1.6.2 Managed Firewall Services (MFS) [C.2.10.1]

Agencies will benefit from secure, low risk, highly available, and flexible managed firewall services (MFS) that exceed government requirements. Agencies have the choice of a network-based or premises-based MFS service offer to thwart attacks and secure its internal networks. MFS will support the Agency's specific security policies and will be tailored for specific needs. MFS is just one of the tools in a layered approach to security that will help reduce service disruptions caused by malicious access attempts.

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

1.6.2.1.a Approach to Service Delivery [L.34.1.6.1.a]

(a) Analyze the service requirements specified in this solicitation and describe the approaches to service delivery for each service. [L.34.1.6.1.a]

AT&T managed firewall services (MFS) provides a proactive security approach to help thwart attacks and to help protect the confidentiality, integrity, and availability of mission-critical resources. MFS offers a variety of options that will support the Agency's most stringent security requirements. Our comprehensive Security in Depth architecture includes inbound and outbound access control, authentication, encryption, filtering, analysis, traffic segregation, and other security tools that add layers of protection to specific applications.

Our MFS suite encompasses network and premised-based solutions that will cohesively integrate with intrusion detection systems (IDS), multiple access redundancy options (MARO), Agencies' extranets and virtual private networks (VPNs), and Internet Protocol (IP)-based protocols to enhance network security and performance. MFS platforms have been subject to extensive evaluation, testing, and certification by AT&T Labs before deployment.

Security is what AT&T does best. Our legacy and vast experience in protecting our own network as well as our customers' networks speaks for itself. MFS also includes the expertise of our network operations and security professionals working together 24x7 to proactively manage, troubleshoot, and resolve security issues in real time. Our comprehensive portfolio of MFS provides the Government a low total cost of ownership, peace of mind, and most importantly, more time to focus on its core business. **Figure 1.6.2.1-1** provides a graphical overview and capabilities of MFS.

Security is no longer simply an enabling technology – it is a fundamental component of network design. As more and more organizations understand that the network can help secure their key transactions and communications, this new, powerful, and convenient medium is becoming the business standard. To help protect the integrity of a customer's network, managed security service providers (MSSPs), such as AT&T, have built security into the infrastructure. AT&T has an end-to-end managed firewall solution that exceeds the requirements of our Government clients, whether the infrastructure resides within the network and/or at the customer's premises.

Table 1.6.2.1-1 describes the various MFS components and their customer benefits. AT&T's MFS service is designed and deployed with the goal of providing secure, reliable, flexible, high-quality and standards based-technology solutions to a diverse user base. This approach has made AT&T an industry leader in the MSSP market place.

Figure 1.6.2.1-1: AT&T Network and Premises-based Managed Firewall Services. *Agencies benefit from a secure, highly available, flexible MFS service that can help to protect an Agency's enterprise.*

SERVICE DELIVERY APPROACH	DESCRIPTION
Shared and dedicated services	• Service delivery in shared environment is provided over AT&T secured network infrastructure. • Service delivery in dedicated environment is provided by deploying security infrastructure inside customer's premises. • Service delivery for personal firewall is provided on individual user machines for remote connectivity.
Multilayer protection	Agency can use network-based, premises-based, or personal firewalls in stand-alone environments or in combination for added protection.
Fully managed service	Comprehensive end -to-end service that includes 24x7 support for proactive, real-time monitoring and management.
E-servicing	Web access to logs, service information, and management reports
Standards compliance	Ability to provide vendor-agnostic services that interoperate and maintain flexibility: • 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
Test and certification	• AT&T will test and certify Agency's MFS service before and after implementation • Verifies that solution will operate and is functioning properly in accordance with KPIs.
Integrated with other services	MFS is easily integrated with other Networx services to develop custom solutions. MFS works with the following services: • Intrusion Detection Systems • VPNS • Encryption • Authentication • Anti-virus • Secure E-mail • Hosting

Table 1.6.2.1-1: MFS Service Delivery Approach. *Agencies can subscribe to a MFS security service which offers feature rich, flexible service offerings and reduce the Agencies total cost of ownership.*

1.6.2.1.b Benefits to Technical Approach [L.34.1.6.1.b]

(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). [L.34.1.6.1.b]

AT&T's Networx services, in general, and MFS 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 1.6.2.1-2** describes each service delivery approach in relation to FEA, summarizes its contribution, and/or provides an example of how it facilitates FEA implementation.

