

6.5 ANTIVIRUS MANAGEMENT SERVICES (AVMS) (L.34.1.6)

Agencies are able to leverage their existing infrastructure and add current technologies for antivirus protection using Qwest AVMS, providing protection and removal of system viruses before they can cause widespread damage in both a cost-effective and highly-reliable manner.

Qwest Antivirus Management Service (AVMS) provides detection and removal of system viruses before they can do critical damage to business operations. Qwest is offering two types of AVMS for the Agency:

- Managed gateway-based antivirus (AV), which provides a gateway that scans Web and email traffic for worms, viruses, and malicious content
- A server-based AV, scanning all files and software housed on a specific server, including the operating system. This host-level protection is provided at Agency-specific time intervals

AVMS uses [REDACTED] top AV software and hardware [REDACTED] products for new implementation to scan executable files and incoming traffic for malicious code. AV applications are constantly active in attempting to detect patterns, activities, and behaviors that may signal the presence of viruses. AVMS enables Agencies to procure AV capabilities that protect their infrastructure.

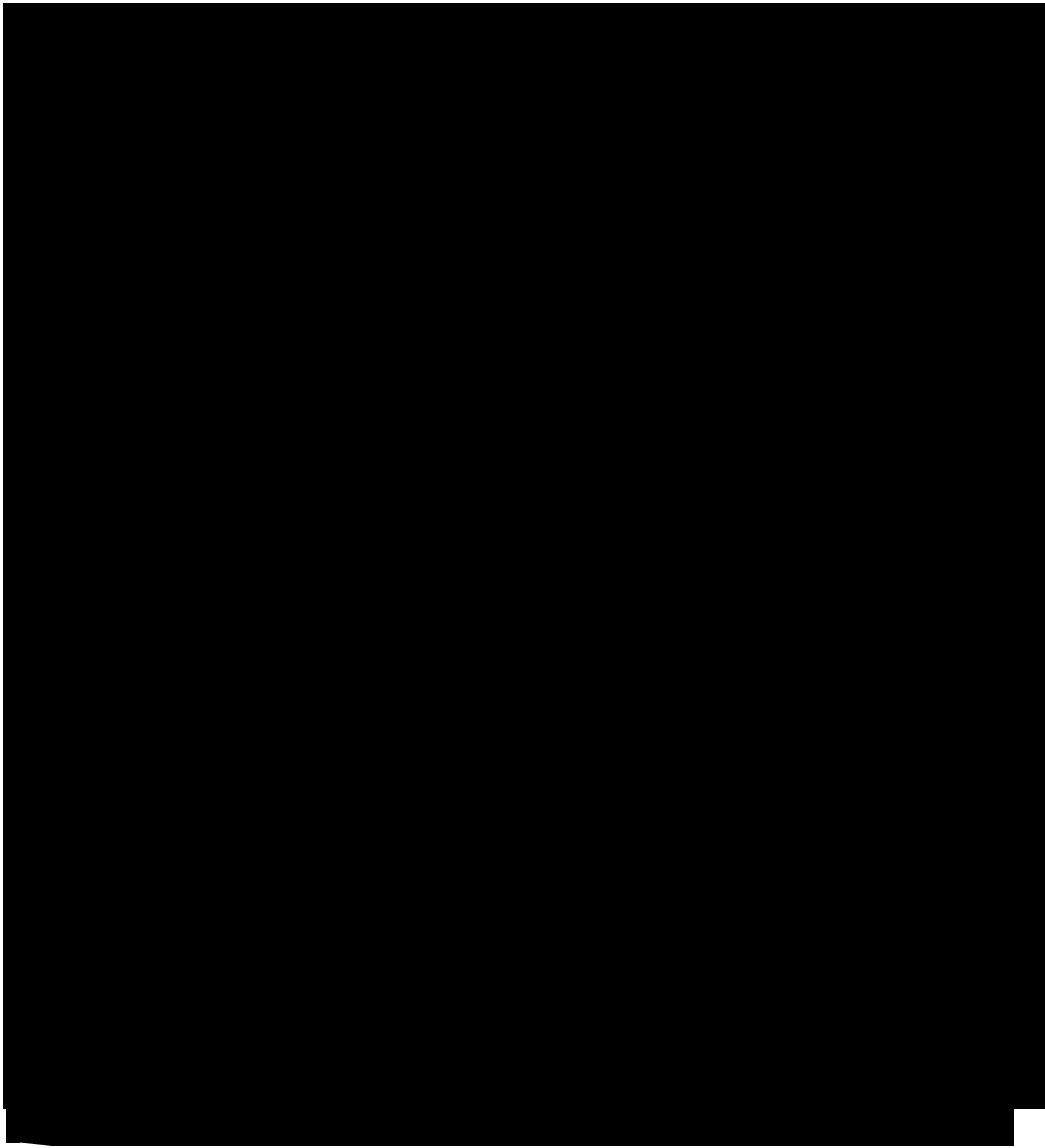
Qwest AVMS is part of an integrated approach to security services. Qwest AVMS extends beyond those of a standard bulk customer Managed Security Service Provider (MSSP). Qwest's approach is to provide an Agency-focused premium service that is vendor and device independent. This allows Agencies to retain their current infrastructure and permits simpler upgrades and technology refreshes in the future.

