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

Agencies will safeguard and protect their infrastructure and critical data by deploying a secure managed email service (SMEMS) that incorporates spam filtering, virus blocking, content management, email policy enforcement, message archiving, and disaster recovery for both inbound and outbound messages; all delivered through a global network of redundant data centers. SMEMS validates the integrity of email before it passes through the Agencies' network gateways, providing a front line of defense and a safe bridge between the Internet and the Agency's enterprise network.

"For implementing extremely flexible management offerings, being the first to bring application security services to the market, and offering the widest array of services in the industry, AT&T [Managed Security Services], is awarded the Customer Solutions Excellence Award."

--Frost & Sullivan
July 2003.

1.6.8.1 Technical Approach to Security Services Delivery [L.34.1.6.1]

1.6.8.1.a Approach to Service Delivery

(a) Analyze the service requirements specified in this solicitation and describe the approaches to service delivery for each service.

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.

> *AT&T presented Customers Solutions Excellence Award for Managed Security Services- for the second consecutive year. AT&T "reigns as the single most prolific MSSP in the market."*
>
> --Frost & Sullivan
> October 2004

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 service.

AT&T's SMEMS service provides Agencies with network-based email security and message management. The service helps validate the integrity of a message before it enters the agency network by providing a front-line defense that safely builds a bridge between the Internet and the Agency enterprise network. AT&T's SMEMS architecture is shown in **Figure 1.6.8.1-1** and the approach to delivery services is highlighted in **Table 1.6.8.1-1**.

AT&T SMEMS service is a 24x7, always-on, network-based service, and is operated by experienced, dedicated AT&T security analysts.

Figure 1.6.8.1-1 SMEMS Architecture. *Agencies benefit from a scalable, reliable SMEMS architecture which provides a more secure Internet email distribution service with built-in [redacted] protection.*

SERVICE DELIVERY APPROACH	TECHNICAL DESCRIPTION
Complete virus protection	• SMEMS provides thorough virus protection for all known viruses through its network-based approach and cloaks Agency email servers to prevent denial of service (DoS) attacks. • Service scans [redacted] of email messages [redacted] with complete known virus removal. • AT&T SMEMS virus updates are installed [redacted] to help eliminate the latest threats.
Fully managed service	Includes scanning of inbound/outbound emails, daily updates management to counter new viruses and spam, and delivering only clean email to the Agency and clean email from the Agency to other recipients. This is a complete end-to-end service with a single point-of-contact (POC) to address any service issues.
Scalable architecture	• Scalable solution, Agencies are not required to own or purchase any new equipment. • SMEMS uses multiple virus scan engines for exhaustive analysis, detection, and removal of email viruses.
Web-based reporting	Provides Agency access to performance reports and statistics located on the web.

Table 1.6.8.1-1: SMEMS Service Delivery Approach. *SMEMS will provide Agencies with all phases of safe email delivery, from gateway scanning and anti-virus/spam protection to web-based management.*

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. The multilayered security approach is further extended by transferring our own proven security innovations to the Agency. This offer is part of a one-stop shop solution for all Agency cyber security requirements.

Gartner

Gartner Rates AT&T Highest in 'Ability to Execute' as a Managed Security Service Provider, February, 2003

--as per Gartner's North American MSSP (Managed Security Service Provider)

1.6.8.1.b Benefits to Technical Approach

(b) Describe the expected benefits of the offeror's technical approach, to include how the services offered will facilitate Federal Enterprise Architecture objectives (see http://www.whitehouse.gov/omb/egov/a-1-fea.html).

AT&T's Networx services, in general, and SMEMS services, in particular, support the Government's vision of transformation through the use of the Federal Enterprise Architecture (FEA) by providing the technologies that

contribute to the Agency's mission objectives. **Table 1.6.8.1-2** describes each service in relation to FEA, summarizes its contribution, and/or provides an example of how it facilitates FEA implementation.

