

6.1.4 ANTI-VIRUS MANAGEMENT SERVICES (AVMS) (L.34.1.6, M.2.1.3)

Agencies are able to leverage their existing infrastructure and add current technologies for anti-virus protection using the Qwest Team's AVMS. We provide protection from and removal of system viruses in a cost-effective and highly reliable manner before they can cause widespread damage.

Qwest has teamed [REDACTED] to provide Agencies with security services to fulfill the requirements of the RFP. Our AVMS provides detection and removal of system viruses before they can do critical damage to business operations. The Qwest Team is offering two types of AVMS for Agencies:

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

We use [REDACTED]

[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.

The Qwest Team's AVMS is part of an integrated approach to security services. Our AVMS extends well beyond those of a standard bulk customer Managed Security Service Provider (MSSP). Our 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]

6.1.4.1 Technical Approach to AVMS Delivery (L.34.1.6.1, M.2.1.3 (b))

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

[Redacted text block]

[Redacted text block]

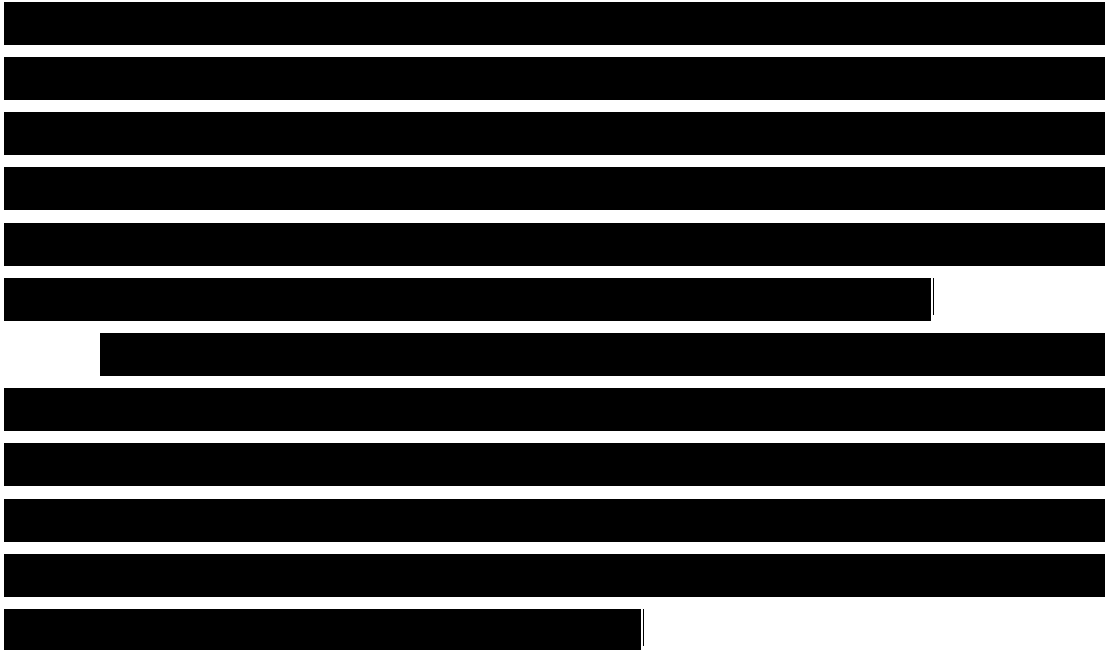
[Large redacted text block]

[REDACTED]

6.1.4.1.1 Technical Approach to AVMS Delivery (L.34.1.6.1 (a))

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

[REDACTED]



The Qwest Team's AVMS complies with the connectivity requirements in the RFP, including interoperability with Agency networking environments, such as Demilitarized Zones, secure Local Area Networks, extranets, and public networks (i.e., Internet).

6.1.4.1.2 Benefits of AVMS Technical Approach (L.34.1.6.1 (b))

The Qwest Team's approach to AVMS maintains an approved standard and avoids the obsolescence of legacy systems. We work with Agencies to export our successful products and services to them. We reduce redundancy where overlap limits the value of IT investments. **Figure 6.1.4-2** shows some of our discriminators and benefits.