[Redacted text block]

6.5.1 Technical Approach to Antivirus Management Services Delivery (L.34.1.6.1)

As part of AVMS, Qwest will set up and configure the AV services that scan traffic for viruses prior to forwarding, and quarantine them if infected. After the implementation, Qwest will monitor the AV gateways 24x7x365 from our Security Operations Center (SOC). [Redacted text]

[Redacted text block]



[Redacted]

[Redacted]

[Redacted]

[REDACTED]

**6.5.1.1 Approach to Antivirus Management Services Delivery
(L.34.1.6.1(a))**

Qwest will provide a highly skilled and experienced design and engineering team that will work with the Agency's technical managers and engineers to deliver Agency-specific solutions. Our engineering team will employ industry-certified systems engineering processes that will ensure the Agency's requirements are met. [REDACTED]

[REDACTED]

Qwest AVMS complies with the connectivity requirements in the Request for Proposal (RFP) including interoperability with Agency networking environments, such as Demilitarized Zones (DMZs), secure Local Area Networks (LANs), extranets, and public networks (i.e., Internet).

6.5.1.2 Benefits of Antivirus Management Services Technical Approach (L.34.1.6.1(b))

Qwest's approach to AVMS maintains an approved standard and avoids the obsolescence of legacy systems. Qwest will work with Agencies to export our successful products and services to them. We will reduce redundancy where overlap limits the value of IT investments. **Figure 6.5.1-3** shows some of our discriminators and benefits.

Figure 6.5.1-3 Qwest Discriminators Set Qwest AVMS Apart

Feature	Benefit	
Analysis of the Current Environment	Qwest SOC's evaluation of the Agency's current AV environment provides a baseline service profile which is used to during threat mitigation.	
Documentation of the Computing Environment	Qwest SOC's AV documentation including log reports assists in meeting regulatory requirements.	
Fully Tested Pilot Implementation with supporting Standard Operating Procedure (SOP) documentation.	Qwest SOC engineers adhere to predetermined SOP for AV mitigation that will provide for an efficient manner in addressing AV threats.	

Qwest's AVMS technical approach is effective in providing Agencies with the means to address the Federal Information Systems Management Act (FISMA) of 2002, which requires Agencies to institute information security programs with the ability to manage and annually re-assess risk. Qwest AVMS offering supports the Federal Enterprise Architecture (FEA) as noted in **Figure 6.5.1-4.**

Figure 6.5.1-4. FEA Objectives. *Qwest AVMS supports FEA objectives for improved utilization of Government information resources, cost savings and avoidance, and increased collaboration.*

FEA Requirement	
Improve utilization of Government information resources	
Enhance cost savings and cost avoidance through a mature FEA Government-wide	
Increase cross-Agency and inter-Government collaboration	

6.5.1.3 Solutions to Antivirus Management Services Problems (L.34.1.6.1(c))

Successful delivery of AVMS is reliant upon interoperability, network and system availability, and organizational security practices. We have addressed interoperability issues through a standards-based infrastructure that specifically provides for support of a wide range of in-place AV applications and environments. Network and system availability are addressed through a redundant architecture. In **Figure 6.5.1-5**, below, we present several potential problems and our solution or mitigation approach.