SERVICE DELIVERY APPROACH	BENEFITS	FEA FACILITATION
Shared and Dedicated Services	Enables Agencies to decide between dedicated vs. shared environments and the associated cost benefits of those options.	As a component of the TRM/Component Framework within the Security section, Agencies can reduce total cost of ownership by utilizing shared environments or attain certain security accreditations with a dedicated environment.
Multilayer Protection	Agencies can design custom MFS solutions that support different configurations ranging from large enterprise offices all the way down to home office or travel use.	As a component of the TRM/Component Framework within the Security section, Agencies can develop security solutions unique to their requirements.
Fully Managed Service	Agencies can confidently reduce management of their MFS services and focus on core Agency objectives.	As a component of the TRM/Component Framework within the Security section, Agencies can reduce total cost of ownership by outsourcing monitoring and management of their MFS environment to a reliable MSSP provider.
E-Servicing	Agencies easily and efficiently update rule sets, receive alert notifications, manage trouble tickets and view management reports.	As a component of the TRM/Component Framework within the Data Management section, Agencies have access to data relevant to planning or managing their service, which allows Agencies to meet their mission objectives more efficiently.
Standards Compliance	Agencies will be technology and vendor agnostic, allowing them the flexibility of not being tied into a particular technology or vendor.	As a component of the TRM/Component Framework within the Security section, Agencies can reduce barriers associated with closed networks and incompatibility between technologies and vendors.
Test and Certification	Agencies will have confidence in the MFS service, because the service will be validated upon installation. The service will operate and function properly in accordance with the KPIs.	As a component of the TRM/Service Interface and Integration within the Interoperability section, Agencies will have documentation illustrating service configuration and interoperability testing.
Integrated with other Services	Agencies can combine their MFS services with other security and Hosting services to create custom environments based on Agencies' unique requirements.	As a component of the TRM/Service Interface and Integration within the Interoperability section, Agencies will have the ability to develop custom solutions that provide for greater flexibility in meeting their objectives.

Table 1.6.2.1-2: Agency Benefits and FEA Facilitation. *Agencies can receive products and service 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 embraces 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.

[redacted], AT&T will assist specific departments and Agencies to meet mission and business objectives through a comprehensive MFS offering.

1.6.2.1.c Major Issue to Service Delivery [L.34.1.6.1.c]

(c) Describe the problems that could be encountered in meeting individual service requirements, and propose solutions to any foreseen problems. [L.34.1.6.1.c]

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 1.6.2.1-3 lists the top seven service delivery risks and our mitigation strategy. As with all large, MFS 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	In our experience, all Agencies are concerned about business disruption when moving to a managed service. Adequate planning will minimize this risk.	[redacted]
Incorrect sizing	Security devices (hardware and software) must be adequately configured to support certain	[redacted]

RISKS	RISK DESCRIPTION	RISK MITIGATION
	number of users, concurrent connections, features, and throughput. AT&T offers small, medium, large, and high-availability configurations, based on specific Agencies' needs.	[redacted]
Equipment failures	Although AT&T uses the most reliable equipment in the industry, it is not uncommon for premises equipment not to live up to manufacturers' or vendors' claims and fail to deliver functionality that customer expects.	[redacted]
Inadequate enforcement of security policies	Incorrectly implemented security policies can cause a firewall to overlook certain parameters or logic permitting unacceptable traffic.	[redacted]
Loss of service.	Availability issues can arise as result of unusual circumstances, such as local fiber cuts, loss of power, attacks to system, etc.	[redacted]
Interference	Updates and upgrades can interfere with Agency's daily schedule.	[redacted]
Untimely administration	Requested changes to system configuration might not be deployed in timely fashion.	[redacted]

