorized access, including voicemail and remote access).

The Qwest Fraud group has developed working relationships with all international carriers for the purpose of disseminating information relating to fraud or potential fraud activities. This proactive sharing of information about suspicious activities on all networks enables Qwest to stay ahead of potential fraud impacting the Qwest network. Qwest continuously monitors and reviews the performance of our international providers and is able to act quickly to resolve any issues by leveraging our relationships with the carriers. The international long distance network is built on bifurcated network architecture with redundancy and fail-safe measures. With multiple carriers on each international route, Qwest is able to switch the provider of each route real-time when necessary.

Qwest's fraud detection system, along with a series of other prevention and detection controls, quickly identifies and resolves potential fraud and/or abuse situations.

Qwest Network Fraud Operations reacts quickly to fraud situations to minimize any exposure and losses that may result from toll fraud. Qwest continuously alerts our customers to new trends in telecommunications fraud, and provides them with up-to-date strategies for protecting themselves against toll fraud.

The Qwest fraud management program regularly assesses current strategies, fraud system performance, and fraud prevention strategies, related not only to the Qwest network, but also to trends that emerge within the industry. This assessment allows Qwest to implement potential safeguards to reduce fraud exposure to Agencies. Qwest participates in various industry fraud organizations [redacted] to assimilate current threats, trends, methodologies, and remedies. As part of our measures, Qwest is continuously contacting Agencies to alert them of potential fraud and assisting them with up-to-date strategies in defending against fraud. Qwest also provides information on our website, www.qwest.com.

The Qwest fraud center proactively and aggressively monitors the Qwest network 24x7x365, to ensure that Agencies receive the highest level of service. Qwest’s state-of-the-art system is continually updated and enhanced to remain efficient and effective in fraud detection. The Qwest fraud management team, as necessary, can rapidly change key thresholds within the system parameters to account for potential emerging threats/trends. Any changes are instantly integrated, and call analysis of the new thresholds starts immediately. Qwest may implement necessary network restrictions involving known fraud entities without impacting Agencies. These preventative steps are implemented to protect Agencies against potential abuse.

Qwest Calling Cards provided to Agencies will be monitored by Qwest’s advanced fraud detection systems for potential fraudulent use, misuse or abuse 24x7x365. If fraud is detected, the Calling Card will be deactivated and the Qwest fraud control center will notify the GSA Networx PMO of the suspected fraudulent calling activity. It is Qwest’s goal to minimize the interruption of service related to the deactivation of a Calling Card due to fraud. Consequently, Qwest will generate a new card for the Agency as quickly as possible. Qwest’s detection parameters include many elements that may be an indicator of unauthorized usage[redacted] Qwest’s Calling Cards can also be restricted from certain types of calling at an Agency’s request, such as no international termination, origination, or domestic only. These restrictions will minimize the potential for fraudulent abuse if the card is compromised.

With respect to Agency premise equipment fraud, Qwest will assist and cooperate fully in efforts to prevent and correct unauthorized use by informing Agencies of suspected fraudulent calling activity. Qwest will proactively consult with the GSA Networx PMO and Agencies regarding defensive measures they can utilize that may reduce their exposure to misuse and abuse associated with the operation of Agency-provided systems, equipment, facilities, or services that are interconnected with Qwest's services.

Qwest also currently employs a series of practices and response teams to identify data services users who may be engaging in practices contrary to the Acceptable Use Policy (AUP), such as sending unsolicited commercial email (also known as "spam"), proliferating malicious software or viruses, or initiating traffic that may indicate a denial of service or other malicious network-based activity. Qwest actively enforces our AUP and works closely with Agencies who may be impacted by such potentially fraudulent activities, including phishing and other Internet threats that are all too common.