SERVICE DELIVERY APPROACH	BENEFIT	FEA FACILITATION
Complete virus protection	Agencies benefit from a high-quality service that detects and removes known viruses before they enter the Agency's network, and delivers "clean" email.	As part of the TRM/Component Framework and Security subsection, SMEMS is an example of supporting security services.
Fully managed service	Agencies benefit from a comprehensive end-to-end service that includes full support and monitoring and provides strong SLAs.	
Scalable architecture	Agencies need not purchase/own equipment, providing a cost-effective solution.	
Web-based reporting	Agencies benefit from having web access to logs and service information, available when and as they need the information.	

Table 1.6.8.1-2: Agency Benefits and FEA Facilitation. *SMES will provide Agencies with all phases of safe email delivery from gateway scanning and anti-virus/spam protection to web-based management.*

AT&T's development of net-centric technologies supports solutions based on service-oriented architecture (SOA), which uses standardized, web-adapted components. Our approach adheres to the following criteria:

- Technical Reference Model capabilities are fully met and linked to the Service Component Reference Model (SRM) and Data Reference Model (DRM).
- These links are structured to support Business Reference Model (BRM) functions and provide line-of-sight linkage to mission performance and ultimate accomplishment per the Performance Reference Model (PRM)
- AT&T operates as an innovative partner through Networx to help achieve the vision of the FEA to enhance mission performance.

In addition to the benefits and FEA facilitations cited earlier, AT&T will assist specific departments and Agencies to meet mission and business objectives through a comprehensive SMEMS offering.

1.6.8.1.c Major Issue to Service Delivery

(c) Describe the problems that could be encountered in meeting individual service requirements, and propose solutions to any foreseen problems.

In transitioning into any new service delivery model, whether it be task-based or fully outsourced, unforeseen issues can always arise. Therefore, it is

important that GSA selects a service provider that brings the depth and background to minimize an Agency's risk during transition. Our experience has enabled us to develop proven methods, processes, and procedures applicable to the simplest or the most complex projects.

Table 1.6.8.1-3 lists the top seven service delivery risks and our mitigation strategy. As with all large, SMEMS projects, we enter each of these risks and others (after identification and characterization) into our risk-tracking database, and immediately take steps to mitigate them before they become an issue. Because risk management is more effective when all stakeholders are active in the process, AT&T engages the GSA, the client Agency, and other Government solution partners for success with risk mitigation activities.

RISKS	RISK DESCRIPTION	RISK MITIGATION
Business disruption	Business disruption associated with implementing new services and integration with the Agency's enterprise architecture	[redacted]
Quick implementation of policy changes	Exposure to security threats while waiting for service provider to implement policy changes	
Jeopardy issues	All large projects encounter jeopardy issues during service delivery differences between quality provider and competitor in how they are handled.	
Unreliable service	Service that has unplanned outages and ad hoc maintenance windows and does not live up to expectations from a quality perspective.	
Equipment functionality problems	It is not uncommon for equipment not to live up to manufacturer's claims and fail to delivery functionality that customers expect.	
Vulnerability to new viruses	Exposure to security threats while waiting for Service Provider to implement virus signatures.	
Denial of Service (DoS) attacks	Agencies are continually experiencing DoS service attacks which can choke an Agencies enterprise network.	

Table 1.6.8.1-3: AT&T Service Delivery Lesson Learned and Risk Mitigation Strategies. *Agencies benefit from lessons learned and experience implementing SMEMS services, which ultimately minimize service delivery risks.*

AT&T has taken steps to identify risk and provide risk mitigation associated with delivering SMES services. AT&T is committed to service excellence, and will work with the customer to identify and support any potential problems that may occur during service delivery.

1.6.8.2 Satisfaction of Security Services Performance Requirements [L.34.1.6.2]

1.6.8.2.a Service Quality and Performance

(a) Describe the quality of the services with respect to the performance metrics specified in Section C.2 Technical Requirements for each service.