Table 1.6.2.1-3: AT&T Service Delivery Lessons Learned and Risk Mitigation Strategies. *Agencies benefit from lessons learned and experience implementing, monitoring and managing MFS services, which ultimately minimize service delivery risks.*

AT&T has taken steps to identify risk and provide risk mitigation associated with delivering MFS services. 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.

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

1.6.2.2.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. [L.34.1.6.2.a]

Government Agencies will experience the highest quality MFS service offered that sets the industry standards for performance and quality. AT&T will comply with and meet or exceed the MFS quality performance metrics specified in Section C.2.10.1.4.1, as illustrated in **Table 1.6.2.2-1.**

KPI	SERVICE LEVEL	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Availability	Routine	99.5%	[redacted]
Event Notification (EN)	Routine	Next business day for a low category event	[redacted]
		Within 4 hours of a Medium category event	[redacted]
		Within 30 minutes of a High category event	[redacted]
Grade of Service (Configuration/ Change)	Routine	Within 5 hours for a normal priority change	[redacted]
		Within 2 hours for an urgent priority change	[redacted]
Time to Restore (TTR)	Without Dispatch	4 hours	[redacted]
	With Dispatch	8 hours	

*

Table 1.6.2.2-1: MFS Performance Metrics. *Agencies will be positioned to better manage their MFS services through performance based contracts that deliver the quality of service required to meet Agency performance objectives.*

AT&T offers [redacted] for our customer base by building our MFS-network based with reliability and redundancy. Redundancy provides reliability. From its inception, MFS-network based was designed to eliminate any single point of failure. Our MFS-network based firewalls are located in physically diverse data centers. The data centers provide redundant power and network connections, as well as emergency generators for added resilience. From a technical perspective, a fully redundant infrastructure is warranted,

virtually eliminating component outages by implementing dual router, switch, and firewalls, [redacted] AT&T provides out-of-band access to all firewalls, as a means to further enhance system availability.

AT&T is committed to providing a quality MFS service to the Government. This commitment is grounded in how we have developed and deployed the service, equipment, systems, and people to monitor and manage this service.

1.6.2.2.b Approach to Monitoring and Measuring Performance [L.34.1.6.2.b]

(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. [L.34.1.6.2.b]

AT&T monitors the KPIs to assess whether they are within the guidelines of the AQLs from the Security Operations Center using our automated [redacted] AT&T will accurately measure system availability and time to restore and/or repair. AT&T also benchmarks our performance against industrywide standards to continually improve service to our clients. **Table 1.6.2.2-2** provides a description of the approach to monitoring and measuring the KPIs, as listed by the Government.

KEY PERFORMANCE INDICATOR	APPROACH TO MONITORING AND MEASURING
MFS Availability	[redacted]
Event Notification (EN)	[redacted]
Grade of Service (Configuration/Change)	[redacted]

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

Table 1.6.2.2-2: Monitoring and Measuring. *Agencies have the ability to determine service performance with easy access to thorough management reports.*

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.

1.6.2.2.c Approach to Perform Service Delivery Verification [L.34.1.6.2.c]

(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. [L.34.1.6.2.c]

[redacted]

[redacted] **Table 1.6.2.2-3** 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 services performance must be verified; KPIs will be monitored to certify that service performance complies with AQLs.

