6.7 SECURE MANAGED EMAIL SERVICE (SMEMS) (L.34.1.6)

Qwest SMEMS provides Agencies with a comprehensive service to filter spam and viruses from Email before it enters the Agency infrastructure at industry-leading protection rates along with the ability to utilize simple-to-implement, centralized services and ensure inbound and outbound Email complies with Agency policy.

Qwest's SMEMS is an effective and reliable Email service that meets the requirements of GSA and the Agencies. Qwest's SMEMS provides Agencies with the ability to centralize and ensure inbound and outbound Email policy compliance, ease of administration, ability to meet legal and regulatory requirements on Email retention, and security/privacy (via a patented pass-through process, not store-and-forward). Qwest's SMEMS also provides the ability to leverage the cost effectiveness of the Internet while providing the confidentiality, integrity and availability of Email services expected by the Federal Government.

Qwest has selected Postini Corporation's Perimeter Manager Enterprise Edition with a rules-based heuristics engine to provide SMEMS for Networx. Postini is a recognized leader in effectively stopping spam, phishing, viruses, directory harvest attacks, and other Email threats through its patented, multi-layer technology. As the incidence and severity of Email viruses has nearly tripled in the past year, Postini consistently demonstrates superior capabilities by eliminating spam and viruses, stopping Denial of Service (DOS), and delivery harvest attacks, guarding content, and improving Email performance and availability. [redacted]

This section describes the SMEMS features, functions, and capabilities, and shows how they meet Agency requirements for service delivery, performance, and service specifications. SMEMS is a valuable component of the Qwest Team's in-depth defense strategy of Managed Tiered Security Services (MTSS). An Agency may choose SMEMS alone or in combination with other services.

Qwest SMEMS features include:

- Powerful spam filtering
- Delivery management
- Multilayer anti-virus protection, coupled with patented technology that protects an Agency's Email system from initial outbreak of a virus until an anti-viral signature is available
- Disaster recovery service
- Event-based alerts
- Real-time monitoring and reporting
- Content filtering
- Attachment filtering

Emails containing viruses are quarantined and can be deleted or cleansed. Users receive immediate notification that an Email has been quarantined because of a virus and can also review virus infected Email in their own quarantine area, if they have been granted this privilege.

Directory Harvest Attack (DHA) prevention—a real-time inspection is made of every Internet Protocol (IP) address that connects to the SMEMS. Patented IP analysis determines if the behavior of the message exhibits the characteristics of a DHA and blocks the attack.

These features, which focus on the security, integrity, usability, and management of Agency Email systems and filter the Email stream before it enters an Agency's network environment, make the Qwest SMEMS an excellent choice for Agencies.

6.7.1 Technical Approach to Secure Managed Email Service Delivery (L.34.1.6.1)

[redacted]

All incoming and outgoing Email is routed through SMEMS and scanned by a sophisticated heuristic-rules engine that analyzes every part of an Email message, from the IP address of the sender to the message content, including language/lexicon and information presented in text,

[redacted]

[redacted]

HyperText Markup Language, graphics, and images. The SMEMS filtering process is executed in a highly secure, automated environment that prevents anyone from viewing valid Email without storing it to disk [redacted]

6.7.1.1 Approach to Secure Managed Email Service Delivery (L.34.1.6.1(a))

The Qwest SMEMS meets all service delivery requirements and can be deployed immediately. With Qwest's SMEMS, Agencies receive a highly scalable infrastructure for hosting value-added Email applications. SMEMS was developed to run on "carrier-class" hardware systems to process over one billion messages per day, while providing unparalleled user visibility into the filtering applied to each message passing through the system. Only minor integration is required by Agencies and messages are transferred using standard Simple Mail Transfer Protocol.

[redacted]

[redacted]

Qwest SMEMS fulfills all the mandatory SMEMS requirements in the Networx Request for Proposal (RFP).

SMEMS Complies with Required Standards including Federal Information Security Management Act, Federal Information Processing Standards (FIPS) PUB 140-2, FIPS PUB 199 and National Institute of Standards and Technology SP 800-45. [redacted] The system is available at any time from any place over the public Internet. [redacted]

[redacted]

[redacted] Users will have access for messaging management, real-time monitoring, and reporting. This system will immediately record and track reported events [redacted]

Qwest SMEMS provides required connectivity for the public Internet access. Qwest SMEMS connects and interoperates with Agency networking environments, and it supports connectivity to the Internet as required in the RFP.

6.7.1.2 Benefits of Secure Managed Email Service Technical Approach (L.34.1.6.1(b)

Qwest's SMEMS provides a multi-layer technology that prevents Email threats from reaching an Agency network. Qwest's SMEMS benefits are summarized in ***Figure 6.7.1-4***.