SMEMS provides redundancy and fault tolerance using geographically dispersed nodes and network management software. AT&T will meet the performance levels and acceptable quality level (AQL) of key performance indicators (KPIs) for SMEMS as presented in the RFP and **Table 1.6.8.2-1**.

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

Table 1.6.8.2-1: SMEMS Performance Metrics. *Agencies gain access to a high quality SMEMS service designed to meet all required KPIs and AQLs.*

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

1.6.8.2.b Approach to Monitoring and Measuring Performance

(b) Describe the approach for monitoring and measuring the Key Performance Indicators (KPIs) and Acceptable Quality Levels (AQLs) that will ensure the services delivered are meeting the performance requirements.

AT&T's SMEMS service has a centralized support staff that is available 24x7 to monitor, manage, and troubleshoot. This centralized support staff is responsible for gathering and reporting on the key performance indicators

(KPIs). **Table 1.6.8.2-2** provides a description of the approach to monitoring and measuring SMEMS KPIs.

KEY PERFORMANCE INDICATOR	APPROACH TO MONITORING AND MEASURING
SMEMS Availability	[redacted]
Time To Restore (TTR)	[redacted]

Table 1.6.8.2-2: Monitoring and Measuring SMEMS. *Agencies can easily manage their SMEMS service with access to executive reports and a dashboard view into service performance.*

Agencies will receive the most accurate assessment of the service when the KPI measurement and monitoring methodology replicates the real performance [redacted]

1.6.8.2.c Approach to Perform Service Delivery Verification

(c) Describe 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.

The first time the service is provided through the Networx contract, the service performance must be verified; KPIs will be monitored to certify that the service performance complies with the acceptable quality levels (AQLs). AT&T has well-defined variables and approaches to measuring those variables, which validate service delivery. These variables and measuring techniques align with the KPIs for SMEMS. **Table 1.6.8.2-3** describes verification and testing procedures for the KPIs listed.

KPI	VERIFICATION APPROACH	VERIFICATION/TESTING PROCEDURES
SMEMS Availability	[redacted]	[redacted]
Time To Restore (TTR)	[redacted]	

Table 1.6.8.2-3: Service Delivery Verification for SMEMS. *Our processes are structured to deliver SMEMS that consistently operates above the AQL thresholds, and t corrective measures are taken expeditiously in the event that these thresholds are missed.*

To simplify the verification process, AT&T has developed and documented an approach and methodology for validating service delivery. [redacted] The service verification process is presented in greater detail in Section 1.3.2.d, Approach to Perform Service Delivery Verification.

Through a comprehensive verification process, Agencies and the GSA will receive concrete data that demonstrates the readiness of the SMEMS. AT&T follows detailed procedures to verify SMEMS by comparing the KPI data against the stated AQLs, as described in the Verification Test Plan.

1.6.8.2.d Performance Level Improvements

(d) If the offeror proposes to exceed the Acceptable Quality Levels (AQLs) in the Key Performance Indicators (KPIs) required by the RFP, describe the performance improvements.

Achieving the AQLs defined by the Government for the Key Performance Indicators will result in superior SMEMS service performance. AT&T does not propose to exceed the required Acceptable Quality Levels at this time but is open to negotiate AQL values with Agencies on a task-order basis.

1.6.8.2.e Approach and Benefits for Additional Performance Metrics

(e) Describe the benefits of, and measurement approach for any additional performance metrics proposed.

The KPIs defined for the SMEMS service will provide a comprehensive assessment for service verification and service performance monitoring. Therefore, AT&T does not propose additional KPIs for SMEMS.

1.6.8.3 Satisfaction of Security Services Specifications [L.34.1.6.3]

1.6.8.3.a Service Requirements Description

(a) Provide a technical description of how the service requirements (e.g., capabilities, features, interfaces) are satisfied.

AT&T provides a complete, comprehensive, and robust security solution to Agencies for their SMEMS needs. AT&T's SMEMS service is depicted in **Figure 1.6.8.3-1** and the technical description is highlighted in **Table 1.6.8.3-1.** SMEMS satisfies core Agency needs through the following services, capabilities, and features applied to inbound/outbound email.

