

6.2.4 Secured Managed Email Service (SMEMS) (L.34.1.6.4, M.2.1.3)

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

Qwest has teamed [REDACTED] to provide Agencies with security services to fulfill the requirements of the RFP. The Qwest Team's SMEMS is an effective and reliable email service that meets the requirements of the Network RFP. Our SMEMS provides Agencies with the ability to centralize and ensure inbound/outbound email policy compliance, ease of administration, the ability to meet legal and regulatory requirements on email retention, and security/privacy (via a patented pass-through process, not store-and-forward). Our 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 Government.

Qwest [REDACTED]

[REDACTED] 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, [REDACTED] consistently demonstrates superior capabilities by eliminating spam and viruses, stopping Denial of Service 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 our defense-in-depth strategy of Managed Tiered Security Services. An Agency may choose SMEMS alone or in combination with other services.

Our 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 antiviral 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 the 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, filter the email stream before it enters

an Agency's network environment, therefore making our SMEMS an excellent choice for Agencies.

6.2.4.1 Reserved (L.34.1.6.4 (a))

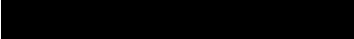
6.2.4.2 Reserved (L.34.1.6.4 (b))

6.2.4.3 Technical Service Requirements (L.34.1.6.4 (c))

[Redacted content]

[Redacted content]

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

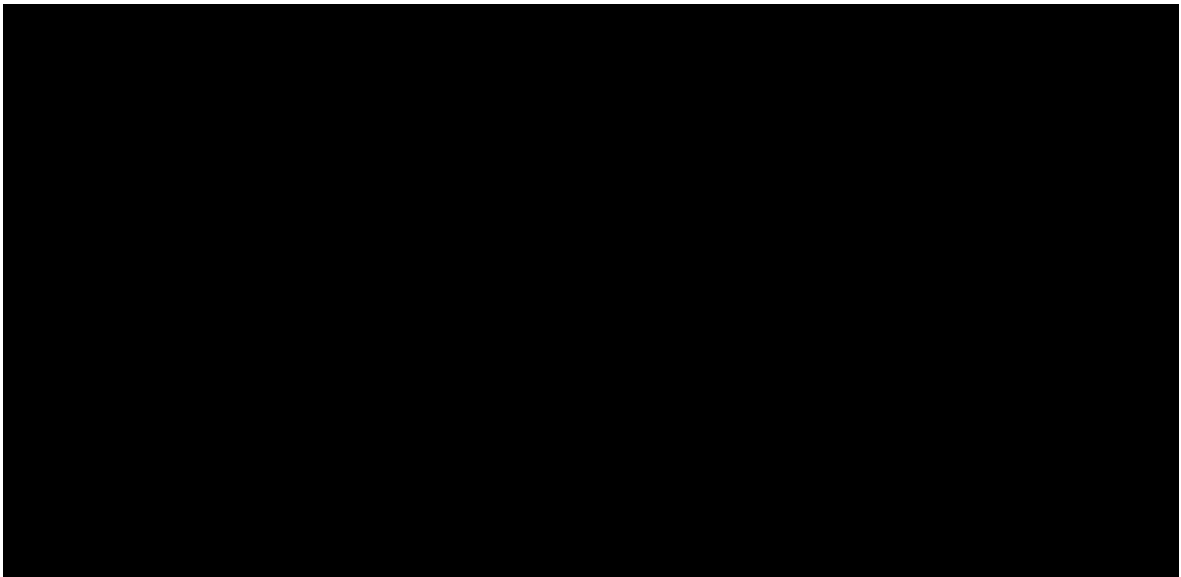
content, including language/lexicon and information presented in text, HyperText Markup Language, graphics, and images. The SMEMS filtering process is executed in a highly secure, automated environment that prevents viewing valid email without first storing it to disk. 