Figure 6.7.1-4. Qwest Discriminators and Benefits

Feature/	Benefit	[redacted]
Email Threat Prevention and Protection.	Qwest SMEMS stops spam, phishing, viruses, directory harvest attacks, and other Email threats with patented, multi-layer technology.	[redacted]
Flexible Policy Enforcement	The Agency will have granular control of Email policies across multiple Email domains.	[redacted]

Feature/	Benefit	[redacted]
Extensive Management Console for Message Administration	Management console provides real-time reporting and policy control of Email services from any location over the Internet.	[redacted]
High Availability and High Performance	Guaranteed Email scanning and delivery.	[redacted]

The Federal Enterprise Architecture (FEA) is an e-Government initiative intended to serve as "a business-based framework for Government-wide improvement." Qwest's SMEMS addresses the objectives of FEA as depicted in ***Figure 6.7.1-5***.

Figure 6.7.1-5. Qwest Addresses FEA Objectives

FEA Requirement	Discussion
Improve Utilization of Government Information Resources	The Qwest SMEMS removal of unwanted spam, bulk Email, viruses, and malicious code improves Agency efficiency and effectiveness Qwest's SMEMS will provide for monitoring and management of Agency Email and allow the Agency to use their limited resources in effective manner and not waste them on managing a secure Email infrastructure. This provides faster elimination of spam, malicious code or viruses in Email as well as a secondary location for Email storage in the event of an Agency Email server failure.
Enhance Cost Savings and Cost Avoidance	The Qwest Team recognizes the time, money, and resources required to reduce unsolicited commercial bulk Email and spam. Qwest's SMEMS service provides a huge reduction in costs and allows for content recognition within Email, protecting Agencies from misuse of networks serving the public.
Increase Cross-Agency and Inter-Government collaboration	Qwest's SMEMS enables Agencies to communicate effectively with Email without the threat and expense of Email spam and virus-prone messages.

6.7.1.3 Solutions to Secure Managed Email Service Problems (L.34.1.6.1(c))

The Qwest Team has learned from experience how to anticipate and solve problems that may arise over the service life as shown in ***Figure 6.7.1-6***.

Figure 6.7.1-6 Anticipated SMEMS Problems and Qwest Solutions

Problem	[redacted]
Encrypted File Scanning	[redacted]

6.7.2 Satisfaction of Secure Managed Email Service Performance Requirements (L.34.1.6.2)

6.7.2.1 Secure Managed Email Service Quality of Services (L.34.1.6.2(a))

Qwest's SMEMS offering is designed to enable sustainable results at an operational level through a performance measurement system based on key performance metrics that meet Acceptable Quality Levels (AQLs). Performance of quantifiable indicators is measured, collected, monitored, and reported to determine the success or failure of Qwest SMEMS on the GSA Key Performance Indicators (KPIs). [redacted]

Servers and systems that host Email applications in the SMEMS infrastructure are designed for redundancy and scalability on "carrier-class" hardware. [redacted]

[redacted]

Qwest's SMEMS offering fully complies with GSA requirements as shown in ***Figure 6.7.2-1***.

Figure 6.7.2-1. Qwest Meets GSA KPI/AQL Requirements

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	AQL	[redacted]
Availability	Routine	99.999%	≥ 99.999%	[redacted]
Time to Restore (TTR)	Without dispatch	4 hours	≤ 4 hours	[redacted]
	With dispatch	8 hours	≤ 8 hours	[redacted]

SMEMS Availability: Qwest's SMEMS is delivered through industry-leading technology and engineered for [redacted] availability. Our alert monitoring tools can isolate potential service disruptions prior to full network fault. Qwest SMEMS is a fault tolerant Email processing system. [redacted] Over the past three years, the SLA commitment has been [redacted] in delivering legitimate Email messages. The Qwest SMEMS management console provides real-time monitoring and alerting as well as comprehensive reporting for administrators. [redacted]

SMEMS TTR: Qwest SMEMS is designed to prevent a complete system failure. The dual redundant architecture ensures Email messages can be processes continuously without measurable latency. Qwest SMEMS complies with the Time To Restore service level of four (4) hours without dispatch and 8 hours with dispatch. The most obvious failure point would be the Agency's Internet connections. If there is a network disruption or malicious event on the Agency's Internet connections Qwest's SOC will triage the event in order to isolate failure and threats. [redacted]

6.7.2.2 Approach for Monitoring and Measuring Secure Managed Email Service (L.34.1.6.2(b))

The Qwest SMEMS service platform will be monitored for availability and performance using a mature open source tool [redacted] (as well as other tools) to perform [redacted] per minute. The [redacted] operations center will monitor the availability dashboard for UP status and receive automated alerts of the SMEMS platform being DOWN, or in a WARNING state, as well as upon recoveries from any non-OK state. Qwest NTM Remedy Trouble Ticket System will document the timing and response to TTR.