Upon identification of specific fraud situations, the Qwest Networx Security Manager will coordinate efforts with the fraud detection and other security functions to provide necessary information and legal processing needed for timely identification and potential prosecution of perpetrators. At the GSA Networx PMO's request, Qwest will selectively block and take other actions which are reasonably under the control of Qwest in order to limit or prevent unauthorized calling resulting from the operation of Agency-provided systems, equipment, facilities, or services. Qwest will also, upon request, assist Agencies in the referral of all relevant information to state or Federal officials for the purposes of prosecuting those individuals responsible for the abuse or misuse of an Agency's service. Qwest will assist the Government in the preparation and submission of relevant information under Qwest's control in all legal actions that the Government may bring against third parties responsible for the abuse or misuse of Qwest's Networx services.

As a provider of communications services globally, Qwest's international coverage extends to [redacted] countries for voice services and to [redacted] countries for data services. This extensive breadth of coverage is due to Qwest's strategy to satisfy the voice and data connectivity requirements of our global customer base, and to provide world-class service with a high level of quality and reliability. [redacted] Based on this strategy, Qwest is able to supply Agencies with best-of-breed service, network connectivity, and mature, well-conceived services. These services also include emerging technologies, such as IP-VPNS and VOIPTS.

As described in Section 3.3.2.2, Qwest has the right organization to plan and implement industry standard security controls and practices across all these environments, to ensure data confidentiality, integrity, and availability of customer and company information in support of our telecommunications services. Our programs also support ongoing relationships and research to ensure we have the right information to provide innovative security solutions, both domestically and non-domestically, as risks evolve.

It is critical to our business that we have service provider agreements under which performance and quality standards are maintained at the highest level. These agreements are administered by our [redacted] organization, which is dedicated exclusively to managing agreements with all domestic and international service providers whether carrier or Postal Telegraph and Telephones (PTTs). [redacted]

[redacted]

In addition, a team of dedicated professionals from Qwest Operations monitors the Service Level Agreement (SLA) performance of our domestic and international providers 24x7x365, and are able to react quickly to any outages or other factors that may impact services. They also obtain credits when service metrics are not met. Our international and domestic service providers monitor their core networks 24x7x365, and are held to the highest standards of quality and reliability to meet Agencies' needs.

[redacted] Qwest [redacted] has developed working relationships with all international carriers for the purpose of disseminating information relating to fraud or potential fraud activities. This proactive sharing of information about suspicious activities on all networks enables Qwest to stay ahead of potential fraud impacting the Qwest network.

Additionally, Qwest continuously monitors and reviews the performance of our international and domestic providers, and we are able to act quickly to resolve any issues by leveraging our relationships with the carriers. The international long distance network is built on a bifurcated network architecture with redundancy and fail-safe measures. With multiple carriers on each international route, Qwest is able to switch the provider of each route in real time when necessary.

Specifically, Qwest will provide the best commercial security practices in supporting service delivery to non-domestic and OCONUS locations. Within 30 minutes of determining a service-impacting or fraud-related event, the Qwest Networx CPO will report verbally to the GSA Networx PMO and the Contracting Officer (CO) any unusual or suspicious outage, blockage, or tampering that may indicate that users of services are being denied service or services are being compromised.

3.3.3.3 Operational Controls (M.3.11(b))

Qwest employs a collaborative approach to set the corporate policies, standards, and processes and to implement the requisite equipment/software to provide the operational controls employed throughout the Qwest infrastructure. For Networx, Qwest will employ an integrated network secure solutions team, consisting of our dedicated Networx Security Manager, [redacted] and the Qwest Networx CPO, to provide the additional level of granularity required to meet Networx-specific requirements.

3.3.3.3.1 Security Requirements and Executive Orders (L.34.2.3.3(d))

Qwest recognizes that security requirements and Executive Orders will require ongoing review to ensure that the overall security posture of Networx services is kept current. To accomplish this, Qwest will maintain current memberships [redacted] along with our activities in standards-setting groups and professional certifications as described in Section 3.3.2.3. The Qwest Networx Security Manager, in conjunction with Qwest Information Security, will be responsible for ensuring the Networx security program stays abreast of and compliant with evolving Government standards, new security requirements, directives and Executive Orders.

3.3.3.3.2 Continuity of Government Services (L.34.2.3.3(e), comp_req_id 10252)

Qwest has years of experience ensuring continuity of services for all Qwest corporate functions and our customers. Qwest is an industry leader in the protection of Government operations and ensuring continuity of Government services. This is accomplished in part by having [redacted] thus ensuring that in any major national event, Qwest will have complete, accurate, and credible information, which helps provide a comprehensive time-saving approach to the restoration of network services.

