1.6.5 Anti-Virus Management Service (AVMS) [C.2.10.4]

The Agency will protect their network and servers from viruses/worms and malicious code by using a high-quality, anti-virus management service (AVMS) security solution. AVMS will take advantage of server and desktop protections, where applicable, to strengthen the security of the Agency computing environment.

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

1.6.5.1.a Approach to Service Delivery

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

AT&T will provide the Agency with an anti-virus management service (AVMS) that is fully compliant with the requirements in the RFP and provides the capabilities discussed in this section. The Agency attains its vision for AVMS through the deployment of a service that offers multilayered protection at gateway, server, and desktop levels. Our AVMS, at the network layer, inspects all packets entering from an unprotected network, such as the Internet, into the Agency's private enterprise network. The network can consist of AT&T's premises-based Internet protocol (IP)-virtual private network (VPN) services (PBIP-VPN) or network-based IP VPN services (NBIP-VPNS). In addition to network gateway virus protection, we will offer desktop and server-based protection as a second layer of security. Virus protection is provided for the entire Agency's network and server equipment to support the integrity of the Agency's Information Technology (IT) services.

Figure 1.6.5.1-1 shows how network based anti-virus protection scans all IP packets for virus signatures within single or multiple packets at the shared gateway. This comprehensive inspection process provides data protection and integrity.

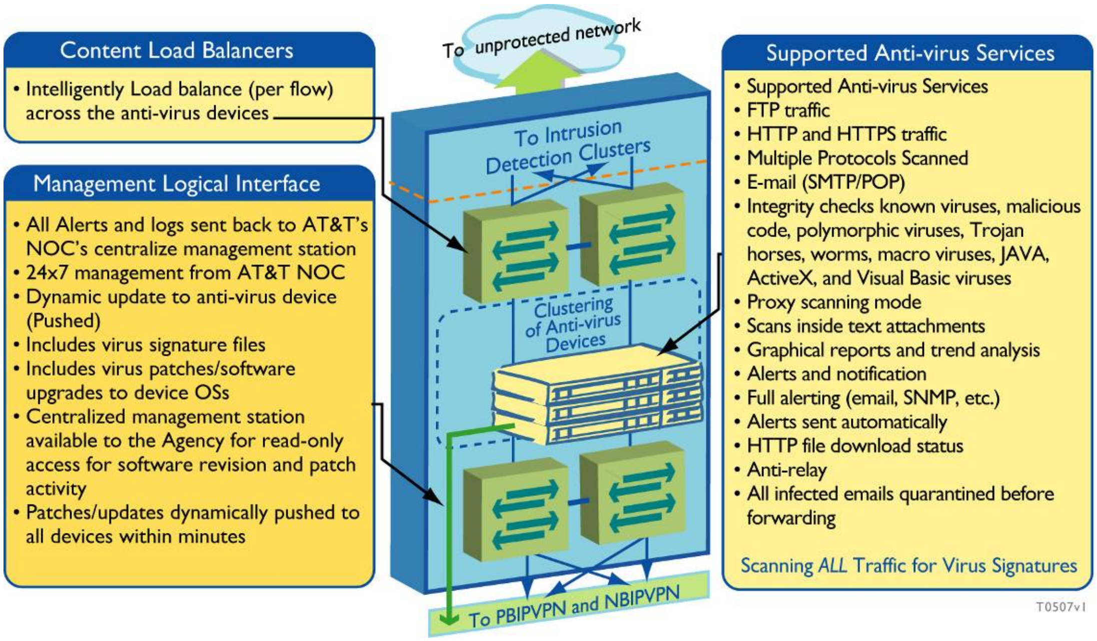
Content Load Balancers
• Intelligently Load balance (per flow) across the anti-virus devices
Management Logical Interface
• All Alerts and logs sent back to AT&T's NOC's centralize management station
• 24x7 management from AT&T NOC
• Dynamic update to anti-virus device (Pushed)
• Includes virus signature files
• Includes virus patches/software upgrades to device OSs
• Centralized management station available to the Agency for read-only access for software revision and patch activity
• Patches/updates dynamically pushed to all devices within minutes
To unprotected network
To Intrusion Detection Clusters
Clustering of Anti-virus Devices
To PBIPVPN and NBIPVPN
Supported Anti-virus Services
• Supported Anti-virus Services
• FTP traffic
• HTTP and HTTPS traffic
• Multiple Protocols Scanned
• E-mail (SMTP/POP)
• Integrity checks known viruses, malicious code, polymorphic viruses, Trojan horses, worms, macro viruses, JAVA, ActiveX, and Visual Basic viruses
• Proxy scanning mode
• Scans inside text attachments
• Graphical reports and trend analysis
• Alerts and notification
• Full alerting (email, SNMP, etc.)
• Alerts sent automatically
• HTTP file download status
• Anti-relay
• All infected emails quarantined before forwarding
Scanning ALL Traffic for Virus Signatures
T0507v1