Figure 6.1.4-2 Discriminators Set Qwest Team AVMS Apart

| Feature | [REDACTED] | [REDACTED] |
|---|------------|------------|
| Analysis of the Current Environment | [REDACTED] | [REDACTED] |
| Documentation of the Computing Environment | [REDACTED] | [REDACTED] |
| Fully Tested Pilot Implementation with supporting Standard Operating Procedure (SOP) documentation. | [REDACTED] | [REDACTED] |

The Qwest Team’s technical approach to AVMS is effective in providing Agencies with the means to address FISMA, which requires Agencies to institute information security programs with the ability to manage and annually re-assess risk. The Qwest Team AVMS supports the Federal Enterprise Architecture (FEA), as noted in **Figure 6.1.4-3**.

Figure 6.1.4-3. FEA Objectives. *Qwest Team AVMS supports FEA objectives for improved utilization of Government information resources, cost savings and avoidance, and increased collaboration.*

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

6.1.4.1.3 Solutions to AVMS 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. [REDACTED] we present several potential problems and our solution or mitigation approach.

Figure 6.1.4-4. Qwest Team Solutions to AVMS Problems

| | |
|------------|------------|
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |
| [REDACTED] | [REDACTED] |

6.1.4.2 Satisfaction of AVMS Performance Requirements (L.34.1.6.2, M.2.1.3 (c))

6.1.4.2.1 Quality of Service (L.34.1.6.2 (a))

Qwest Team AVMS meets all performance requirements, as summarized in **Figure 6.1.4-5**. 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 6.1.4-5. Qwest Team AVMS Meets All of GSA’s AQLs

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

Availability: Qwest Team AVMS is delivered through industry-leading security appliances and software that are engineered for near 100 percent availability. [REDACTED]

[REDACTED]

[REDACTED]

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

[REDACTED]

Time to Restore (TTR). [REDACTED]

[REDACTED]

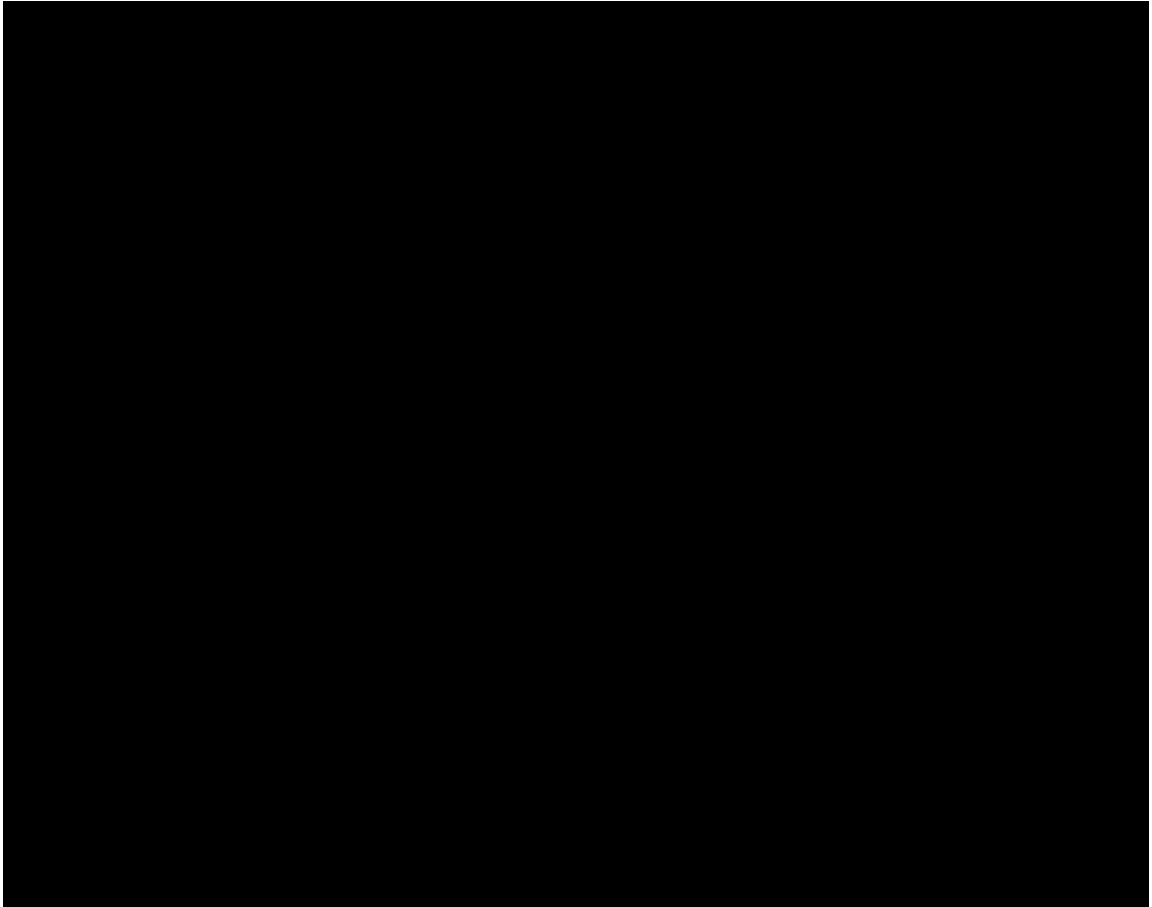
[REDACTED] All troubles recorded as Normal or Urgent (Emergency) in [REDACTED] are routed to the SOC for immediate attention. On a 24x7x365 basis, the Qwest Team will detect, prioritize, isolate, diagnose, and repair faults affecting contract services and restore them to meet the Agency's specifications.