6.7.2.3 Verification of Secure Managed Email Service (L.34.1.6.2(c))

The SMEMS system continuously monitors and measures various system components. If there is an issue with a component, alerts are automatically sent to Qwest SMEMS operations personnel.

6.7.2.4 Secure Managed Email Service Performance Improvements (L.34.1.6.2(d))

[redacted]

6.7.2.5 Additional Secure Managed Email Service Performance Metrics

[redacted]

6.7.3 Satisfaction of Secure Managed Email Service Specifications (L.34.1.6.3)

Qwest fully complies with all mandatory stipulated and narrative capabilities, features, and interface requirements for SMEMS. The following Figure 6.7.3-1 summarizes Qwest's response to the SMEMS capabilities listed in RFP C.2.10.8.1.4, features of RFP C.2.10.8.2, and interfaces of RFP C.2.10.8.3. This subsection is intended to provide the technical description required per L.34.1.6.3(a), and not to limit or caveat Qwest's compliance in any way.

6.7.3.1 Satisfaction of Secure Managed Email Service Requirements (L.34.1.6.3(a))

The Qwest SMEMS is fully compliant with the mandatory technical capabilities shown in ***Figure 6.7.3-1***.

Figure 6.7.3-1. GSA SMEMS Mandatory Capabilities

SMEMS Capabilities	[redacted]
1. The contractor shall monitor Email in real-time, on a 24 hours a day, 7 days a week basis, for timely and accurate detection of harmful traffic and unwanted content.	[redacted]
2. The Email security system shall support the following functions:	[redacted]
a. Antivirus Scanning, which monitors all inbound and outbound messages and attachments for: i. Known Viruses and Unknown Viruses ii. Trojan Horses, Worms, Macro Viruses and Other Malicious Files iii. Behaviors and Characteristics that May Indicate the Presence of Email Viruses iv. Different Strains of Polymorphic Viruses v. Viruses Residing in Compressed Files as required by the Agency vi. Viruses in Different Languages (for example, JAVA, ActiveX, Visual Basic)	[redacted]

SMEMS Capabilities	[redacted]
b. Anti-Spam Filtering, which prevents unsolicited marketing and messages from entering the Agency's network, and taxing human, bandwidth and storage resources. The system shall support: i. Anti-spam methods including fingerprinting, blacklists, open relay blocking, honeypots, Bayesian probability, heuristic and rule-based filtering, as appropriate ii. Capability to distinguish between legitimate Email and spam, reducing false negatives and positives. iii. Agency ability to customize spam lists, and specify domains, IP and Email addresses which are to be allowed or blocked.	[redacted]
c. Content Control, which screens inbound and outbound Email for content that may signal system abuse or violation of Agency communications policies. The systems shall support the following: i. Blocking of specific words, phrases, adult or sexually-explicit material, and other inappropriate content ii. Preventing transmission of intellectual property and confidential information iii. Stopping files and attachments based on type, size, formats, number, and delivery time	[redacted]

SMEMS Capabilities	[redacted]
3. The service shall respond to Email infections and Agency policy violations, providing the following at a minimum: a. Alerts notifying the systems/network administrator via Email, pager, fax, or telephone, as directed by the Agency's notification procedures. The sender and recipient shall also be notified, as applicable. b. Virus infected file isolation for cleaning, deletion, or post-alert analysis and interpretation. The system shall also store or forward spam and policy-violating content to an alternate Email address for Agency review in order to prevent the deletion of legitimate business Email, or handle such content according to Agency directives.	[redacted]
4. The contractor shall support a secure Web-based management and reporting interface which provides the following: a. Configuration tools allowing the Agency to set policies, rules and routing options	[redacted]
b. Email activity trends, such as daily, weekly, monthly, and yearly volumes and patterns	[redacted]
c. Email cleaned, deleted, or rejected	[redacted]
d. Forwarding of weekly reports to designated Agency representative	[redacted]
e. Management of user and domain permissions	[redacted]

SMEMS Capabilities	[redacted]
f. Potential threats flagged	[redacted]
g. Real-time service statistics and availability data	[redacted]
h. User and company domain activity	[redacted]
i. Viruses, spam, and other inappropriate content blocked on a daily, weekly, monthly, or yearly basis	[redacted]
5. The contractor shall queue and retain Email in the event of an Agency mail server or connection failure, in order to prevent messages from bouncing. The contractor shall gradually transmit queued Email upon resolution of the problem to avoid overloading the servers.	[redacted]
6. The contractor shall implement security procedures to preserve the confidentiality and integrity of all Agency Email traversing its network and data center. These include, but are not limited to, authentication, encryption, and access restriction.	[redacted]
7. The contractor shall support Email requirements of varying complexity, in terms of load and volume.	[redacted]

Qwest's SMEMS supports the User-to-Network Interfaces defined in Section C.2.4.1, Internet Protocol Service.