Figure 1.6.5.1-1: AT&T Robust Anti-virus Process and Platform. *With the centralized management station, patches and updates can be dynamically pushed to all devices within minutes.*

AT&T's robust anti-virus process and platform supports the scanning of packets traversing the gateway from a trusted environment to an untrusted one for a high level of virus protection. [redacted] appliance is installed behind the gateway firewalls and intrusion detection systems (IDSs). These anti-virus appliances will scan and remove all detected viruses and malware with little or no impact on the performance of an Agency's network services. The [redacted] appliance is an integrated solution that combines award-winning anti-virus, anti-spam, and content management software with enhanced hardware. Tuned for performance, the [redacted] appliance offers [redacted], quickly addressing the Agency's anti-virus requirements. The appliance will be configured in a cluster configuration that will allow for redundancy and scalability. Clustering allows the appliances to function virtually as a single device, while physically being multiple devices. This clustering will enable AT&T to add another appliance when the traffic load requires more virus scanning processing.

AT&T will monitor and manage 24x7 all the devices at the gateway. [redacted] is automatically updated with the latest anti-virus data files so that the anti-virus devices are always running the latest version providing complete anti-virus protection. The centralized management station supports this update and complies with the Federal Computer Incident Response Center (FedCIRC) standards, policies, and recommendations. This includes the capability to automatically update the virus signatures from a central server (located within our [redacted]) that will push updates to each managed and value-added workstation and server. If a virus is found on a host system, this event is logged, and an alert is generated. **Table 1.6.5.1-1** summarizes the anti-virus management system (AVMS) delivery approach for protecting Agencies from security threats associated with detected viruses.

SERVICE DELIVERY APPROACH	TECHNICAL DESCRIPTION
Standards compliance	Support the following standards as applicable: • E-Government Act of 2002, Title III (Federal Information Security Management Act (FISMA)) • National Institute of Standards and Technology (NIST) Federal Information Processing Standards Publication (FIPS) 140 - 2 — Security Requirements for Cryptographic Modules • NIST FIPS PUB 199 — Standards for Security Categorization of Federal Information and Information Systems • United States Computer Emergency Readiness Team (US-CERT) reporting requirements
2-tiered protection architecture	• Deployment of gateway level [redacted] appliance fully engineered for maximum throughput and load balancing. • Deployment of [redacted] capable of automatic download of new definition and rules on Agency windows-based servers.
Shared network based services	Network-based virus protection is provided to Government in shared environment and protects Agency from virus threats that can be introduced from the Internet.
Clustering of anti-virus appliances/load sharing	Multiple anti-virus servers are clustered at gateway. This clustering enables many anti-virus servers to operate as single server.
All servers	• WebShield appliance is configured to scan inbound and outbound traffic for simple mail transfer protocol (SMTP), HyperText transfer protocol (HTTP), FTP, and post office protocol version 3 (POP3) protocols, as desired by Agency.

SERVICE DELIVERY APPROACH	TECHNICAL DESCRIPTION
	• Agency windows-based servers are loaded with AV software and configured to detect and mitigate malicious code. • Loaded AV software complements AV software already implemented on Agency desktops. • AT&T configures AVMS solution components to automatically update latest definitions rules to detect and remove new discovered viruses/worms. • AT&T deploys necessary ePO servers, FTP servers, and SQL servers in AT&T IDCs.
Windows-based mail servers	[redacted] software supplied for these servers.
Microsoft exchange mail servers	[redacted] supplied for these servers.
Lotus domino mail servers	[redacted] supplied for these servers.
Integrated with other security services	• Integrated security solutions allow Agencies to build appropriate amount of security depth that will meet their security requirements and budget. • Integrates through layering between our intrusion detection and firewalls
Test and certification	• AT&T will test and certify Agency's AVMS before and after implementation • Verifies that solution operates and functions in accordance with KPIs.