The Qwest integrated Networx Security Team, in conjunction with the [redacted], will work with the Qwest Networx CPO to ensure that continuity of services is maintained at the day-to-day operational level according to the security requirements identified in L.34.2.3.3 (d).

Additionally, Qwest's integrated Networx Security Team will ensure that all offsite backup and storage of critical Networx services configurations and OSS data and information generated and stored at its facilities will be documented [redacted]

3.3.3.3.3 National Security (L.34.2.3.3 (f))

Qwest Risk Management functions, including our dedicated representative at the NCC for Telecommunications, will support the Qwest Networx CPO by maintaining Qwest's compliance with the Department of Homeland Security Council's National Incident Management System (NIMS). This will provide a consistent, nationwide approach for Federal, state, and local governments to work together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity.

[redacted]

3.3.3.4 Technical Controls (M.3.11(c), comp_req_id 10220, comp_req_id 10215, comp_req_id 10214, comp_req_id 10216, comp_req_id 10221, comp_req_id 10212, comp_req_id 10248, comp_req_id 10203, comp_req_id 10208)

Qwest understands the need to ensure that strong access control measures are in place to manage identification, authentication, and authorization for those personnel involved in providing Networx services, especially technicians who access network elements and routing policies, and who require access to network management and other systems that may include Agency-related information. Standardized identity management controls are described in Section 3.3.3.4.1, and are a key element of our technical controls. Additional detail is provided in Appendix 2, Qwest's Networx Security Plan. Specifically, Qwest will provide and maintain real-time operational procedures and capability for detecting and monitoring suspected abuse for intrusions to the network and set off alarms for those events that require immediate attention by the PMO, the affected Agency or site, and/or contractor staff.

The Qwest integrated Networx Security Team will work in conjunction with the Qwest Networx CPO to validate the access requirements for all personnel requiring access to Networx components and to ensure Agency expectations are met or exceeded for controlling such access. Specifically, Qwest will provide access controls consistent with Federal Government accepted security principles and practices, per NIST SP 800-14, or better, to protect its infrastructure and switching systems from attacks via publicly accessible ports (e.g., maintenance ports).

As detailed, Qwest employs a strong set of access controls and other defensive measures to protect our infrastructure[redacted]. These measures are consistent with the principles and practices described in NIST 800-14. Specifically, Qwest will physically protect and prevent unauthorized access to Networx services operations facilities, equipment, material and documents, and any other Networx-related contractor facility and equipment that stores or handles Networx-related information or data.

As a part of Qwest's broad security monitoring and risk management program that meets and often exceeds NIST SP 800-14 and other Government security manuals, Qwest has deployed additional information assurance measures [redacted] to safeguard critical network backbone services and infrastructure against cyber attacks. Details of our current measures and those under development are detailed as key technical controls in Section 3.3.3.4.1.

[redacted] has the responsibility of setting policies, standards, and processes, and implementing the requisite equipment/software to provide the technical controls for the Qwest network. As described in Section 3.3.3.4.1, Qwest employs a series of technical controls to protect network elements, in addition to access control and management.

The specifics on access control policy are [redacted] Specifically, Qwest will ensure that our access controls provide access to network management or Government-related information only to authorized contractor personnel and Government personnel. [redacted]

[redacted]

Qwest's integrated Networx Security Team will work in conjunction with the Qwest Networx CPO to identify personnel that will require access to any network elements to perform their Networx duties and ensure this data is flowed to the proper Qwest personnel to ensure access is granted.

Specifically, Qwest will adhere, as applicable, to Federal Government accepted security principles and practices per NIST SP 800-14, or better, to protect our transmission facilities, switching components, network management systems and other essential contractor facilities from denial-of-service attacks, intrusions and other perceived threats.

As detailed in this section, Qwest maintains a series of technical controls and has processes in place not only to prevent security events but also to rapidly detect, respond, and communicate with appropriate program contacts in the unlikely event that a breach does occur.