KPI	VERIFICATION APPROACH	TESTING PROCEDURES
MFS Availability	[redacted]	[redacted]

KPI	VERIFICATION APPROACH	TESTING PROCEDURES
Event Notification (EN)	[redacted]	[redacted]
Grade of Service (Configuration/ Change)	[redacted]	[redacted]
Time To Restore (TTR)	[redacted]	[redacted]

Table 1.6.2.2-3: Service Delivery Verification. *The Key Performance Indicators are closely monitored through a comprehensive verification approach and testing procedure that certifies the service performance achieves or exceeds the Acceptable Quality Levels.*

To simplify the verification process, AT&T has automated the process. [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 MFS services. AT&T follows detailed procedures to verify MFS, by comparing the KPI data against the stated AQLs, as described in the Verification Test Plan.

1.6.2.2.d Performance Level Improvements [L.34.1.6.2.d]

(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. [L.34.1.6.2.d]

Agencies will benefit from enhanced service performance when the KPI performance thresholds are exceeded. **Table 1.6.2.2-4** summarizes the proposed improvements to the key performance indicator (KPI) performance thresholds.

KPI	NETWORX AQL THRESHOLD	AT&T PROPOSED AQL THRESHOLD	IMPROVEMENT PERCENTAGE
[redacted]	[redacted]	[redacted]	[redacted]

Table 1.6.2.2-4: Performance Level Improvements. *Agency end users experience higher service availability and quality through the key performance indicator improvements.*

[redacted]

1.6.2.2.e Approach and Benefits for Additional Performance Metrics [L.34.1.6.2.e]

(e) Describe the benefits of, and measurement approach for any additional performance metrics proposed. [L.34.1.6.2.e]

The KPIs defined by the Government for the MFS service will provide a comprehensive assessment for service verification and service performance monitoring. [redacted]

1.6.2.3 Satisfaction of Security Services Specifications [L.34.1.6.3]

1.6.2.3.a Service Requirements Description [L.34.1.6.3.a]

(a) Provide a technical description of how the service requirements (e.g., capabilities, features, interfaces) are satisfied. [L.34.1.6.3.a]

According to the AT&T/Economist Intelligence Unit Networking and Business Strategy Survey of 2004, the biggest security vulnerability appears to be

people. An astonishing admission was that 78 percent of respondents admitted to having opened an email attachment from an unknown person within the last year. AT&T security and network professionals work together to address issues from this survey and other sources of information to enhance MFS and bring resolution to potential security issues. We understand that a *one-size* fits all solution is not appropriate for our Government customers. Therefore, AT&T offers options between a network-based or premises-based MFS to best meet their security requirements. Federal Agencies can also combine the network-based with premises-based MFS for a multilayer approach.

The various MFS solutions let the Agency define its own security policy, tailor the solution to the size of the user base, and enforce security policies on each interface of the firewall. We use third-party hardware and software solutions from leading vendors, [redacted] AT&T offers various types of implementations, including: appliances, and hardware and software-based routers and/or servers. AT&T assumes the end-to-end monitoring, management, and maintenance of all systems we deploy. Personal (client-based) firewalls are also available for the remote-user or teleworker community. **Table 1.6.2.3-1** lists the various features available with MFS:

SERVICE REQUIREMENTS	DESCRIPTION	BENEFIT TO AGENCY
Network-based MFS	Shared firewall farm inside AT&T data center with logical separation of customer traffic. Network infrastructure provides redundancy, load balancing, and all necessary hardware and software for secured Internet access. See **Figure 1.6.2.3-1**.	• Lower total cost of ownership by reducing number of perimeter firewalls at branch locations • Highly redundant infrastructure in hardened AT&T data center facilities • Simplified, centralized policy management and change control process across enterprise • Centralized monitoring and reporting • Elimination of backhaul from branch offices to customer headquarters for Internet access • Highly scalable with pre-provisioned bandwidth and security components
Premises-based MFS – [redacted]	Dedicated infrastructure placed at customer location. Uses high-performance, reliable security appliance with advanced logic to support complex applications and	[redacted] • Integrated hardware and software package from industry-leader, [redacted], to provide unmatched security reliability and performance