Table 1.6.5.1-1: AVMS Approach. *The AVMS solution provides a full set of features to meet the Agency's anti-virus scanning needs, including gateway and server protection mechanisms to detect and eliminate malicious code before it enters the Agency's internal networks.*

The AT&T AVMS solution is the leading anti-virus detection and removal answer in the industry for protecting the Agency's networks, as well as AT&T's own complex infrastructure. It is consistent with AT&T's security vision of moving protections onto the gateway level, where potential problems will be detected and mitigated on ingress and egress before they ever reach the Agency's servers.

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) Magic Quadrant

1.6.5.1.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 anti-virus 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 1.6.5.1-2** describes each service in relation to FEA, summarizes its contribution, and/or provides an example of how it facilitates FEA implementation.

SERVICE DELIVERY APPROACH	BENEFITS	FEA FACILITATION
Standards compliance	Delivers a service that is consistent with the established best practices	Service Access and Delivery: • Service Transport – Supports network services Component Framework • Security - Supports security services
2-tiered protection architecture	Offers virus protection at network and server level, providing higher level of protection to Agency.	
Shared network based services	Offers flexibility for large Agencies and affordability for small Agencies.	
Clustering of anti-virus appliances/load sharing	• Offers scalability to the agency by allowing AT&T to add a new appliance to the cluster. • Improved reliability clustering allows virus appliances to offer a backup capability to another.	
All servers	• The [redacted] appliance is configured to scan inbound and outbound traffic for SMTP, HTTP, FTP, and POP3 protocols, as desired by the Agency. • Agency windows-based servers are loaded with AV software and configured to detect and mitigate any malicious code. • Loaded AV software complements the AV software already implemented on Agency desktops. • AT&T configures AVMS solution components to automatically update the latest definitions rules to detect and remove any new discovered viruses/worms. • AT&T deploys the necessary [redacted] in AT&T IDCs.	
Windows-based mail servers		
Microsoft exchange mail servers		
Lotus domino mail servers		
Integrated with other security services	Integrated security solutions allow Agencies to build the appropriate amount of security depth that will meet their security requirements and budget.	
Test and certification	Verifies that a solution will operate and is functioning properly in accordance with the KPIs.	

Table 1.6.5.1-2: Agency Benefits and FEA Facilitation. *Agencies will receive products and services components that are easily integrated, commonly manageable, and aligned to support FEA objectives and meet FEA guidelines.*

AT&T's development of net-centric technologies supports solutions based on service-oriented architecture (SOA), which uses standardized, web-adapted components. Our approach ensures that the criteria listed below are followed:

- 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 AVMS offering.

1.6.5.1.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 select 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 1.6.5.1-3 lists the top ten service delivery risks and our mitigation strategy. As with all large, anti-virus 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.

RISK	DESCRIPTION	RISK MITIGATION
Business disruption	In our experience, all Agencies are concerned about business disruption when moving to a new service. Adequate planning will minimize this risk.	[redacted]
Gateway sizing	Often, when scanning many packets on very large enterprises, anti-virus clusters can become overwhelmed and impede performance.	[redacted]

RISK	DESCRIPTION	RISK MITIGATION
		[redacted]
Equipment functionality	It is not uncommon for premises equipment not to live up to manufacturers' claims and fail to deliver functionality that Agency expects.	[redacted]
Jeopardy issues	All large projects encounter jeopardy issues during service delivery differences between quality provider and competitor in how they are handled.	[redacted]
Viruses not caught at gateway level	Since not all security protection is foolproof, it is possible that viruses cannot be caught at gateway level.	[redacted]
Loss of service	Server and appliance availability can be an issue.	[redacted]
Interference	Updates and upgrades can interfere with Agency's daily schedule.	[redacted]
Untimely administration	Requested changes to system configuration cannot be deployed in a timely fashion.	[redacted]
New compromised devices	• To achieve AV protection at gateway level, AT&T deploys multiple WebShield appliances at Agency premise behind Agency network facing firewall. • To achieve AV protection at server level, AT&T deploys multiple AV update servers at AT&T IDC and establishes connectivity with Agency's network.	[redacted]
Open firewall ports	Agency is required to open Ports 1000, 1001, and 1011 for [redacted] communication. [redacted] communication also needs Port 1433 for SQL, and FTP port for AV file download.	[redacted]

Table 1.6.5.1-3: Risk Mitigation to Service Delivery. Agencies will receive reliable AVMS though risk mitigation, allowing the Agency to concentrate on core business issues.

AT&T has taken steps to identify risk and provide risk mitigation associated with delivering AVMS. AT&T is committed to service excellence and will work with the Agency to identify and resolve potential problems that might occur during service delivery.