3.3.3.4.1 Protection Measures (comp_req_id 10242)

As a part of our broad security monitoring and risk management program, Qwest has deployed a variety of information assurance measures to safeguard critical network backbone services and infrastructure against cyber attacks, preventing and/or minimizing the impact of any possible security disruptions. Upon contract award, the Qwest's Networx integrated Security Team will ensure that any additional infrastructure or technical controls required to support the Networx contract are included in our Networx Security Plan. Detailed technical controls currently in place and offered by Qwest may be best understood as a set of tools and techniques used within the Qwest infrastructure, and a series of service offerings provided to Agencies to further improve their own security posture.

Existing protections, along with innovative solutions targeted to thwart cyber attacks within the Qwest infrastructure, include but are not limited to the following controls:

- Configuration management controls ensure network element configurations and software images conform to vendor and industry best common practices and recommendations. [redacted]

- User and protocol access controls restrict access to the management and control planes of the network elements, including use of encryption and two-factor authentication methods. Rate-limiting and blocking of protocols directed specifically to the network elements, along with blocking of management and control plane traffic to network elements from non-trusted sources, provides further protection.

[redacted]

- IP spoofing prevention measures include implementation of anti-spoofing technologies on the majority of our edge and border routers to prevent spoofed network attacks from entering the Qwest network[redacted]
- Comprehensive monitoring and alarming of infrastructure components provides real-time monitoring of network elements with alarm notifications to the Qwest Network Management Center (operating 24x7x365) and rapid response to events that may indicate a security issue, utilizing standard processes, tools, and techniques as described in Section 3.2, Network Management.

- Denial of Service and Distributed Denial of Service (DoS/DDoS) monitoring and mitigation measures include: flow monitoring across our border routers to provide proactive attack identification and mitigation; Qwest and Agency-initiated IP address [redacted]
- In-depth certification testing ensures comprehensive hardening, testing, and ongoing auditing of the network elements including routers, switches, and servers.
- Robustness and failover of IP traffic and backbone services provides rapid recovery and minimal Agency impact from events using techniques and capabilities such as: [redacted] systems that provide a highly, geographically redundant, DNS service; redundant router and circuit links in each point of presence; and additional capabilities currently under development, including enhanced backbone traffic separation for different risk domains.
- Virus protection controls, including anti-malware/anti-spyware controls are incorporated at multiple layers in the Qwest infrastructure. We accomplish this mission via clear standards-setting, and a vendor diversity strategy to ensure the timeliest response to new threats and well-defined, operational incident response procedures. [redacted] Virus pattern updates are pushed out to the users using regularly

scheduled, automated techniques that can be executed more rapidly in times of emergencies, ensuring the latest viruses are recognized and deleted. On email systems connected to the Internet, content scanning on incoming and outgoing email messages for malicious code is also conducted with real-time updates for virus pattern files, along with an aggressive file attachment blocking strategy. [redacted]

- Logical perimeter security and intrusion detection/prevention techniques ensure the Qwest infrastructure is protected from Internet-borne threats or unauthorized access through our network connection points. Techniques include a variety of firewall, intrusion detection and prevention, and other protective controls, including two-factor authentication for remote access users.
- Standardized identity management controls ensure that all those who access Qwest systems are granted unique identifiers and are given access only to those systems for which they have a specific business need. In addition to this least-privilege model of security, Qwest also employs two-factor controls, such as tokens and digital certificates, for access to critical elements and remote access to our networks. [redacted] are restricted to authorized users with access based on demonstration of a specific business need-to-know (least-privilege model).

The policies and standards governing the appropriate use of security credentials, including the rules for requesting, granting, authorizing, approving, using, resetting, modifying, revoking, auditing, and deleting credentials and passwords are owned by the Information Security organization. Specific credentials and mechanisms are selected for network elements according to risk factors and their technical capabilities.