SERVICE REQUIREMENTS	TECHNICAL DESCRIPTION	BENEFIT TO AGENCY
Anti-spam filtering	AT&T's SMES service is a multilayer spam technology that automatically filters out unsolicited mail before it enters the Agency messaging system and disrupts employee productivity and burdens the messaging infrastructure. All messages are run through three layers of advanced spam filtering technologies: Blacklisting, Fingerprinting and Rules-based Scoring.	Agencies only receive legitimate email. Spam is removed allowing Agency employees to increase productivity by not having to deal with spam.
Anti-virus scanning	AT&T's SMES service provides the most complete anti-virus service available. Unlike premise-based solutions that may update only daily, AT&T's service provides API-level integration of [redacted] to update virus definitions every [redacted] so that the Service can identify and block viruses before they reach firewalls or servers. Outbound virus scanning is also supported.	Agencies can have confidence that their messages have been screened for the latest viruses.
Content control/ policy enforcement	Policy rules are easily enforced with Agency defined rules at the domain level for inbound and outbound email, confirming that message flow complies with agency rules and policies as well governmental laws and regulations. Agencies can block messages by attachment name/type; file size; number of recipient; domain; email address; and words and phrases.	Agencies have total control over email content and file attachments. Agencies can develop custom rules sets that meet their requirements for policy and content. Keeping messages delivered free of harmful contents and inappropriate material.
Disaster recovery	If the Agency's email server becomes unavailable, the AT&T SMEMS service stores all the emails so no email is lost or bounced. Once the Agency's service is restored, all stored mail is automatically forwarded in a "flow controlled" fashion.	Agencies can rely on AT&T SMEMS to store messages while the Agencies host email servers are down, essentially providing business continuity solution.
Reporting	Web-based management interface to the Agency for policies, rules, and routing requirements along with	Agencies have access to dashboard/executive reports to

SERVICE REQUIREMENTS	TECHNICAL DESCRIPTION	BENEFIT TO AGENCY
	email activity trends, such as [redacted] and [redacted]. Availability of statistics at AT&T's SMEMS platform.	manage their service.
Service robustness	• Proactively scanning and monitoring email traffic at AT&T SMEMS platform at gateway level, before it enters Agency's network. • Very quick processing of email at AT&T SMEMS platform to avoid any latency in delivery of email to Agencies. • SMEMS will be configured to handle any given email load and volume.	Agencies have access to a single service that provides spam filtering, virus blocking, and content management for both inbound and outbound messages.
Security integration	Supporting security functions, such as anti-virus scanning, anti-spam filtering, and content control.	Agencies can rely on a single service to satisfy three security requirements: virus scanning, spam filtering, content control
Updates	Continuously updating security engines to maintain effectiveness against threats and inappropriate material every [redacted]	Agencies are protected from the latest viruses and phising scams, because the security engines are [redacted]
Existing email support	Works in conjunction with existing Agency email systems.	SMEMS service can easily be integrated with current email systems and does not require the Agency to purchase any new equipment or software.
Secure communications	Encrypting email to/from AT&T SMEMS platform at transport layer using secure sockets layer (SSL).	Agency email is sent securely from the AT&T SMEMS servers to the Agency email servers enhancing the overall security of the email services.

Table 1.6.8.3-1: SMEMS Service Delivery Approach Summary. *SMEMS will provide the Agency with all phases of safe email delivery, from gateway scanning and anti-virus/spam protection to web-based management developed to Agency requirements.*

AT&T's SMEMS service incorporates anti-spam filtering, anti-virus blocking and content management/policy enforcement for both inbound and outbound messages. Using highly accurate, multilayered filtering technologies hosted in AT&T's global network of Internet Data Centers, the service provides a front-line defense against viruses, unsolicited email and inappropriate content.

