1.6.1 Managed Tiered Security Services (MTSS) [C.2.7.4]

The Agency will realize their vision for Managed Tiered Security Services (MTSS) through the deployment of a service that offers flexibility through our ability to support different environments – from small LANs to the largest, most complex network – with differing protection services.

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

1.6.1.1.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, with its deep security expertise, demonstrates the due diligence and discipline that a service provider can take to successfully protect an Agency's network and computing infrastructures. The basic principles adopted by AT&T in managing our corporate enterprise and in securing our networks are leveraged to provide managed tiered security services (MTSS) to Government and commercial enterprises. This experience has led to the following core security principles:

AT&T's expertise was demonstrated by its ability to ward off the Microsoft® Structured Query Language (MS-SQL) worm attack that slowed global Internet traffic to a crawl for millions of users on hundreds of Information Service Provider (ISP) networks in January, 2003.

- **Defense in Depth**: One of AT&T's fundamental security design principles is the strategy of "Defense in Depth" to provide a multi-layered secure environment. "Defense-in-Depth" helps many integrated mechanisms provide multiple levels of protection against attacks. Should one security mechanism be breached, other mechanisms continue to provide protection and prevent or limit the potential damage.
- **Prevention:** AT&T focuses on preventing network attacks by designing security into every AT&T network and service from the start, from

architecture to deployment, using the best available methods and technology. This includes designing our networks with security as a primary concern. AT&T has adopted measures to verify that our network, systems, and services are secure against all known attacks.

- **Security Management:** AT&T is focused on deploying a variety of methods and systems for dealing with the evolving security environment. Areas of interest include software management and system integrity; configuration management, traffic measurement and detection; response and mitigation; and post-event analysis and remediation. As part of this effort, AT&T is moving intelligence into the IP network to eliminate the costly inefficiencies of deploying security solutions at the edge of the network.
- **Innovation Transfer**: AT&T has always treated our enterprise network and infrastructure as a living laboratory where innovations are put into place and rigorously tested for feasibility, scalability, and reliability. AT&T has long had a practice of developing and implementing security innovations on our enterprise network first and then extending those technologies to our networks and services provided to customers. A number of innovations discussed throughout this proposal were developed in this fashion.

Each of these security-guiding principles is used in developing our MTSS. MTSS offers four tiers of service to meet the requirements described in the Networx RFP. **Figure 1.6.1.1-1** illustrates our four-tier protection service delivery approach.

Figure 1.6.1.1-1: Multi-Layer Protection. *Agencies receive multiple layers of protection to enable tiered security levels to be attained for defense in depth across their enterprise.*

These service tiers define the level of protection at each layer. The tools and processes used for each tier are the same where applicable (help desk, anti-virus, firewall, Intrusion Detection Service (IDS), Incident Response, packet filtering, Premises-Based IP Virtual Private Network (PBIPVPN), Secure Managed Email, Certification and Accreditation (C&A), and Vulnerability Scanning to offer service consistency across each of the tiers . The primary difference in delivering tier 3 and 4 MTSS is the need to deploy a private security operations center.

Each service tier will be delivered using standard methods, procedures, tools, and a suite of systems. **Table 1.6.1.1-1** summarizes the MTSS service delivery approach.

SERVICE DELIVERY APPROACH	DESCRIPTION
Standards compliance	We will support Federal standards and publications as applicable for MTSS to include NIST, NSA, NIACAP, DITSCAP, and FISMA.
Custom tailored solutions for Tier 1, 2, 3, and 4	AT&T will deliver the technical capabilities and features required through either a shared security operations center (Tier 1 and 2) or a customer private operations center (Tier 3 and 4) using the same AT&T develop systems and platforms.
Standard IDS, Firewall, Antivirus, VSS, VPN, and Incident Response platforms	For all four tiers AT&T will offer the same platforms and services for all four tiers as described in section 1.6 of our proposal.
24 x 7 Help Desk	AT&T will offer a 24 x 7 help desk that delivers the technical expertise for Agencies to discuss security issues for all tiers.
Private license security systems	For tier 3 and 4 AT&T will license [redacted] platforms that will provide the system capabilities to manage the security infrastructure. • [redacted] – Is an AT&T Labs develop toolset that will enable the collection of [redacted] and [redacted] it for security issues . Section 1.6 and 1.6.6 provides a more detailed discussion of Aurora capabilities. • [redacted] – Is an AT&T Labs develop toolset that will enable the management of [redacted]
Professional security specialists	AT&T will deliver Certification and Accreditation support using our experience security practice where personnel not only possess certification, such as CISSP, but also have Government security clearances.
Defense Information Infrastructure (DII) / Defense Messaging Service (DMS) Guard	This high assurance multi-level solution is the only available NSA approved mechanism that provides the exchange of electronic mail (e-mail) between a High Assurance Tier-3 network and a Protected Tier-2 enclave. This device will be used to deliver mail exchange between tier 3 and 2 security levels.
Onsite installation and management	AT&T will provide security service implementation and management through our team of security experts and security operations center that may be shared for tier 1 and 2 but private for tier 3 and 4 security levels.
Established processes for security maintenance	AT&T offers established methods and procedures that will be used in our shared NOC for tier 1 and 2 and private agency NOC for tier 3 and 4.