SERVICE REQUIREMENTS	DESCRIPTION	BENEFIT TO AGENCY
	protocols, including IPSec and 3-DES encryption, Adaptive Security Algorithm (ASA), Network Address Translation (NAT), Simple Mail Transfer Protocol (SMTP), HyperText Transfer Protocol (HTTP), Telnet (out), File Transfer Protocol (FTP), Internet Control Message Protocol (ICMP), and Domain Name Service (DNS). See **Figure 1.6.2.3-2**.	[redacted] • Demilitarized zone (DMZ) support allows companies to share public information without jeopardizing proprietary information • Extranet support allows customers to communicate with their suppliers/partners securely and efficiently • VPN support reduces capital investment or expense by reducing amount of hardware involved in creating VPN tunnels
Premises-based MFS – Router-based Firewall	AT&T Managed Internet Service (MIS) optional service, [redacted] Access availability varies from 56K to DS-1 and supports up to 200 concurrent users. Protocol support includes HTTP, SMTP, Telnet, FTP, DNS, H.323, Real Audio, and ICMP. See **Figure 1.6.2.3-2**.	• [redacted] provide all-in-one solutions that perform routing, provide secure Internet connectivity, and apply distinct security characteristics according to a user-defined security policy. • AT&T provides security system components (hardware and software) as well as installation, day-to-day management and maintenance, and most importantly, expert customer support and proactive network monitoring to protect the Agency's network perimeter. • Simpler configuration of dual-homed option (separate segments for Internet and internal network) reduces internal network maintenance requirements. • Even if there is Internet security break[redacted] helps protect customer's internal network, servers, and PCs.
Premises-based MFS-Server-based (SB) Firewall	AT&T MFS-SB provides essential network security functions for AT&T MIS customers who implement Internet with access speeds up to DS-3 for unlimited amount of concurrent users. See **Figure 1.6.2.3-2**.	Fully managed service provides: • Security system components • Installation • Day-to-day management for router, firewall server, and software • Extensive customer support • AT&T will maintain and upgrade firewall hardware and software, freeing customer from expensive technology upgrades
AT&T Personal Firewall Service	AT&T has partnered with [redacted] to build AT&T personal firewall service.	• Unique solution for remote employee workstation and laptop security policy compliance management • Centralized management tools for control of remote endpoint firewalls, anti-virus, and software patches • Provides control over applications operating on remote access endpoints • Full accountability and management through detailed reports
Access	Supports digital subscriber line (DSL), cable, whole and fractional T1s and T3s, OC-3, OC-12, OC-48, extended gigabit Ethernet, asynchronous transfer mode (ATM), and frame relay (FR) access to AT&T's OC48/OC192 backbone and interconnection with AT&T high-speed packet services (HSPS).	Agencies benefit from a wide range of access methods, which provides flexibility to develop custom MFS solutions.
High Availability and Load Balancing	Dynamic load balancing across shared firewalls and failover mechanisms, such as redundant	Supports the ability to design MFS solutions with no single points of failure. MFS designs will be based on an Agency's unique requirements.

SERVICE REQUIREMENTS	DESCRIPTION	BENEFIT TO AGENCY
	configurations, permanent virtual circuit (PVC) redirection, mirroring, backup power, to provide same site and alternate site redundancy.	
Scalability	Small, medium, large, and X-large environments [redacted]	Agencies benefit from the ability to select solutions that are sized appropriately to meet their requirements.
Peak-Bandwidth allocation	Ensures some customers' bandwidth-hungry applications do not consume all network resources. Performs traffic optimization for consistent performance and reduction in server outages and recovery time.	Ability to limit the effect of one end user on the enterprise network.
Identification and Authentication	• Dynamic, per user authentication [redacted]	Various methods by which to identify and authenticate end users.
Static and dynamic Network Address Translation (NAT) support	Static NAT maps local IP addresses to one global address. Dynamic NAT maps local IP addresses to any of a pool of global IP addresses.	Agencies benefit from the ability to mask internal IP addresses and protect the enterprise network.
Support for Domain Name Service (DNS)	AT&T provides IP addresses and resolves DNS naming structures.	Allows the Agency to focus on core Agency objectives.
Email Security	• Stripping Headers • Outbound Domain Header Translation change the internal domain of a user's e-mail address to a standard domain • E-mail Filtering protects a network from being overwhelmed by large attachments. Anti-spamming and virus protection are also available.	Agencies benefit the following ways: • Provides privacy by preventing additional information about the customer's network from going to users outside of the trusted network. • Limits the amount of information available to outsiders. • Limits the size of attachments that are allowed through the firewall.