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

1.6.5.2.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.

AT&T is committed to offering the Government the highest quality in security service. This commitment extends beyond simple promises. Our commitment is supported by offering the Government financial commitments in the form of SLAs. [redacted] meet the [redacted] of key performance indicators (KPIs) for AVMS for routine and critical users, as presented in the RFP and in **Table 1.6.5.2-1**.

> THE WALL STREET JOURNAL.
> *Cyber-Security is Hot Niche in which AT&T has established an early lead.*

KEY PERFORMANCE INDICATOR (KPI)	SERVICE LEVEL	PERFORMANCE STANDARD (THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
AVMS Availability	Routine	99.5%	[redacted]
Time To Restore (TTR)	Without Dispatch	4 hours	[redacted]
	With Dispatch	8 hours	[redacted]
Grade of Service (Virus Updates)	Routine	Within 24 hours for a normal priority schedule	[redacted]
		Within 2 hours for an urgent priority update	[redacted]

Table 1.6.5.2-1: IP Network Performance Parameters. *Agencies will be positioned to better manage anti-virus services through performance-based contracts that deliver the quality of service required to meet Agency performance objectives.*

AT&T's confidence in our ability to deliver these performance results is supported by past performance and is backed by stringent service credits.

1.6.5.2.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 monitors the KPIs to verify they are within the guidelines of the AQLs within our [redacted] using our [redacted] AT&T will accurately measure server availability and time to restore (TTR) and/or repair. AT&T also benchmarks our performance against industry-wide standards to ensure that we continually improve on service to our clients. **Table 1.6.5.2-2** provides a description of the approach to monitoring and measuring of the KPIs, as listed by the Government.

KEY PERFORMANCE INDICATOR	APPROACH TO MONITORING AND MEASURING
AVMS Availability	[redacted]
Time To Restore (TTR)	[redacted]
Grade of Service (Virus Updates)	[redacted]

Table 1.6.5.2-2. Monitoring and Measuring AVMS. *Agencies can easily manage the anti-virus service with easy to access and use data delivered through the AT&T* ***Business****Direct*[®] *web portal. AT&T maintains availability, grade of service and time to restore KPIs.*

Of equal importance to identifying the KPIs for a service is the method by which the KPIs are captured, measured, and monitored. 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.

1.6.5.2.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.

AT&T will conduct monthly service quality reviews with the Agency to discuss performance, including adherence to contracted performance guarantees. **Table 1.6.5.2-3** describes verification and testing procedures for the KPIs, as listed by the Government. 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 AQL.

KPI	VERIFICATION APPROACH	VERIFICATION/TESTING PROCEDURES
AVMS Availability	[redacted]	[redacted]
Time To Restore (TTR)	[redacted]	[redacted]
Grade of Service (Virus Updates)	[redacted]	[redacted]

Table 1.6.5.2-3: Verification of Acceptable Performance for AVMS. *Agencies will receive AVMS that consistently operates above the AQL thresholds and takes corrective measures expeditiously in the event that these thresholds are missed.*

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

1.6.5.2.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 Acceptable Quality Levels defined by the Government for the KPIs will result superior AVMS performance. [redacted]

1.6.5.2.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 by the Government for the AVMS will provide a comprehensive assessment for service verification and service performance monitoring. However, we understand the importance of Agencies needing more comprehensive KPIs [redacted]

1.6.5.3 Satisfaction of Security Services Specifications [L.34.1.6.3]

1.6.5.3.a Service Requirements Description

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

1.6.5.3.a.1 Service Description

The following sections present an understanding of the standards, connectivity needs, and required technical capabilities related to providing AVMS functional description, connectivity, and technical capabilities.

1.6.5.3.a.2 Functional Description

Most providers of AVMS do not offer multiple protections against viruses. They will block anti-virus at the server and desktop level only. Additionally, there are network level protections that look for [redacted] at the [redacted] before scanning at the server and desktop level. Our two-tiered solution will scan for viruses at both the network and server level to minimize the risk associated that a virus will infect and Agency's enterprise.

Our AVMS meets the Agency's anti-virus scanning requirements through the AVMS architecture at the gateway server levels (**Figure 1.6.5.3-1**).