While Qwest employs extensive controls within our infrastructure as described above, a complete security posture for Agencies is made available through the following additional security technical controls we are offering to fulfill the Networx technical requirements:

- The Qwest Managed Firewall Service (MFS) provides a comprehensive management service, delivering three levels of tiered service, a multitude of value-added features, and a robust offering of Service-Enabling Devices (SEDs) to meet the requirements of GSA and Agencies.
- Qwest's Intrusion Detection and Prevention Service (IDPS), Qwest can offer Agencies effective systems and processes to: monitor their networks for attacks, misuse, and anomalies; detect and record such intrusions; and begin immediate corrective responses.
- The Qwest Vulnerability Scanning Service (VSS) allows Agencies to conduct effective and proactive assessments of critical networking environments, enabling the rapid correction of vulnerabilities before they are exploited.
- The Qwest Anti-Virus Management Service (AVMS) provides detection and removal of system viruses before they can do critical damage to business operations.
- The Qwest Incident Response Management Service (INRS) provides incident response capability assessment, an incident tracking system, a

mock crisis management scenario, incident response support services, and on-site support.

- The Qwest Managed E-Authentication Service (MEAS) provides design, implementation, and operational capabilities for both token-based and certificate-based e-authentication services in a variety of hosting and operational environments. We also offer significant capabilities in identity management, access control, and biometrics.
- The Qwest Secure Managed Email Service (SMEMS) will provide Agencies with the ability to: centralize and assure inbound and outbound email policy compliance; administer these email services; meet legal and regulatory requirements on email retention; achieve desired levels of security/privacy [redacted] [redacted] and the ability to leverage the cost effectiveness of the Internet while providing confidentiality, integrity and availability of email services that have become expected in Federal business.
- The Qwest Managed Tiered Security Service (MTSS) provides Agencies with security solutions that can be customized for Agencies based on the respective level of mission criticality and information sensitivity.

Together, these controls within the Qwest infrastructure and security service offerings provide Agencies an opportunity to build a comprehensive security posture using proven solutions, as well as new innovations currently under development. Qwest service offerings across all of the Networx service categories include their own, specialized controls to protect Agency information, and also offer Agencies a customized set of technical controls to ensure a strong security posture. Qwest team members are experienced in applying these products and services to specific Agency situations.

3.3.3.4.2 Vulnerabilities and New Threats (L.34.2.3.3 (g), comp_req_id 10210 comp_req_id 10223, comp_req_id 10224)

Qwest is committed to a proactive approach for the identification of vulnerabilities and new threats that may pose a security risk to Networx products and services. The following Qwest process, [redacted] identifies how the Qwest integrated Networx Security Team reduces vulnerabilities, adapts to new threats, and ensures that Networx security management capabilities are maintained to the latest standards and practices. Additionally, Qwest's approach and methodology for protecting our infrastructure also applies to our vendors and subcontractors. Qwest uses the same technical, managerial, and operational controls to protect our infrastructure from all domestic and non-domestic entities (including Qwest subcontractors).

[redacted]

[redacted]

[redacted]

The Networx Security Manager will keep the Qwest Networx CPO and GSA Networx PMO apprised of the status of any Networx-impacting security alerts and the results of patching and/or other appropriate mitigation plans undertaken by Qwest. Feedback is input to the loop closure process to ensure effective information assurance management, and is included in regular reports to drive a process of continuous improvement.

Qwest is committed to the protection of our infrastructure. We have taken a proactive approach to the identification and timely remediation of vulnerabilities and threats that may pose a security risk to Networx products and services as discussed in Sections 5.0 and 12.0 of the Networx Security Plan. Qwest supports a proactive set of planning and management controls, including security-related policy making, evaluations, and risk assessments, in order to make security practices a priority as new products, services, and other infrastructure components are contemplated. In addition to implementing this proactive vulnerability management process, Qwest also takes measures to further protect our infrastructure from any information threats or attacks (e.g., threats from hackers, criminals, and terrorist activities) in accordance with information assurance and security best practices. Qwest's current security breach detection/prevention practices include regular assessments and reviews for effectiveness that include closed-loop compliance assurance methods to continually improve those processes. These reviews, along with Qwest's extensive security expertise and experience with guiding innovative security technologies, provide information used to continuously improve Qwest's security breach detection/prevention practices, including development and application of new techniques. Qwest currently employs formal processes to both prevent and manage security events, including potential breaches of our network, OSS, and databases. While the preventative practices focus on detailed vulnerability management, the event management processes also include specific post-event gap analysis and review activities, to identify any additions or changes to prevent a subsequent event. Our comprehensive approach to security management and practices as described in Section 3.3.3 provides a proactive program that focuses on risk assessment to prevent security events, or to minimize the impact if an event does occur. Additionally, to further the state-of-practice for proactive security measures across the Internet community, Qwest participates in a number of industry forums and standards organizations [redacted]