Figure 1.6.8.3-1: Secure Email Features. *SMEMS scans and monitors email traffic at the network level before it is allowed to enter the Agency's network, thereby protecting the Agency from viruses, Trojan horses, and other hostile content.*

Descriptions of SMEMS key features and capabilities are described below:

- **Anti-spam Filtering – Figure 1.6.8.3-2** shows how multilayer spam technology filters unsolicited email automatically before it enters the Agency messaging system, thereby preventing disruption of employee productivity and burdening the messaging infrastructure. All messages are run through [redacted] of advanced spam filtering technologies: [redacted]

Figure 1.6.8.3-2: SMEMS Spam Filtering. *The AT&T SMEMS platform has [redacted] of filtering to eliminate spam emails.*

- **Anti-virus Blocking – Figure 1.6.8.3-3** shows SMEMS complete anti-virus service. Unlike premises-based solutions that can be updated only daily, AT&T's service provides API-level integration of virus engines from various vendors, allowing each vendor to update virus definitions every [redacted] Therefore, SMEMS will identify and block viruses before they reach firewalls or servers.

Figure 1.6.8.3-3: SMEMS Virus Filtering. *Email is filtered using* [redacted] *updated every* [redacted] *as necessary, to eliminate email infected with virus before it reaches the Agency network.*

- **Content Control – Figure 1.6.8.3-4** shows SMEMS policy rules are easily enforced with Agency-defined rules at the domain level for inbound and outbound email in compliance with company rules and policies as well as Governmental laws and regulations. The Agency can block messages by attachment name/type; file size; number of recipients; domain; email address; and words and phrases.
- **Outbound Service –** AT&T SMEMS includes the ability to provide outbound virus scanning and enables the monitoring of email and attachments through configurable policy enforcement set by the Agency. This can include blocking any secret information from leaving the Agency through email.

Figure 1.6.8.3-4: SMEMS Content Filtering. *AT&T enforces Agency policy rules at the SMEMS platform to prevent unwanted content from reaching its network.*

- **Disaster Recovery –** If the Agency email server becomes unavailable, the AT&T SMEMS stores mail so that no messages are lost. Once service is restored, stored mail is automatically forwarded in a flow-controlled fashion to Agency mail servers. AT&T SMEMS automatically continues to try every [redacted] to determine if the Agency servers are up and ready to accept email. The SMEMS platform is also provisioned to store Agency's email for [redacted] and deliver it once Agency servers are restored.

1.6.8.3.b Attributes and Values of Service Enhancements

(b) If the offeror proposes to exceed the specified service requirements (e.g., capabilities, features, interfaces), describe the attributes and value of the proposed service enhancements.

The service requirements defined by the Government for SMEMS are complete and comprehensive. [redacted]

1.6.8.3.c Service Delivery Network Modifications

(c) Describe any modifications to the network required for delivery of the services. Assess the risk implications of these modifications.

Agencies receive a low-risk solution through AT&T's ability upon contract award to provide SMEMS without any modifications to the network or operational support systems.

1.6.8.3.d Security Services Experience

(d) Describe the offeror's experience with delivering the mandatory Security Services described in Section C.2 Technical Requirements.

Agencies are offered extensive experience providing managed security services that create value to our customers to both in Government and commercial entities. This experience has given us the ability to engineer and deliver quality services. AT&T's experience is described in **Table 1.6.8.3-2**. AT&T's operations background makes us an obvious choice for many companies who require mission critical email services.

[redacted]

Client Need	Solution	Created Value
[redacted]	[redacted]	[redacted]

Table 1.6.8.3-2: Service Experience. *AT&T has an extensive history in providing secure email services to customers as well as protecting their own vast infrastructure.*

1.6.8.4 Stipulated Deviations

AT&T takes neither deviation nor exception to the stipulated requirements.

Stratecast Partners

AT&T receives the "2005 Best-in-Class NSP Managed Security Services Award" for being "best positioned to serve the broadest and largest number of customers and create strategic differentiation for the company (either as AT&T or the merged AT&T and SBC) in the evolving communications industry."

--April 2005