Figure 1.6.5.3-1: AVMS Desktop and Server Security Solution. In *addition to the AVMS network-based scanning capabilities, we will offer desktop and server protection with auto-upgrades and provide a web management interface for reports and scans.*

In searching for a comprehensive and effective anti-virus solution to protect Government and commercial customers, [redacted] we believe that this server-based, anti-virus solution is the leading anti-virus detection and removal software in the Industry. This is consistent with our security vision of moving protections onto the network, where potential problems can be detected and mitigated on ingress and egress before they ever reach the Agency's networks. **Table 1.6.5.3-1** lists our services features and functions.

FEATURES	DESCRIPTION
Presales design and engineering services	Before task order issuance, AT&T will provide engineering assistance to work with Agencies to gain understanding of security environment, provide technical details about our services and solutions, and provide design services.
Support for government standards	AT&T will offer solutions that will meet Federal Information Security Management Act (FISMA), Federal Information Processing Standard (FIPS) 140-2, National Institute of Standards and Technology (NIST) FIPS 199, and US-CERT.
Implementation support	AT&T will provide installation, configuration, and integration support to the Agency per the Agency's requirements and security design.
Antivirus load sharing	Our solution will use clustering technology that provides a better load-sharing capability.
Fully managed service	• Complete end-to-end service with single POC to address any anti-virus pertaining to issue. • AVMS includes trained, certified staff to develop, operate, and maintain consistent and reliable service. • AVMS provides high-quality service backed by strong SLAs. • 24x7x365 monitoring of AV solution and anti-virus advisories. • Alert to network administrators.
Web-based reporting	Web access to logs and service information.
Gateway level protection	At the Agency gateway level or first layer of defense, AT&T's fully managed [redacted] appliance is inserted seamlessly and transparently into the Agency's existing network. As traffic passes through the [redacted], it is fully inspected to determine whether it is legitimate or malicious.
Server level protection	• At the second layer of defense, the Agency-identified, window-based servers are loaded with anti-virus software. • AT&T works with the Agency to load the initial anti-virus software, [redacted] • The anti-virus software will be running in a proactive mode, monitoring every write and read access on the server. The proactive monitoring ensures detection and removal of any malicious viruses from files. • The AV software is configured to scan executable files and boot blocks on a preconfigured time interval basis. • AT&T suggests this configuration, which is subject to Agency application performance considerations. Extensive scans can result in reduced performance on a machine and should not be executed during peak production times.
Automatic routine updates	• All [redacted] are managed by AT&T hosted [redacted] servers. [redacted] are configured to receive daily routine updates. [redacted]
Priority updates	• All [redacted] are managed by AT&T-hosted [redacted] configures [redacted] so that critical updates will be pushed to all the managed devices in [redacted]
Web interface	• AT&T's AVMS provides a web portal that will provide reports, anti-virus advisories, and software, hardware maintenance, and anti-virus software upgrades of [redacted] • At the AV server update level, AT&T deploys multiple AV update FTP servers in their IDC. • AT&T deploys FTP update servers in DNS round robin to provide load balancing, reliability, and redundancy, without modifying the options setting on Agency servers.
Surveillance	Scheduled, on-demand, automatic update of new virus signature files on gateways scanning appliance and servers
Test and certification	AT&T will test and certify Agency's AVMS before and after implementation to verify KPI compliance.

Table 1.6.5.3-1: AVMS Capabilities Meets Agency's Anti-Virus Scanning Requirements. *The Agency will be provided with a fully-managed, high-quality service to guard against viruses entering its network.*

Agencies will receive a comprehensive suite of AVMS features and capabilities that will provide them with two layered protection from virus threats.

1.6.5.3.a.3 Interfaces Description

Our service will provide interface to Agencies networks as shown in **Figure 1.6.5.3-1**. These interfaces will consist of connections to IPS, PBIPVPN, and NBIPVPN through the shared gateway perimeter protection.

1.6.5.3.b Attributes and Values of Service Enhancements

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

The current set of requirements protects the Agency's network from detected virus activity. No other requirements are proposed.

1.6.5.3.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 to offer AVMS upon contract award without modifications to the network or operational support systems.

> *"But in the last year and a half they [AT&T] have been bitten by the security bug. They are aggressively evaluating next-generation technology. [AT&T] is a true thought leader in the industry."*
>
> --The Yankee Group, June 2003

1.6.5.3.d Security Services Experience

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

AT&T has provided AVMS to both internal, Government, and commercial entities in the past. This experience has given us the ability to engineer and deliver services that create value to our customers. **Table 1.6.5.3-2** cites some examples of AT&T's ability to deliver AVMS.

