

1.6.8 Secure Managed Email Service (SMEEMS) [C.2.10.8]

Agencies will safeguard and protect their infrastructure and critical data by deploying the AT&T secure managed email service (SMEEMS) that incorporates spam filtering, virus blocking, content management, email policy enforcement, message archiving, and disaster recovery for both inbound and outbound messages, [REDACTED]

[REDACTED] AT&T's SMEEMS validates the integrity of email before it passes through the Agencies' network gateways, providing a front-line of defense that provides a safe bridge between the Internet and the Agency enterprise network.

Now, more than ever before, email is a mission-critical application. Agencies use email to communicate with co-workers, outside agencies, partners, and constituents and expect the communications to be treated with an even higher sense of urgency and importance than telephone calls or even overnight delivery services. Virtually every type of information – confidential or not – is now sent electronically in emails, including agency records, agency data, and other sensitive information.

Email carries a wide array of security risks that can compromise the agency infrastructure, the very fabric of the agency, with potentially catastrophic consequences. Damaged or lost data, interruption in network operations, loss of Internet connectivity can disrupt an agency and reduce employee productivity.



One of the primary issues regarding the security of email, or lack thereof, cuts to the core of the application's ubiquity: in order to receive email, an Agency must allow anyone, anywhere in the world, to connect to its email servers. Such an open door policy unavoidably invites the bad along with the good. Email servers are critical servers, and must be protected behind the enterprise firewall, because if they are taken down, Agency communications could come to a halt. With email servers resident behind firewalls, not only are email servers vulnerable to attack, the network on which they reside, is more at risk. The problem is rooted in the necessity for Agency email servers to accept all inbound (Simple Mail Transfer Protocol) SMTP connections. With this opening, the firewall cannot completely protect the network, a dilemma for network security administrators that is addressed by AT&T SMEMS.

[REDACTED]





[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

[REDACTED]

The service offers the latest anti-virus and anti-spam technology at a low total cost of ownership and provides business continuity. SMEMS has provided a safe computing environment for our customers as well as for AT&T.

As part of AT&T's overall security strategy, SMEMS has a multilayered security environment focusing on methods and systems to enhance security and respond to and mitigate incidents. [REDACTED]

[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]
[REDACTED]



[REDACTED]

[REDACTED]

1.6.8.c Technical Description [L34.1.6.4.c]

The offeror shall describe all optional Security Services offered to include:
(c) A technical description of how the service requirements (e.g., capabilities, features, interfaces) are satisfied for all proposed optional services. [L34.1.6.4.c]

AT&T provides a complete, comprehensive, and robust security solution to Agencies for their SMEMS needs. [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]



[Redacted text block]

[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]
[Redacted]	[Redacted]	[Redacted]



[REDACTED]

[REDACTED]



[Redacted text block]

[Redacted text block]



[Redacted text block]

[Redacted text block]



[REDACTED]

1.6.8.d Service Quality and Performance Metrics
[L34.1.6.4.d]

The offeror shall describe all optional Security Services offered to include:
(d) A description of the quality of the services with respect to the performance metrics specified in Section C.2 Technical Requirements for each proposed optional service, and other performance metrics used by the offeror. [L34.1.6.4.d]

AT&T SMEMS provides [REDACTED]

KEY PERFORMANCE INDICATOR (KPI)	SERVICE LEVEL	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
SMEMS Availability	Routine	99.999%	[REDACTED]
Time to Restore (TTR)	Without dispatch	4 hr	[REDACTED]
	With dispatch	8 hr	[REDACTED]

[REDACTED] **SMEMS Performance Metrics.** Agencies gain access to a high quality SMEMS designed to meet all required KPIs and AQLs.

Focusing on an Agency’s service experience produces a high-quality solution; service experience must be measured quantitatively through the KPIs. These AQLs represent the minimum level of service quality that AT&T intends to consistently deliver for SMEMS.

