3.1 APPROACH TO ENSURE INFRASTRUCTURE SECURITY (L.34.1.3.1)

Qwest maintains one of the most secure communications infrastructures commercially available [redacted]

Qwest Information Security-related functions are performed in collaboration with Qwest's Operations organizations, as follows:

[redacted]

These security functions interoperate with operational management for all transport services. Qwest's security management organizations have extensive capabilities that provide the Networx Program Management Office a strong, dedicated partner that understands the security challenges the Government faces. This is demonstrated through Qwest's numerous, well-established security policies, standards, and processes. Conducting ongoing risk assessments of individual systems, network elements, and end-to-end system testing are also a normal part of Qwest's security processes.

Qwest security management processes include:

[redacted]

[redacted]

[redacted]

[redacted]

3.1.1 Mechanisms and Controls (L.34.1.3.1(a))

Qwest has a long history of providing industry-leading network management and security services to protect Qwest and its customers against threats, attacks, and system failures (including physical plant, hardware, and software) that are aligned with best commercial practices. Qwest's network and security-related services are designed to ensure the confidentiality, integrity, and availability of information assets and supporting resources of the Qwest network over its wide range of customers and geographical locations.

To protect the Qwest infrastructure and information assets, including those of our customers, Qwest relies on a detailed risk management methodology that is comprised of a wide variety of controls for security assurance. [redacted]

As a part of the Qwest broad security monitoring and risk management program, Qwest has deployed a variety of information assurance measures to safeguard critical network services and infrastructure against cyber attacks to prevent and/or minimize the impact of any possible security disruptions. Detailed technical controls offered by Qwest and currently in place are best understood as a set of tools and techniques used within the Qwest infrastructure as well as a set of additional service offerings provided to customers, such as the Agencies served by Networx to further improve their own security posture.

Qwest's security risk analysis processes address infrastructure components, such as physical plant, routers, switches, firewalls, and servers,

as well as the processes used to maintain them, along with the environment used to deliver specific security services to Networx Agencies.

[redacted]

To deliver the outstanding reliability of its network, Qwest has established [redacted]

Qwest conducts periodic security risk analyses, reviews, assessments, and evaluations of all Qwest services. The objective of these reviews is to provide verification that the controls selected and installed provide a level of protection commensurate with the acceptable level of risk for delivery of our services.

By using these combined comprehensive processes, we ensure the security of the Qwest infrastructure such that customer service does not degrade over time as technology changes, the system evolves, or people and procedures change. Periodic review provides assurance that management, operations, personnel, and technical controls are functioning effectively and providing adequate levels of protection.

Qwest uses multiple redundant locations to monitor our domestic and international network. A list of key organizations that ensure protection of

Qwest infrastructure and provide security for the services offered to our customers is as follows:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3.1.2 Measures to Protect Against Cyber Attacks (L.34.1.3.1(b))

As a part of our broad security monitoring and risk management program, Qwest has deployed many additional information assurance measures to safeguard critical network backbone services and infrastructure against cyber attacks. These include but are not limited to: Denial of Service (DoS) detection and mitigation; Domain Name Server (DNS) redundancy; pinhole firewalls protecting H.323; Media Gateway Control Protocol (MGCP) in use on Voice over Internet Protocol (VoIP) systems; protection against Signaling System Seven (SS7) attacks; anti-spoofing mechanisms; and Message-Digest algorithm 5 (MD5) authentication for routing updates to prevent routing table corruption.

Specific protections against cyber attacks include:

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

3.1.3 Consistent with Best Practices for Security and Reliability (L.34.1.3.1(c))

As one of the leading communications common carriers, Qwest implements industry-standard security best practices to ensure data assurance, integrity, and confidentiality of customer and company information in support of our telecommunications services. These practices include implementing controls specifically in the areas of personnel, systems, and facility security. Qwest has also implemented comprehensive business continuity and disaster recovery measures and controls to ensure the availability of customer and corporate networks.

To ensure the security architecture stays current with best practices, Qwest takes a lead role in developing standards, working with vendors, and implementing new, innovative approaches to improve our products, including

[redacted]

security services. Qwest maintains relationships with key network equipment vendors to provide a bi-directional dialog on best security practices and new feature development, along with our membership and participation in a variety of industry and standards forums. These include the [redacted]

[redacted]

3.1.4 Approach for Integration of Commercially Available Products/Services (L.34.1.3.1(d))

Qwest takes a lead role in developing standards, working with vendors, and implementing new, innovative approaches to improve our products, including security services. As one of the largest communications common carriers, Qwest maintains relationships via professional telecommunications forums and standards groups along with our membership and participation in a variety of industry trade groups with key network equipment vendors. As these groups develop security solutions and infrastructure security enhancements, Qwest is able to take the best of these recommendations and push for standards-based solutions and implementations in association with equipment vendors and with the backing of the standards organizations or trade groups. ***Figure 3.1.4-1*** describes potential problems encountered and solutions proposed as new security enhancements become commercially available in the timeframe covered by this acquisition.

Figure 3.1.4-1. Discussion of Potential Problems and Solutions

Problem	Solution
[redacted]	[redacted]

Problem	Solution
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

3.1.5 Experience in Certification and Accreditation (L.34.1.3.1(e))

Qwest has extensive experience in the iterative process involved in developing the complex documentation required for the certification and accreditation (C&A) process.

Qwest has performed C&A activities and extensive policy development support for [redacted] years. These activities have been both integrated into the larger scope of security engineering of entire systems and as individual C&A efforts when requested by Agencies and commercial customers. [redacted]

The Qwest Enterprise Security Solutions Group has long been involved in the C&A of information systems, most notably in the area of

networked system test and evaluations, multi-level security system validations, and the development and execution of System Test and Evaluation plans, risk assessments, vulnerability assessments, and System Security Authorization Agreements (SSAAs). [redacted]

Qwest recently supported the [redacted] Standard Operating Procedures were updated and written as required to ensure all operational procedures were fully documented.

Qwest is currently under contract to the [redacted]

Qwest has current and significant experience in developing and implementing secure network architectures. We developed and implemented

the technical security architecture for the [redacted]

Qwest provided support to the [redacted]

Qwest's past experience in conducting security assessments provides an efficient process that will minimize time in response to [redacted] The typical Qwest approach to conducting a security assessment [redacted]