Filtering	• [redacted]. At a minimum, URL filtering will support:
	  • Advertisements
	  • Illegal or questionable sites
	  • Computer hacking
	  • Online gaming and gambling
	  • Sexually explicit/adult material
	  • Hate promotion
	  • Violence or profanity
	• Java blocking is another form of filtering that stops all Java applets from being passed through the router.
		Agencies benefit from the ability to develop custom filters based on their requirements.

SERVICE REQUIREMENTS	DESCRIPTION	BENEFIT TO AGENCY
VPN/Encryption	Support for remote access, broad-band, and site-to-site tunnel encryption. [redacted]	Agencies benefit from the ability to include remote workers into the Agency's enterprise network, thus promoting teleworker programs.
[redacted]	[redacted]	[redacted]
Extranet and DMZ	Support for dual-homed, triple-homed, and quadrupled-homed (triple-homed with additional extranet segment) configurations.	Supports the ability to segment Agency traffic into multiple zones which promotes service flexibility and allows for the creation of custom security environments.
Protocol Support	Transmission control protocol/Internet protocol (TCP/IP), simple mail transfer protocol (SMTP), domain naming system (DNS), HyperText transfer protocol (HTTP), file transfer protocol (FTP), terminal-remote host protocol program (TELNET), and network news transport protocol (NNTP)	Agencies are at less risk because the service will support multiple protocols and applications.
Denial of Service (DoS) Detection and Prevention	DoS detection and prevention defends router services against common SYN floods and associated TCP attacks.	Agencies benefit from the ability to prevent common DoS attacks.
[redacted]	[redacted]	[redacted]
Audit Trails	Lists source and destination ports, service port, quantity of bytes transmitted and associated timestamps relevant to attack attempts. [redacted]	Provides the ability to track events/threats and see associated steps to mitigate these events/threats. Allows Agencies to monitor MFS activities.

Table 1.6.2.3-1: MFS Security Capabilities. *Agencies will be provided with a fully managed, high-quality service to guard against external security threats entering their network.*

AT&T's Network-based Firewall Service requires no additional equipment be placed on a customer premises. The network-based security devices reside in AT&T Data Centers, which reduces capital expenditures, risk of technological obsolescence, and need for additional technical support staff. AT&T owns all security assets and provides 24x7 monitoring and attack management of the firewall service. AT&T's Network works with the following

transport services: IPS, ATMS, FRS, and VPN services. **Figure 1.6.2.3-1** shows a graphical representation of the Network-based Firewall Service.

Figure 1.6.2.3-1: Graphical Representation of the Network-based Firewall Service. *AT&T's Network-based Firewall provides a fully managed, secure, cost-effective solution that allows Agencies to manage and control employee access to the Internet while preventing unauthorized access to the Agency enterprise network.*

AT&T Premises-based Managed Firewall Service provides a highly functional layer of security to an Agency's network. The service is designed to:

- Defend against unauthorized connection to the Enterprise LAN
- Provide security to end users with remote access requirements via encryption
- Provide a secure environment to Agencies that require unlimited number of concurrent user sessions
- Support remote monitoring and management of the firewall server.

