3.1 APPROACH TO ENSURE INFRASTRUCTURE SECURITY (L.34.1.3.1) (M.2.1.1 (B.))(C.2.1.11)

Qwest maintains one of the most secure telecommunications infrastructures commercially available. With an industry-recognized team of engineering security experts, we offer Agencies standards-based security technology and practices.

In providing network security, Qwest Information Security (InfoSec) has matured into an advanced industry-recognized business organization with supporting groups that specialize in the different network areas of today's telecommunications architectures and technologies.

These security functions interoperate with operational management for all transport services. Qwest Information Security-related functions are performed in collaboration with Qwest's Operations organizations, as follows:

[redacted]

Conducting ongoing risk assessments of individual systems, network elements, and end-to-end system testing are a normal part of Qwest's security processes.

Qwest security management processes include:

[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 systems, networks and our customers against threats, attacks and system failures (including physical plant, hardware and software) that are aligned with best commercial practices. Qwest's networks and security-related services are designed to ensure the confidentiality, integrity, and availability of customer information assets. To protect the Qwest network 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.

Qwest has deployed a variety of information assurance measures to safeguard critical network services and infrastructure against cyber attacks and to prevent and/or minimize the impact of any possible security disruptions [redacted]

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 Agencies.

[redacted]

To provide the outstanding reliability of our network, Qwest has established [redacted]

[redacted]

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

These combined comprehensive processes assure the security of the Qwest network infrastructure [redacted] Periodic reviews provide assurance that management, operations, personnel and technical controls are functioning effectively and providing adequate levels of protection.

Qwest also uses multiple Operation Centers, in redundant geographic locations, to monitor our international networks. The key organizations that assure protection of Qwest's network infrastructure and provide security for the services offered to our customers are:

[redacted]

[redacted]

[redacted]

[redacted]

[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 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]

[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 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 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. [redacted]

Qwest has described in Sections 3.1, 3.1.1, 3.1.2, 3.1.3 and in 3.1.5, below, a detailed and comprehensive set of processes and procedures along with their associated Qwest organizations, some of the components that contribute to making Qwest one of the industry leading and recognized communications security companies. Qwest takes a full, complete, and comprehensive view towards achieving a network architecture that is truly consistent with the best practices in the industry for security and reliability. The time-tested and proven successful overarching model for this success is not to depend upon any one element, but to provide multiple layers of security and reliability in a defense-in-depth posture that all contribute to achieving success. [redacted]

[redacted]

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

Qwest takes a leading interactive role in aiding the development of telecommunication standards, working with vendors, trade organizations and implementing new, innovative approaches to improve our processes, products, and 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. For examples of several potential problems that have surfaced within these groups, see ***Figure 3.1.4-1***.

Figure 3.1.4-1. Discussion of Potential Problems and Solutions

[redacted]	[redacted]
[redacted]	[redacted]
[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 process.

Qwest has performed C&A activities and extensive policy development support for more than [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. Recent Qwest customers receiving Certification and Accreditation support include [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 tests 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]

[redacted] Standard Operating Procedures (SOPs) were updated and written as required to ensure all operational procedures were fully documented.

[redacted] The tasking under this contract includes risk and vulnerability assessments of information systems using a variety of open source, commercial products, interviews, and observation.

Qwest has current and significant experience in developing and implementing advanced, secure network architectures. [redacted]

[redacted]

[redacted]

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

[redacted]

Figure 3.1.5-1.Security Services and FISMA Compliance

	FISMA	A-130	FIPS-199	FIPS- 200	800-37	800-53	800-53A	800-59	800-60
Managed Firewall	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply
Intrusion Detection and Prevention	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply
Managed Tiered Security	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply
Anti-Virus Management	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply
Managed e-Authentication	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply
Vulnerability Scanning	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply
Incident Response	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply
Secure Managed email	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply	Comply

Table Key:
FISMA: Federal Information Security Management Act of 2002
A-130: Office of Management and Budget Circular A-130 "Management of Federal Information Resources
FIPS-199: Standards for Categorization of Federal Information and Information Systems
FIPS-200: Minimum Security Requirements for Federal Information and Information Systems
800-37: Guide for the Certification and Accreditation of Federal Information Systems
800-53: Recommended Security Controls for Federal Information Systems
800-53a:Guide for Assessing the Security Controls in Federal Information Systems
800-59: Guidelines for Identifying an Information System as a National Security System
800-60: Guide for Mapping Types of Information and Information Systems to Security Categories