Figure 6.5.1-5. Qwest Solutions to AVMS Problems






Problem	
Antivirus update services require high availability.	[Redacted]
Many users are not AV experts.	[Redacted]
Agencies may have unique networks, systems, architectures, or requirements.	[Redacted]


6.5.2 Satisfaction of Antivirus Management Services Performance Requirements (L.34.1.6.2)

6.5.2.1 Antivirus Management Services Quality of Service (L.34.1.6.2(a))



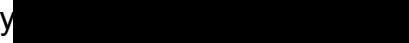
Qwest's AVMS meets all performance requirements, as summarized below in **Figure 6.5.2-1**. We have proven monitoring and measurement systems, procedures, and evaluation methods in place. The required Government performance measures are consistent with commercial standards and we are able to meet each of them.

Figure 6.5.2-1. Qwest Meets All of GSA’s Acceptable Quality Levels (AQLs)

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (AQL)	
Availability	Routine	99.5%	≥ 99.5%	
Grade of Service (Virus Updates)	Routine	Within 24 hours for a Normal priority update	≤ 24 hours	
		Within 2 hours for an Urgent priority update	≤ 2 hours	
Time to Restore (TTR)	Without dispatch	4 hours	≤ 4 hours	
	With dispatch	8 hours	≤ 8 hours	



Availability: Qwest AVMS is delivered through industry-leading security appliances and software which are engineered for near 100% availability 




 Changes initiated by Qwest require Agency consent prior to implementation. Changes are categorized as Normal or Urgent (Emergency 



TTR: 

 All troubles are recorded as Normal or Urgent (Emergency) and routed via the  Trouble Ticket System to the SOC for immediate attention. On a 24x7x365 basis, Qwest will detect, prioritize, isolate, diagnose, and repair faults affecting contract services and restore them to the Agency’s specifications.

6.5.2.2 Approach for Monitoring and Measuring Antivirus Management Services (L.34.1.6.2(b))

[Redacted content]

6.5.2.3 Verification of Antivirus Management Services (L.34.1.6.2(c))

[Redacted content]

6.5.2.4 Antivirus Management Services Performance Improvements (L.34.1.6.2(d))

[Redacted content]

[REDACTED]

**6.5.2.5 Antivirus Management Services Performance Metrics
(L.34.1.6.2(e))**

[REDACTED]
[REDACTED] We [REDACTED] define and implement an associated measurement and reporting approach [REDACTED]
[REDACTED]

6.5.3 Satisfaction of Antivirus Management Services Specifications (L.34.1.6.3)

Qwest's AVMS offering meets the required specifications for capabilities, features, standards, connectivity, and interfaces. Qwest fully complies with all mandatory stipulated and narrative capabilities, features, and interface requirements for AVMS. The following Figure 6.5.3-1, Figure 6.5.3-2, and Section 6.5.3.1.3 summarize Qwest's response to the AVMS capabilities listed in RFP C.2.10.4.1.4, features of RFP C.2.10.4.2, and interfaces of RFP C.2.10.4.3. These subsections are intended to provide the technical description required per L.34.1.6.3(a) and do not limit or caveat Qwest's compliance in any way.

6.5.3.1 Satisfaction of Antivirus Management Services Requirements (L.34.1.6.3(a))

6.5.3.1.1 Satisfaction of Antivirus Management Services Capability Requirements (L.34.1.6.3(a), C.2.10.4.1.4)

Qwest AVMS offering meets the capabilities required in the RFP as enumerated in **Figure 6.5.3-1**.

Figure 6.5.3-1 Qwest complies with all the AVMS requirements

AVMS Capabilities	
1. The contractor shall provide design and implementation services in order to determine the appropriate AV solution suited to Agency needs.	[REDACTED]
2. The contractor shall provide installation, configuration and integration support to the Agency, including testing of service equipment and software.	[REDACTED]
3. As part of the AV service, the contractor shall provide the software and hardware components, including servers and gateways, as required by the Agency. This shall include, as applicable:	[REDACTED]
a. A managed gateway-based AV service which provides a gateway that scans Web and email traffic for worms, viruses, and malicious content.	[REDACTED]
b. A server-based AV service that scans all files and software housed on a specific server, including the operating system. This host-level scanning is provided at Agency-specified time intervals.	[REDACTED]
4. The contractor shall monitor the system on a 24/7 basis for indications of infection.	[REDACTED]
5. The service shall allow real-time and on-demand virus scanning.	[REDACTED]
6. The contractor shall screen incoming and outgoing File Transfer Protocol (FTP), HyperText Transfer Protocol (HTTP), HyperText Transfer Protocol Secure (HTTPS), Point of Presence (POP), and Simple Mail Transfer Protocol (SMTP) traffic for possible infection.	[REDACTED]