[redacted] to develop best practices in a variety of security areas focused on the telecommunications industry.

As described in Sections 3.3.3.4.1 and 3.3.3.4.2, Qwest currently employs formal processes to both prevent and manage security events, including potential breaches of our network, OSS, and databases.

Our comprehensive approach to security management and practices as described in Section 3.3.3.1 provides a proactive program that employs all commercially reasonable, prudent measures, including a focus on risk assessment to prevent security events, or to minimize the impact if an event does occur. These processes are consistent with widely accepted practices such as those described by the NIST 800 series.

3.3.3.4.3 Networx-related Security Breaches (L.34.2.3.3(h) comp_req_id 10240, 10241)

The threat climate and risks to technology components, such as the Qwest network, OSS, and databases, are dynamic in nature. Qwest therefore takes a proactive approach in developing methods to prevent, detect, and report security breaches of its network, OSS, and databases. Qwest's current security breach detection/prevention practices include regular assessments and reviews for effectiveness that include closed-loop compliance assurance methods to continually improve those processes. These reviews, along with Qwest's extensive security expertise and experience with guiding innovative security technologies, provide information used to continuously improve Qwest's security breach detection/prevention practices, including development and application of new techniques.

The Qwest integrated Networx Security Team's commitment to Networx is to provide reliable security services to the Government that meet or exceed the requirements set forth in the Networx RFP. In the event that there is a security breach, Qwest will maintain a multi-pronged approach to meet a variety of technology scenarios. These depend on the location of the detected security-related event, either on the Agency or Qwest infrastructure, Regardless of the event's source, the Qwest integrated Networx Security Team will ensure that all incidents are reported within the required time frame, including a verbal notification to the GSA Networx PMO and affected Agencies within fifteen minutes of initial discovery and within four hours for results of investigations and corrective measures applied. A written Security Breach Notification Report will be submitted within seven calendar days of said breach and a monthly report detailing all security breaches for that month will be provided.

If a security-related event is detected and is found to have taken place in the Agency infrastructure, those events will be detected by the SOC via the specific security services. The SOC will coordinate with the Agency involved, following established escalation and reporting mechanisms already agreed upon. Depending on the types of security services utilized under the Networx contract by that Agency, follow-up and remediation activities will commence. If the Agency decides to engage law enforcement, Qwest will provide subject matter expertise and any Agency-specific data that is required.

[redacted]

This process [redacted] includes specific criteria and procedures for engaging operational groups [redacted]

[redacted]

[redacted]

[redacted]

The Qwest Networx Security Manager or his designee will be notified and will be responsible for providing information to the GSA Networx PMO to include the event status and potential impacts, if any, to Agencies. This will ensure effective communications and follow-up for all events.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3.3.4 Security Summary

Qwest understands GSA’s need to ensure the security of the networks, computing infrastructure and OSS, physical environment, and personnel engaged in satisfying the requirements of the Networx program, while also strengthening the overall information security posture against a variety of threats for Agencies using Networx services. We share the GSA’s high-priority concerns for protecting the nation’s critical infrastructure services, and are both experienced and well-positioned to meet this need. In addition, Qwest understands that managing today's security risk levels requires a broad view across a variety of technologies and therefore Qwest provides a strong set of security-related offerings tuned to each Agency's information technology environment and security needs. By building on our pre-existing leadership and experience in the areas of risk management, information security, disaster preparedness, and operational knowledge, we will ensure the confidentiality, integrity, and availability of Networx-related data and communications.