**6.1.4.2.2 Approach for Monitoring and Measuring KPIs and AQLs
(L.34.1.6.2 (b))**

[REDACTED]

[Redacted text block]

[Redacted text block]



6.1.4.2.3 Verification of Services (L.34.1.6.2 (c))



6.1.4.2.4 Proposed Performance Improvements (L.34.1.6.2 (d))

[Redacted content]

6.1.4.2.5 Additional Performance Metrics (L.34.1.6.2 (e))

[Redacted content]

6.1.4.3 Satisfaction of AVMS Specifications (L.34.1.6.3, M.2.1.3 (d))

Our AVMS offering meets the required specifications for capabilities, features, standards, connectivity, and interfaces.

6.1.4.3.1 Satisfaction of Anti-virus Management Services Requirements (L.34.1.6.3 (a))

This section addresses the AVMS Technical Capabilities, Features, and Interface requirements.

6.1.4.3.1.1 Satisfaction of Anti-virus Management Services Capability Requirements (L.34.1.6.3 (a), C.2.10.4.1.4)

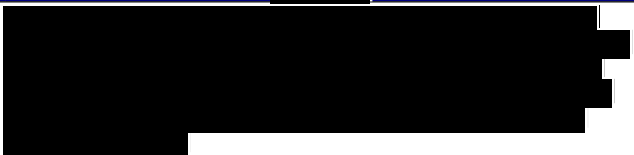

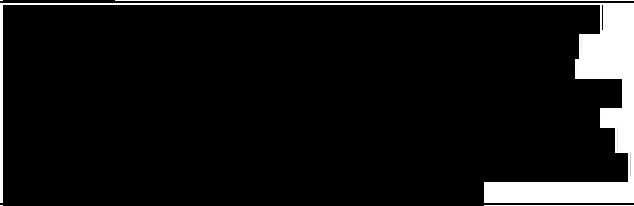
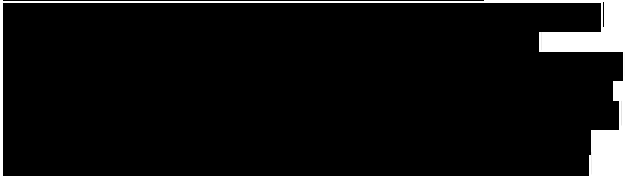