Table 1.6.1.1-1: MTSS Service Approach. *Agencies will receive MTSS that provides a full set of features to meet their security needs with experienced security professionals, proven tools and systems, and commercial platforms.*

Our Defense-in-Depth strategy will help Agencies realize the appropriate level of protection for their data. MTSS provides a critical role in a defense-in-depth strategy. MTSS allows for an Agency to gain the level of security needed on an Automated Information System (AIS), pursuant to the level of security required to secure those resources.

1.6.1.1.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 MTSS 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 1.6.1.1-2** describes each service in relation to FEA, summarizes its contribution, and/or provides an example of how it facilitates FEA implementation.

TECHNICAL APPROACH	BENEFITS	FEDERAL ENTERPRISE ARCHITECTURE OBJECTIVE
Standards compliance	Provides consistency in security service levels. This consistency enables quality service delivery across tiers.	Supports the Federal Enterprise Architecture's (FEA's) SPP for agencies to incorporate security and privacy requirements and services into their EA development lifecycle. In particular: • Service Access and Delivery *Service Transport* – Supports network services • Component Framework *Security* - Supports security services
Custom tailored solutions for Tier 1, 2, 3, and 4	This approach offers the same features and capabilities as our commercial offerings without investment in developing systems saving the Government budget.	
Standard IDS, Firewall, Antivirus, VSS, VPN, and Incident Response Platforms	Allows an Agency to use commercial proven security technology within a multi-tier environment.	
Private license security systems	Allows for the use of similar platforms that are in commercial use with AT&T customer's to be licensed to Government Agencies to provide tier 3 and 4 security levels saving the Government budget.	
Professional security specialists	Using a proven security consulting practice offers the Government personnel that will be able to deliver on our commitments.	
Defense Information Infrastructure (DII) / Defense Messaging Service (DMS) Guard	Offering NSA-approved solutions provides the Government the confidence that solutions will provide the appropriate security protection.	
Established processes for security maintenance	Proven methods and procedures reduce cycle time and service costs.	

Table 1.6.1.1-2: Agency Enterprise Architecture Benefits Using Our MTSS. *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 verifies 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 MTSS offering.

1.6.1.1.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, such as AT&T, which brings the depth and background that 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 MTSS projects.

Table 1.6.1.1-3 lists the top seven service delivery risks and our mitigation strategy. [redacted]

RISKS	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]
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	[redacted]

RISKS	RISK DESCRIPTION	RISK MITIGATION
	and competitor in how they are handled.	[redacted]
False positives	Sensors are prone to generating false positives	[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]

Table 1.6.1.1-3: AT&T Service Delivery Lessons Learned and Risk Mitigation Strategies . *Agencies benefit from lessons learned and experience implementing MTSS services, which ultimately minimize service delivery risks.*

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

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

1.6.1.2.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 will meet the performance levels and acceptable quality level (AQL) of key performance indicators (KPIs) for MTSS for routine and critical users as presented in the RFP and in the below **Table 1.6.1.2-1**.

KEY PERFORMANCE INDICATOR (KPI)		SERVICE LEVEL	PERFORMANCE STANDARD (THRESHOLD)	ACCEPTABLE QUALITY LEVEL (AQL)	AT&T AQL
Grade of Service (Configuration/Rule Change		Routine	Within 5 hours for a normal priority change	[redacted]	[redacted]
			Within 2 hours for an urgent priority change	[redacted]	[redacted]
Event Notification		Routine	Within 2 hours of a low category event	[redacted]	[redacted]
			Within 5 minutes of a high category event	[redacted]	[redacted]
Av (Firewall)		Routine	99.5% of the time	[redacted]	[redacted]
Help Desk	EN (Outage Notification to Customer)	Routine	Within 2 hours of a low category event	[redacted]	[redacted]
			Within 5 minutes of a high category event	[redacted]	[redacted]
	GoS (Percentage of Calls Abandoned)	Routine	3%	[redacted]	[redacted]
	Response Time	Routine	All incoming calls to the Help Desk will be answered on or before the fifth ring.	[redacted]	[redacted]
Av (Multilevel Security Solutions) NSA Approved		Routine	100% of the time	[redacted]	[redacted]
Av (Type 1 Encryption)		Routine	100% of the time	[redacted]	[redacted]
Av (Web Portal)		Routine	99.7% of the time	[redacted]	[redacted]
EN (Security Incident Reporting		Routine	Near real time	[redacted]	[redacted]

Table 1.6.1.2-1: Performance Standards. *Agencies will access the highest quality MTSS offered that sets the industry quality standards for performance.*

Focusing on an Agency's service experience produces a high-quality solution, and service experience must be measured quantitatively through the KPIs. [redacted] Agencies will receive high-quality service through the combination of the five network and service attributes that ultimately directly affect the quality delivered to the end user: scale, administration, high availability, notification, and quick-service restoration.