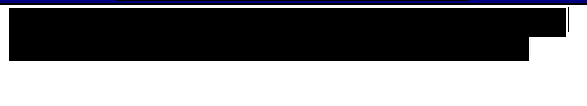



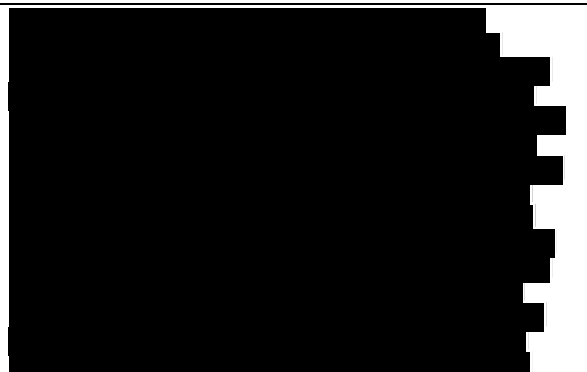




6.2.4.3.1 Satisfaction of SMEMS Capability Requirements (L.34.1.6.4 (c), C.2.10.8.1.4)

The Qwest Team's SMEMS is fully compliant with the mandatory technical capabilities shown in **Figure 6.2.4-3**. Qwest fully complies with all mandatory stipulated and narrative capability requirements for SMEMS. The text in Figure 6.2.4-3 provides the technical description required per L.34.1.6.4 (c) and does not limit or caveat Qwest's compliance in any way.

Figure 6.2.4-3. GSA SMEMS Mandatory Capabilities

SMEMS Capabilities	
<p>1. The contractor shall monitor email in real-time, 24x7x365, for timely and accurate detection of harmful traffic and unwanted content.</p>	
<p>2. The email security system shall support the following functions:</p>	
<p>a. Antivirus Scanning, which monitors all inbound and outbound messages and attachments for:</p> <ul style="list-style-type: none"> 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) 	
<p>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:</p> <ul style="list-style-type: none"> 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 that are to be allowed or blocked. 	
<p>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:</p> <ul style="list-style-type: none"> 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 	

SME MS Capabilities	
<p>3. The service shall respond to email infections and Agency policy violations, providing the following at a minimum:</p> <ul style="list-style-type: none"> 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. 	
<p>4. The contractor shall support a secure Web-based management and reporting interface that provides the following:</p> <ul style="list-style-type: none"> a. Configuration tools allowing the Agency to set policies, rules, and routing options 	
<ul style="list-style-type: none"> b. Email activity trends, such as daily, weekly, monthly, and yearly volumes and patterns 	
<ul style="list-style-type: none"> c. Email cleaned, deleted, or rejected 	
<ul style="list-style-type: none"> d. Forwarding of weekly reports to designated Agency representative 	
<ul style="list-style-type: none"> e. Management of user and domain permissions 	
<ul style="list-style-type: none"> f. Potential threats flagged 	
<ul style="list-style-type: none"> g. Real-time service statistics and availability data 	
<ul style="list-style-type: none"> h. User and company domain activity 	
<ul style="list-style-type: none"> i. Viruses, spam, and other inappropriate content blocked on a daily, weekly, monthly, or yearly basis 	

SMEMS Capabilities	
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]

6.2.4.3.2 Satisfaction of SMEMS Feature Requirements (L.34.1.6.4 (c), C.2.10.8.2)

There are no Feature requirements under RFP Section C.2.10.8.2.

6.2.4.3.3 Satisfaction of SMEMS Interface Requirements (L.34.1.6.4 (c), C.2.10.8.3)

The Qwest Team’s SMEMS supports the User-to-Network Interfaces defined in Section C.2.4.1, *Internet Protocol Service*. Qwest fully complies with all mandatory stipulated and narrative interface requirements for SMEMS. The text in Section C.2.4.1 provides the technical description required per L.34.1.6.4 (c) and does not limit or caveat Qwest’s compliance in any way.

6.2.4.4 Achieving Quality of Service Goals (L.34.1.6.4 (d))

The Qwest Team’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 Key Performance Indicators (KPIs). [REDACTED]

[REDACTED]

Servers and systems that host email applications in the SMEEMS infrastructure are designed for redundancy and scalability on carrier-class hardware. [REDACTED]

[REDACTED]

The Qwest Team’s SMEEMS fully complies with GSA requirements, as shown in **Figure 6.2.4-4**.

Figure 6.2.4-4. Qwest Meets GSA KPI/AQL Requirements

Key Performance Indicator (KPI)	Service Level	Performance Standard (Threshold)	Acceptable Quality Level (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]

SMEEMS Availability: The Qwest Team’s SMEEMS is delivered through industry-leading technology and engineered for [REDACTED] percent availability. Our alert monitoring tools can isolate potential service disruptions prior to full

network fault. The Qwest Team's SMEMS is a fault tolerant email processing system. [REDACTED]. Over the past three years, the Service Level Agreement (SLA) commitment has been [REDACTED] in delivering legitimate email messages. Our SMEMS management console provides real-time monitoring and alerting as well as comprehensive reporting for administrators. Real-time SMEMS statistics are available via this Web console.