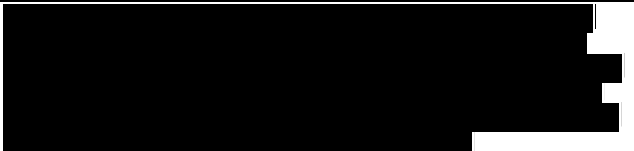
The Qwest Team AVMS offering meets the capabilities required in the RFP as enumerated in **Figure 6.1.4-8**. The Qwest Team fully complies with all mandatory stipulated and narrative capabilities requirements for AVMS. The text in Figure 6.1.4-8 provides the technical description required per

L.34.1.6.3(a) and does not limit or caveat the Qwest Team's compliance in any way.

Figure 6.1.4-8 The Qwest Team complies with all of 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 that 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 24x7x365 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), HTTP Secure (HTTPS), Post Office Protocol, and Simple Mail Transfer Protocol (SMTP) traffic for possible infection. | [REDACTED] |
| 7. The service shall perform data integrity checks and, at a minimum, protect against the following: | [REDACTED] |
| a. Known viruses | [REDACTED] |

| AVMS Capabilities | |
|--|------------|
| 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, 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] |
| c. Control of user access and environment for the malicious file | [REDACTED] |

| AVMS Capabilities | |
|---|--|
| <p>9. The contractor shall maintain the AV system and perform the necessary hardware/software upgrades, updates, and replacements.</p> |  |
| <p>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.</p> |  |
| <p>11. The contractor shall provide automatic and timely updates of the virus pattern and signature files as they become available to ensure adequate protection.</p> |  |
| <p>12. The contractor shall perform periodic gateway scans capable of revealing any vulnerabilities of the AV system.</p> |  |
| <p>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.</p> |  |
| <p>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:</p> |  |
| <p>a. Infections detected</p> |  |
| <p>b. Malicious emails</p> |  |
| <p>c. Rule violations</p> |  |

| AVMS Capabilities | [Redacted] |
|--|------------|
| d. Traffic/mail statistics | [Redacted] |
| 15. The contractor shall support networks of varying complexity in terms of size, bandwidth, and speeds. | [Redacted] |

6.1.4.3.1.2 Satisfaction of Anti-virus Management Services Feature Requirements (L.34.1.6.3 (a), C.2.10.4.2)

The Qwest Team AVMS offering provides a [Redacted] solution to meet the required features as enumerated in **Figure 6.1.4-9**. The Qwest Team fully complies with all mandatory stipulated and narrative feature requirements for AVMS. The text in Figure 6.1.4-9 provides the technical description required per L.34.1.6.3(a) and does not limit or caveat the Qwest Team’s compliance in any way.

Figure 6.1.4-9. How The Qwest Team Meets Load Balancing Requirements

| Name of Feature | Description | [Redacted] |
|---------------------------|--|------------|
| Anti-virus 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. | [Redacted] |

6.1.4.3.1.3 Satisfaction of Anti-virus 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), PBIP-VPNS (RFP Section C.2.7.2) and NBIP-VPNS (RFP Section C.2.7.3).

6.1.4.3.2 Proposed Service Enhancements (L.34.1.6.3 (b))

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

6.1.4.3.3 Network Modifications (L.34.1.6.3 (c))

[REDACTED]

6.1.4.3.4 The Qwest Team Experience Delivering AVMS (Including Subs) (L.34.1.6.3 (d))

The Qwest Team 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 text block containing multiple paragraphs of blacked-out content]

[REDACTED]

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

AVMS is part of the Qwest Team MTSS technical solution. Design, implementation, and delivery according to General Services Administration's Managed Tiered Security Profile (MTSP), as shown in **Figure 6.1.4-10**, will be addressed to meet an Agency's requirements based on security service levels identified in Section 6.1. An in-depth defense strategy and technical solution that includes AVMS will be engineered as described in Section 6.1.1 to account for specific differences in each tier.

[REDACTED]

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

[Redacted content]