Agencies can choose from four AT&T Premises-based Firewall solutions that best meet their mission requirements. The four options are as follows:

[redacted]

[redacted]

These services let Agencies define their own security policy and tailor the solution to the size of their user base and enforce security policy on each interface of the firewall. **Figure 1.6.2.3-2** shows a graphical representation of the Premises-based Firewall Service.

Figure 1.6.2.3-2: Graphical Representation of the Premises-based Firewall Service. *Premises-based Managed Firewall Service is a fully managed solution, which includes all hardware and software components, configuration, installation, day- to-day management and maintenance, as well as expert customer support and proactive network monitoring.*

True security comes from working with a technology partner that does more than just help overcome pain when an attack is launched. As illustrated in **Table 1.6.2.3-2**, Agencies have several MFS options to choose from. AT&T will work with each Agency to develop custom security architecture and security policies based on the Agency's specific requirements.

1.6.2.3.b Attributes and Values of Service Enhancements [L.34.1.6.3.b]

(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. [L.34.1.6.3.b]

In addition to the standard services, Agencies can enhance their MFS service with additional features and capabilities for an additional fee. **Table 1.6.2.3-2** highlights additional service features and capabilities available with MFS service. AT&T proposes the attributes in **Table 1.6.2.3-2** as service enhancements.

SERVICE ENHANCEMENT	DESCRIPTION	BENEFIT
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 1.6.2.3-2: MFS Service Enharnachements. *Agencies can subscribe to security professional services and other security services, allowing them to concentrate on core Agency objectives by offloading design, project management, and implementation to the MSSP.*

AT&T offers a complete range of low risk, highly available and flexible security services that provide Agencies with integrated business continuity and security solutions to support complex network environments. AT&T helps design, deploy, manage and evolve networks, systems and applications that are safe, reliable and secure against cyber attacks.

1.6.2.3.c Service Delivery Network Modifications [L.34.1.6.3.c]

(c) Describe any modifications to the network required for delivery of the services. Assess the risk implications of these modifications. [L.34.1.6.3.c]

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

1.6.2.3.d Security Services Experience [L.34.1.6.3.d]

(d) Describe the offeror's experience with delivering the mandatory Security Services described in Section C.2 Technical Requirements. [L.34.1.6.3.d]

Among our MFS options, the AT&T's managed PIX firewall suite was AT&T's best seller in 2004, operating in a variety of elements encompassing small, medium, large, and extremely large, complex installations. **Table 1.6.2.3-3** addressed some of our recent MFS deployments across various industries and how they have created value.

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

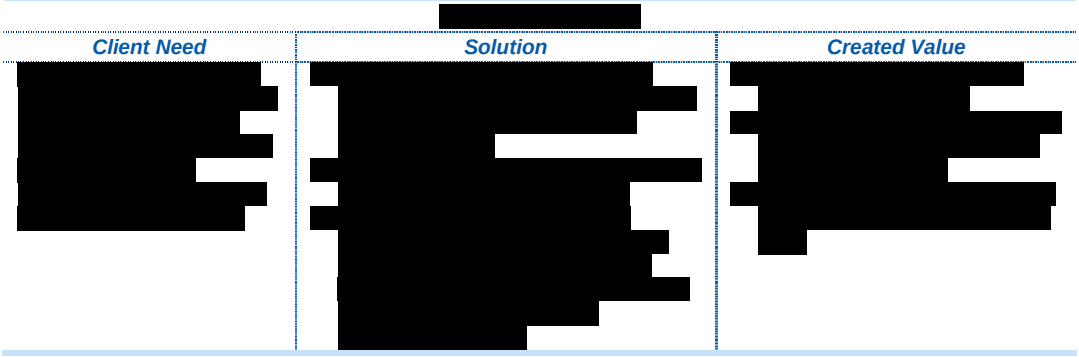

Table 1.6.2.3-3: Experience Delivering MFS Services. *Success is measured by the ability to deliver solutions to Agencies that create value to their business.*

In addition to the Federal market, AT&T supports the following industries with our MFS services: financial, auto manufacturing, pharmaceuticals, shipping and receiving, and many more that require robust and dependable security.