[redacted]

AT&T NEED	SOLUTION	CREATE VALUE

AT&T NEED	SOLUTION	CREATE VALUE
[redacted]	[redacted]	[redacted]

Table 1.6.5.3-2: Service Experience. *AT&T has an extensive history in providing anti-virus services to both customers as well as protecting their own vast infrastructure.*

1.6.5.4 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 in the evolving communications industry."

--April 2005

1.6.5.5 EMNS AntiVirus Management Service (AVMS)

The added sections are provided to Agencies ordering Enhanced Managed Network Service (EMNS) and are ordered with other EMNS service components.

1.6.5.5.1 EMNS AVMS - Service Description

The AT&T virus protection solution inspects all packets entering the Internet access point protecting the Agency-wide enterprise from viruses. We provide virus protection for all EMNS managed equipment to protect the integrity of the EMNS managed network services.

Figure 1.6.5.5-1 shows how our anti-virus protection scans all IP packets for virus signatures within a single or multiple packets. This comprehensive inspection process provides superior data protection and integrity.

Figure 1.6.5.5-1. EMNS AVMS Service: [redacted]

The [redacted] in conjunction with the [redacted] represents a comprehensive anti-virus, anti-spam, and content filtering solution. The [redacted] will filter and discard all mail traffic for viruses and spam mail.

The [redacted] appliance installed behind the firewall service module scans all web traffic and removes viruses and malware with little or no impact on the performance of the Agency's EMNS services. The Agency's network and users are protected when browsing the Web, downloading files, or during e-mail activities.

The [redacted] also provides a centralized management solution that gives the Agency the ability to view all logs and alerts. Logs and alerts are stored for [redacted] year on-line and [redacted] years off-line. The Agency has read-only access to the anti-virus equipment and secure data feed to the Agency SOC.

AT&T will automatically update [redacted] with the latest anti-virus data files so that the anti-virus devices are always running the latest version, providing complete anti-virus protection. A centralized management station supports this update and complies with Federal Computer Incident Response Center (FedCIRC) standards, policies, and recommendations.

AT&T will provide that all EMNS workstations and servers remain secure and free of viruses along with securing all network traffic. AT&T provides an anti-virus client on each workstation or server deployed as part of the EMNS services (Web Servers, DNS, E-mail servers, etc). This includes capability to automatically update the virus signatures from a central server located within the Agency intranet that can 'push' updates to each EMNS-managed and value-added workstation and server. If a virus is found on a host system, this event is logged.

When required, load-balance switches intelligently distribute the IP flows across a cluster of antivirus appliances. The cluster design allows the antivirus solution to scale to support all the required peak bandwidths.

AT&T complies with all FedCIRC recommendations and will provide proof of compliance in the bi-monthly meeting with the Agency.

Table1.6.5.5-1 describes the peak port speeds for the EMNS IDPS service:

DESCRIPTION
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

DESCRIPTION
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]
[redacted]

Table 1.6.5.5-1: EMNS AntiVirus Management Service Port Speeds. *The EMNS AVMS provides peak ports speeds that range from* [redacted].

1.6.5.5.2 EMNS AVMS – EMNS AVMS Enhanced SED (ESED) Description

For the EMNS AVMS service, the [redacted] series security appliance will be provided as EMNS AVMS ESED. The [redacted] is a stand[redacted] that scans inbound and outbound traffic for SMTP, HTTP, FTP and POP3 protocols looking for viruses. Always up-to-date, the [redacted] Appliance automatically seeks and downloads the latest definitions, rules and engines.

One of the following [redacted] security appliances will be bundled with the EMNS AVMS offering:

[redacted]

In addition to providing a [redacted] Webshield appliance at each EMNS AVMS location, the following ancillary site services are included with the EMNS AVMS.

- Equipment and accessories required to install and maintain the EMNS AVMS ESED at all EMNS AVMS sites. This shall include, but is not limited to racks, cables, tools, etc.
- Space and power requirements - such as such as physical space, rack space, power, and HVAC - defined for EMNS AVMS ESED at each EMNS AVMS site.

- Operations and management of hardware and software components up to the EMNS AVMS demarcation point.

AT&T will label and run cable according to guidelines provided by the Government in locations where cable extensions are required to connect an EMNS AVMS ESED to the Government-specified demarcation point. Government guidelines and any additional local procedures provided by the Government will be followed for accessing, installing and maintaining all EMNS AVMS ESEDs.

The Installation and Maintenance CLINs for the EMNS AVMS ESEDs will be found in the SED section (B.4.11) of the Pricing Volume.