AVMS Capabilities	
7. The service shall perform data integrity checks and, at a minimum, protect against the following:	[REDACTED]
a. Known viruses	[REDACTED]
b. Behaviors and patterns that may indicate the presence of viruses	[REDACTED]
c. Malicious mobile code	[REDACTED]
d. Different strains of polymorphic viruses	[REDACTED]
e. Viruses residing in encrypted messages and compressed files, as required by the Agency	[REDACTED]
f. Viruses in different languages (for example, JAVA, ActiveX, and Visual Basic)	[REDACTED]
g. Trojan horses and worms	[REDACTED]
h. Macro viruses	[REDACTED]
8. The service shall respond to infections and violations of the Agency networking environment and provide the following minimum capabilities:	[REDACTED]
a. Alert Service:	[REDACTED]
i. Systems/Network Administrator notification via email, pager, fax, or telephone, as directed by the Agency's notification procedures.	[REDACTED]
ii. Sender and recipient notification, in case of email-borne virus	[REDACTED]
b. Infected file isolation for cleaning, deletion, or post-alert analysis and interpretation	[REDACTED]

AVMS Capabilities	
c. Control of user access and environment for the malicious file	[REDACTED]
9. The contractor shall maintain the AV system and perform the necessary hardware/software upgrades, updates, and replacements.	[REDACTED]
10. The contractor shall deploy the latest system patches and bug fixes as soon as they become available in order to ensure optimal performance of the service.	[REDACTED]
11. The contractor shall provide automatic and timely updates of the virus pattern and signature files as they become available to ensure adequate protection.	[REDACTED]
12. The contractor shall perform periodic gateway scans capable of revealing any vulnerabilities of the AV system.	[REDACTED]
13. The contractor shall perform configuration changes as initiated and prioritized by the Agency. Changes initiated by the contractor require Agency consent prior to implementation.	[REDACTED]
14. The contractor shall provide the Agency with secure Web access to logs and service information, which shall contain, but not be limited to, the following, as applicable:	[REDACTED]
a. Infections detected	[REDACTED]
b. Malicious emails	[REDACTED]
c. Rule violations	[REDACTED]
d. Traffic/mail statistics	[REDACTED]

AVMS Capabilities	
15. The contractor shall support networks of varying complexity in terms of size, bandwidth, and speeds.	

6.5.3.1.2 Satisfaction of Antivirus Management Services Feature Requirements (L.34.1.6.3(a), C.2.10.4.2)

Qwest AVMS offering provides a [REDACTED] solution to meet the required features as enumerated in *Figure 6.5.3-2*.

Figure 6.5.3-2. How Qwest Meets Load Balancing Requirements

Name of Feature	Description	
AV Load Balancing	The contractor shall implement a hardware or software load balancing capability, as applicable. This addresses large systems requirements by distributing traffic across multiple servers.	

6.5.3.1.3 Satisfaction of Antivirus Management Services Interfaces Requirements (L.34.1.6.3(a), C.2.10.4.3)

Qwest provides all required interfaces based upon the capabilities of our proposed services as defined in: IPS (RFP Section C.2.4.1), Premises-based IP VPN Services (RFP Section C.2.7.2), and Network Based Internet Protocol VPN Services (RFP Section C.2.7.3).

6.5.3.2 Proposed Enhancements for Antivirus Management Services (L.34.1.6.3(b))

Qwest will meet the specific requirements for AVMS and is willing to discuss enhancements to the service requirements in the event an Agency has a specific business need or application problem.

6.5.3.3 Network Modifications Required for Antivirus Management Services (L.34.1.6.3(c))

[Redacted]

6.5.3.4 Experience with Antivirus Management Services (L.34.1.6.3(d))

Qwest has many years of providing AVMS for large and small organizations with multiple platforms and products. [Redacted]

[Redacted]

[Redacted] The Qwest Team provides information security services to most Government Agencies as well as to the financial, IT, energy, aerospace, health, entertainment, and publishing industries. We have been providing AVMS management services for the last four years.