6.7.3.2 Proposed Enhancements for Secure Managed Email Service (L.34.1.6.3(b)

[redacted]

6.7.3.3 Network Modifications Required for Secure Managed Email Service Delivery (L.34.1.6.3(c))

[redacted]

6.7.3.4 Experience with Secure Managed Email Service (L.34.1.6.3(d))

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

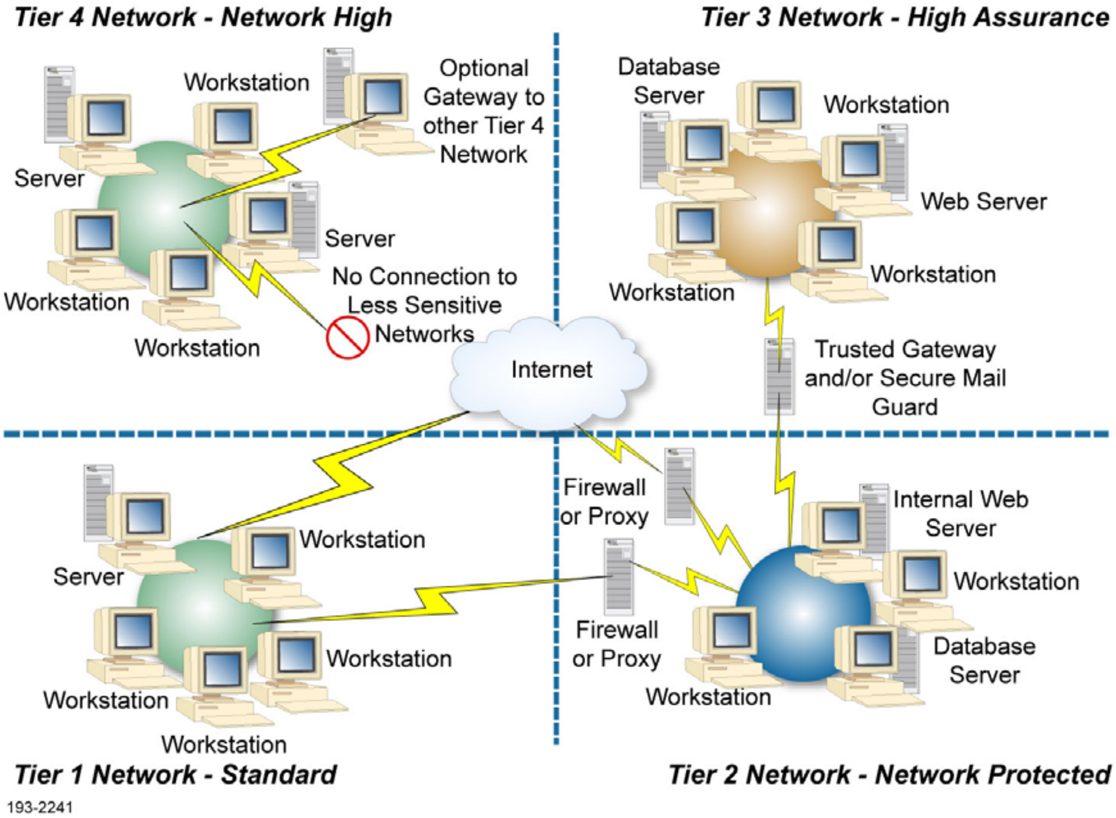
[redacted]

[redacted]

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

SMEMS is part of Qwest MTSS technical solution. Design, implementation and delivery according to GSA's MTSP, ***Figure 6.7.3-2***, will be addressed to meet an Agency’s requirements based on security service

Figure 6.7.3-2. MTSP Notional Architecture



levels identified as described in Section 6.8 [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 DOS attacks. Security enhancements include a combination of firewall, premises-based virtual private network (encrypted tunnels), filtering router, proxy server, and boundary anti-virus detection technologies configurable to the subscribing Agency's security policy(s) and specifications.

[redacted]

[redacted]

[redacted]