> *"We take care of our network from the inside, and take comfort in the knowledge that we don't have to worry about the external security of our network. AT&T takes care of that."*
>
> United States Olympic Committee.

1.6.2.4 Stipulated Deviations

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

1.6.2.5 EMNS Managed Firewall Service (MFS)

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

1.6.2.5.1 EMNS MFS - Service Description

For Enhanced MFS, AT&T provides a [redacted] firewall that operates [redacted]. The firewall [redacted] enables the integrity of the Agency's services and information; the default setting for all inbound and outbound ports to the Internet is functionally equivalent to "deny". Additionally,

the EMNS firewall service provides secure support for future services such as VoIP and VLAN. As defined in **Figure 1.6.2.5.1-1**, the firewall [redacted] offers [redacted] inspection of [redacted] and application of [redacted] services entering and exiting the Agency's network. Additionally, a Network Address Translation (NAT) scheme will be applied at the firewall. Only authenticated inbound traffic on explicitly approved ports will be allowed to establish connections to the Agency's workstations and servers. It also provides a centralized management solution with centralized user authentication and security event logging that provides the Agency with near real-time access to security event logs and alerts that are stored for 1 year on-line and 5 years off-line.

Figure 1.6.2.5-1: Enhanced Managed Firewall Service. *AT&T [redacted] firewall solution [redacted] all filtering requirements while allowing the addition of future services as well as sufficient capacity for these services.*

The [redacted] inspection by the firewall service module provides the Agency with full bandwidth [redacted] support. The wide variety of in-bound and out-bound filtering features that are offered through the firewall our solution creates a flexible platform for implementing even the most complex security policy. All inbound traffic will be blocked unless that the traffic is explicitly permitted.

Robust support for additional and future services gives an Agency the ability to support Network Address Translation (NAT) and Port Address Translation (PAT) functionality, which provides the innermost boundary for all down stream non-public Web servers and client workstations.

Table1.6.2.5-1 describes the peak port speeds for the Enhanced MNS Managed Firewall Service:

DESCRIPTION
[redacted]

Table 1.6.2.5-1: EMNS [redacted] Managed Firewall Service Peak Port Speeds. *The EMNS [redacted] Managed Firewall Service provides peak ports speeds that range from [redacted]*

1.6.2.5.2 EMNS MFS – EMNS MFS Enhanced SED (ESED) Description

For the EMNS MFS service, the [redacted] Series Firewall will be provided as EMNS MFS ESEDs. The [redacted] Series Firewall Edition

enables Agencies to securely deploy mission-critical applications and networks in a highly reliable manner, while providing significant investment protection and lower operational costs through its unique, modular design. Agencies can protect their networks from unauthorized access using the [redacted] Series Firewall Edition's robust policy enforcement services. These services combine with market-leading VPN services to enable Agencies to securely extend their networks. This flexible solution can adapt as an organization's needs evolve along with the ever-changing security threat landscape, giving Agencies the ability to easily integrate market-leading intrusion prevention, antivirus, antispam, antispyware, URL filtering, and other advanced content security services for additional layers of protection.

One of the following [redacted] Firewalls will be bundled with the EMNS MFS offering:

[redacted]

In addition to providing a [redacted] Firewall at each EMNS MFS location, the following ancillary site services are included with the EMNS MFS ESEDs:

- Equipment and accessories required to install and maintain the EMNS MFS ESEDs at all EMNS MFS sites. This shall include, but is not limited to, racks, cables, tools, etc.
- Space and power requirements - such as physical space, rack space, power, and HVAC - defined for EMNS MFS ESEDs at each EMNS MFS site.
- Operations and management of hardware and software components up to the EMNS MFS 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 MFS 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 MFS ESEDs.

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