[REDACTED]

[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]
[REDACTED]	[REDACTED]

Agencies will receive the most accurate assessment of the service when the KPI measurement and monitoring methodology replicates the real performance that Agency personnel experience. AT&T's approach to monitoring and measuring KPI is complete and helps validate service delivery.

Achieving the AQLs, defined by the Government for the KPIs, will result in superior SMEMS performance. [REDACTED]

[REDACTED]

1.6.8.e Attributes and Value of Service Enhancements **[L34.1.6.4.e]**

The offeror shall describe all optional Security Services offered to include:
(e) If the offeror proposes to exceed the specified service requirements (e.g., capabilities, features, interfaces), a description of the attributes and value of the proposed service enhancements. [L34.1.6.4.e]

[REDACTED]

1.6.8.f Offeror's Experience [L34.1.6.4.f]

The offeror shall describe all optional Security Services offered to include:
(f) A description of the offeror's experience (including major subcontractors) with delivering each proposed optional service. [L34.1.6.4.f]



[REDACTED]

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

[REDACTED]

1.6.8.g Approach to Perform Service Verification [L34.1.6.4.g]

The offeror shall describe all optional Security Services offered to include:
(g) A description of the offeror's approach to perform verification of individual services delivered under the contract, in particular the testing procedures to verify acceptable performance and Key Performance Indicator (KPI)/Acceptable Quality Level (AQL) compliance. [L34.1.6.4.g]

The first time the service is provided through the Networkx contract, the service performance must be verified; KPIs will be monitored to certify that the service performance complies with the AQLs. AT&T has well-defined variables and approaches to measuring those variables that validate service delivery.

These variables and measuring techniques align with the KPIs for SMEMS.

[REDACTED]

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

[REDACTED]

To simplify the verification process, [REDACTED]

The service verification process is [REDACTED]

Through a comprehensive verification process, Agencies and the GSA will receive concrete data that demonstrates the readiness of the SMEMS. [REDACTED]

1.6.8.h Optional Services Impact on Network Architecture **[L34.1.6.4.h]**

The offeror shall describe all optional Security Services offered to include:
(h) A description of how the delivery of any optional services would impact the network architecture (e.g., security, quality and reliability, performance). [L34.1.6.4.h]

[REDACTED]

1.6.8.i Approach to Satisfy NS/EP Requirements **[L34.1.6.4.i]**

The offeror shall describe all optional Security Services offered to include:
(i) A description of the offeror's approach to satisfy each NS/EP basic functional requirement listed in Section C.5.2.2.1.1. [L34.1.6.4.i]



AT&T's approach to satisfy National Security/Emergency Preparedness (NS/EP) is [REDACTED]

1.6.8.j National Capital Region Assured Service Network Architecture [L34.1.6.4.j]

The offeror shall describe all optional Security Services offered to include:
(j) A description of how the network architecture will satisfy the requirements in Section C.5.2.7 for assured service in the National Capital Region, if applicable. [L34.1.6.4.j]

AT&T's approach to satisfy a service in the National Capital Region is [REDACTED]

1.6.8.k Section 508 Approach [L34.1.6.4.k]

The offeror shall describe all optional Security Services offered to include:
(k) A description of the offeror's approach for providing the capabilities needed to meet Section 508 provisions identified in Section C.6.4 for the proposed optional services. [L34.1.6.4.k]

AT&T's approach to meet Section 508 provisions is [REDACTED]

1.6.8.l Approach for Incorporating Optional Services, Enhancements, and Improvements [L34.1.6.4.l]

The offeror shall describe all optional Security Services offered to include:
(l) A description of the approach for incorporating into the proposed optional services, technological enhancements and improvements that the offeror believes are likely to become commercially available in the timeframe covered by this acquisition, including a discussion of potential problems and solutions. [L34.1.6.4.l]

[REDACTED]



[REDACTED]

1.6.8.m Stipulated Responses [L.34.1.2]

If the offeror proposes exceptions or deviations to any stipulated requirement, the rationale shall be stated in the Technical Volume and proposal references shall be provided in the cross reference table. [L.34.1.2]

[REDACTED]