[Redacted]

[REDACTED]

Delivering customer-specific design and engineering services [REDACTED]. A prime example of our customer-specific design and engineering services is the work we do for [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

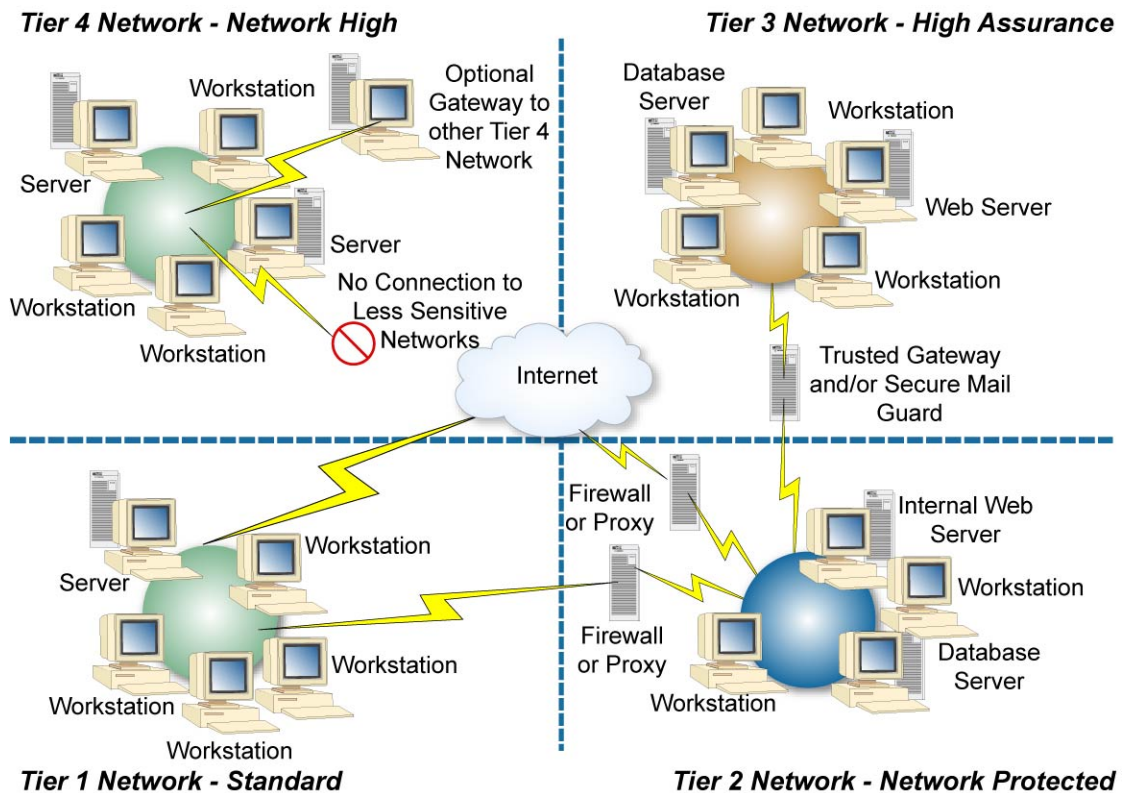
[REDACTED]

6.5.3.5 Managed Tiered Security Services (MTSS) Approach (L.34.1.6.3(e))

AVMS is part of the Qwest MTSS technical solution. Design, implementation, and delivery according to GSA's Managed Tiered Security Profile (MTSP), as in **Figure 6.5.3-3**, will be addressed to meet an Agency's requirements based on security service levels identified in Section 6.8. An in-depth defense strategy and technical solution that includes AVMS will be engineered as described in 6.8.3.1.1 to account for specific differences in each tier.

MTSP Tier 2 - Protected Service shall provide security enhancements to the subscribing Agency with additional protection from unauthorized activities and the proliferation of malicious code. Protected service shall also

Figure 6.5.3-3. MTSP Notional Architecture



193-2241

mitigate the potential for Denial of Service attacks. Security enhancements include a combination of firewall, premises-based VPN (encrypted tunnels), filtering router, proxy server, and boundary anti-virus detection technologies configurable to the subscribing Agency's security policy(s) and specifications.

Tier 2 is tailored to Sensitive but Unclassified mission functions and information. It employs both technical and network management components appropriate to the respective mission and/or information sensitivity.

[Redacted content]