SMEMS TTR: The Qwest Team's SMEMS is designed to prevent a complete system failure. The dual redundant architecture ensures that email messages can be processed continuously without measurable latency. The Qwest Team's SMEMS complies with the TTR service level of four hours without dispatch and eight hours with dispatch. The most obvious failure point would be the Agency's individual Internet connections. If there is a network disruption or malicious event on the Agency's Internet connections, the Qwest Team's Secure Operations Center (SOC) will triage the event in order to isolate the failure and threats. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]

6.2.4.5 Proposed Service Enhancements (L.34.1.6.4 (e))

[REDACTED] When an Agency has a specific business need or application problem, Qwest will collaboratively discuss service enhancements. Qwest will operate in good faith to engineer a SMEMS solution to serve unique Agency needs. Qwest is able to leverage our product portfolio that includes a variety of SED hardware and software providers and specific SMEMS solutions. Through a special

combination of vendor solutions and engineering capabilities, we will serve Agencies' unique business needs.

6.2.4.6 Qwest Team Experience (L.34.1.6.4 (f))

[Redacted content]

[REDACTED]

6.2.4.7 Approach to Performance Verification (L.34.1.6.4 (g))

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

All incident response reports are tracked [REDACTED]
[REDACTED] Reports are processed by analysts according to an established work

flow, and response times are tracked for each report and event. Data to support the measurement of the Government-specified KPIs are collected on a continuous basis; computed statistics are made available to authorized Agency personnel [REDACTED]. The raw data is collected through the SMEEMS system, network, and availability monitoring tools as well as through our customer change/problem tracking system.

6.2.4.8 Service Impact to Network Architecture (L.34.1.6.4 (h))

Qwest anticipates no impact to our network architecture due to delivery of SMEEMS.

6.4.2.9 Approach to Satisfying NS/EP Requirements (L.34.1.6.4 (i))

The Qwest Team supports the telecommunications requirements for national security and emergency preparedness (NS/EP) that are based on a set of telecommunications policies and procedures established by the National Communications System (NCS) in accordance with Executive Order 12472, developed to ensure that critical Government and industry needs are met when an actual or potential emergency threatens the security or the economic capabilities of the United States.

Specifically, the Qwest Team supports the following 14 basic functional requirements for NS/EP telecommunications and IT services. These are identified by the NCS and the Office of Science and Technology Policy for NS/EP telecommunications services as follows:

1. Enhanced Priority Treatment (C.5.2.1(1)) – The SMEEMS infrastructure that will support the Agency user community will be configured to enable dedication of one or more individual blade servers to support the needs of those identified priority users. These blades will not accept traffic on behalf of other users, and the priority user list can be configured to be event/incident specific. Thus it would be possible to build preconfigured scripts to rapidly implement one or more of pre-definable configurations.

2. Secure Networks (C.5.2.1(2)) – The service enabling portals and infrastructure all require use of appropriate authentication and are partitioned to limit access and perform tasks appropriate to the role of each authorized individual. Physical safeguards at data centers meet or exceed general acceptable industry practices for physical security, access control, and surveillance.

3. Non-Traceability (C.5.2.1(3)) – SMEMS can support controlled Number Address Translation and IP masquerading if implemented in a coordinated manner.

4. Restorability (C.5.2.1(4)) – The SMEMS infrastructure is distributed into multiple geographically diverse venues, each of which can support the provision of services. Service profiles are automatically distributed to support implementation of Border Gateway Protocol (BGP)-driven routing to failover sites.

5. International Connectivity (C.5.2.1(5)) – SMEMS infrastructure is peered with the Internet, thereby providing access to and from international destinations and carriers.

6. Interoperability (C.5.2.1(6)) – the SMEMS infrastructure processes message traffic presented in internationally accepted standard formats. Because this infrastructure provides commercial service internationally, it is designed to extend to support modification to existing, or introduction of new formats. Access to the provisioning and management portal is through standard Secure Sockets Layer (SSL) Web browser sessions, thereby not requiring maintenance of custom APIs.

7. Mobility (C.5.2.1(7)) – According to RFP Section C.5.2.2.1, this requirement is not applicable to SMEMS.

8. Nationwide Coverage (C.5.2.1(8)) – SMEMS infrastructure is peered with the Internet, thereby providing access to/from Government users wherever located, as long as they have Internet access.

9. Survivability/Endurability (C.5.2.1(9)) – The SMEMS infrastructure is distributed over multiple geographically diverse venues, each of which can support the provisioning of services. Service profiles are automatically distributed to support implementation of BGP-driven routing to failover sites. The venues are provided with utility related services designed to sustain independent operations despite localized failures. Transport facilities connecting the SMEMS infrastructure to the Internet are high-capacity and diversely routed.

10. Voice Band Service (C.5.2.1(10)) – According to RFP Section C.5.2.2.1, this requirement is not applicable to SMEMS.

11. Broadband Service (C.5.2.1(11)) – According to RFP Section C.5.2.2.1, this requirement is not applicable to SMEMS.

12. Scaleable Bandwidth (C.5.2.1(12)) – According to RFP Section C.5.2.2.1, this requirement is not applicable to SMEMS.

13. Affordability (C.5.2.1 (13)) – SMEMS is provided using commodity hardware infrastructure servers and a mixture of commercial-off-the-shelf and custom software at the data center. The client (end user) requires no specialized hardware or software to make use of the service. It is a highly affordable, commercially available service.

14. Reliability/Availability (C.5.2.1(14)) – 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. Qwest's teammate, Postini, has never lost an email. Over the past three years, the SLA commitment has been [REDACTED] uptime with no

measurable latency in delivering legitimate email messages. The Qwest SMEMS management console provides real-time monitoring and alerting as well as comprehensive porting for administrators.

**6.2.4.10 Approach to Assured Service in the National Capital Region
(L.34.1.6.4 (j))**

Qwest is currently a leading provider of network services in the National Capital Region (NCR) with robust network architecture to ensure service continuity in the event of significant facility failures. Qwest has and will continue to engineer critical services to meet the requirements of each customer to eliminate single points of failure for their network services.

Qwest understands the Government's requirement to assure performance of network services in and around the NCR. To meet this important requirement, Qwest has established Point-of-Presence (POP) diversity in the NCR. [REDACTED]

[REDACTED] Each of these gateways provides complete redundancy to access Qwest nationwide and international network capabilities as well as regional voice and data services. [REDACTED]

[REDACTED]

Qwest recently acquired OnFiber, a metro SONET and Ethernet provider with yet another diverse network in the NCR. This gives Qwest [REDACTED] [REDACTED] regional fiber optic networks to use to ensure redundancy and survivability in the greater Washington D.C. area. Section 3.5.2 provides further detail on our NCR infrastructure.

The Qwest Team has multiple SOCs and hosting centers that are geographically diverse, and no Managed Security Service is dependent on assets located solely within the NCR region.

6.2.4.11 Approach to Meeting Section 508 Provisions (L.34.1.6.4 (k))

The Qwest approach to Section 508 provisions is to ensure that all Agency users are able to access all systems and services. To ensure this, the Qwest Control Network Portal will be 508 compliant. The Qwest Control Network Portal is the gateway to Qwest Network support systems. The support systems for SMEMS are compliant with applicable accessibility standards in Subpart B. This Portal will serve as the primary conduit for daily status pertaining to ongoing projects and other service delivery activities for Agencies.

In addition, Qwest has enlisted a single toll-free number for 24x7x365 access: 1-866-GSA-NETWorx (1-866-472-6389). This toll-free number will allow domestic Agency users to have access to our Customer Support Office, which will also be 508 compliant, enabling access by email, fax, telecommunications display device, text messaging, or other methods as required. Qwest customer service support will be accessible around the clock for all Agency users, wherever they may be located.

The Qwest approach for ensuring that our products and services are 508 compliant is to go through the same rigorous testing and evaluation that all products and services go through before they are made available to the public. Qwest works with industry and specific assistive technology vendors to ensure that all of the Qwest products and services are 508 compliant. Section 3.5.3 provides further information regarding our compliance with Section 508 provisions.

6.2.4.12 Approach to Incorporating Technological Enhancements and Improvements (L.34.1.6.4 (l))

Qwest has a proven mature process that enables us to envision, research, evaluate, engineer, deploy, and operate new or emerging services including SMEMS. Driven initially by the Chief Technology Office, Qwest

evaluates new products and technologies for incorporation into the Qwest network, in partnership with Qwest Product Management.

[Redacted text block]

[Redacted text block]

[Redacted text block]

[REDACTED]

Qwest's vision for convergence will drive future capabilities developed for our customers. Partnerships will become more pervasive and will be required to complete the converged value chain. Qwest's business processes, people, and technical infrastructure are capable of extending the value chain to flexibly handle a wide array of teaming arrangements in delivering a seamless Agency experience. Qwest aligns service, network and systems projects, and initiatives, all with an eye toward delivery of converged capabilities. We develop and manage the road map that results in the successful delivery of fully integrated capabilities and infrastructure.