1.6.1.2.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.

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. **Table 1.6.1.2-2** outlines the methods used to measure the various IP key performance indicators.

Key Performance Indicator		Approach for Measuring
Grade of Service (Configuration/ Rule Change		[redacted]
Event notification		[redacted]
Av (firewall)		[redacted]
Help Desk	EN (Outage Notification to Customer)	[redacted]
	GOS (Percentage of Calls Abandoned)	[redacted]
	Response Time	[redacted]

KEY PERFORMANCE INDICATOR	APPROACH FOR MEASURING
Av (Multilevel Security Solutions) NSA Approved	[redacted]
Av (Type 1 Encryption)	[redacted]
Av (Web Portal)	[redacted]
EN (Security Incident Reporting	[redacted]

Table 1.6.1.2-2: Monitoring and Measuring MTSS. *Agencies can easily manage the MTSS service with easy to access and use data delivered through the AT&T* ***Business****Direct® web portal and other systems and tools.*

1.6.1.2.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; Key Performance Indicators (KPIs) will be monitored to certify that the service performance complies with the AQL. **Table 1.6.1.2-3** summarizes the verification and testing procedures for the MTSS KPIs. The verification will be a general service verification that demonstrates our ability to meet these KPIs rather than an Agency specific verification since the service will have just been installed.

KEY PERFORMANCE INDICATOR		TESTING PROCEDURES
Grade of Service (Configuration/Rule Change		[redacted]
Event notification		[redacted]
Av (firewall)		[redacted]
Help Desk	[redacted]	[redacted]
	[redacted]	[redacted]
	[redacted]	[redacted]
Av (Multilevel Security Solutions) NSA Approved		[redacted]

KEY PERFORMANCE INDICATOR	TESTING PROCEDURES
	[redacted]
Av (Type 1 Encryption)	[redacted]
Av (Web Portal)	[redacted]
EN (Security Incident Reporting	[redacted]

Table 1.6.1.2-3: Service Delivery Verification. *The Key Performance Indicators are verified through a comprehensive verification approach and testing procedure that certifies the service performance achieves or exceeds the Acceptable Quality Levels.*

The common testing platform provides an integrated system to perform service verification testing and present the results either on AT&T **Business**Direct or by written report. The service verification process is presented in greater detail in Section 1.3.2.d, Approach to Perform Service Delivery Verification.

1.6.1.2.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 KPIs will result superior MTSS service performance. [redacted]

1.6.1.2.e Approach and Benefits for Additional Performance Metrics

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

[redacted]

1.6.1.3 Satisfaction of Security Services Specifications [L.34.1.6.3]

1.6.1.3.a Service Requirements Description

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

1.6.1.3.a.1 Agency Sponsored Type 1 Encryption (Tiers III & IV)

AT&T has extensive experience working with classified networks at the Secret, Top Secret, and SCI classification levels. With this experience, AT&T has provided Government customers, with classified requirements, proven expertise in the design, implementation and management of secure communication networks. AT&T will provide management, installation, operations, maintenance and upgrade services for NSA-approved Type I encryption devices using the approved and supported processes and methodologies supported by NSA.

AT&T will provide the capability of remotely managing NSA Type I approved encryption devices from a central location. Using the [redacted] AT&T will manage [redacted] through Agency sponsorship. Depending on the configuration of the secure network environment a specific GEM platform will be used. AT&T will use the GEM platform to perform the following functions:

[redacted]

[redacted]

As part of the secured service, AT&T will conduct [redacted] will occur at predefined time intervals and whenever [redacted] occurs as dictated by the approved security practice. [redacted] will occur at predefined time intervals and whenever [redacted] occurs as dictated by the approved security practice. With the features provided using the GEM Encryptor Management solution and managing [redacted] from a central location, AT&T will be able to maintain device synchronization and limit the end-to end latency to maximize the security and throughput of sensitive data.

AT&T will provide the required Key Management Services in accordance with the Agency Key Management Plan, the COMSEC Supplement to the National Industrial Security Program Operating Manual (NISPOM), the National Security Telecommunications and Information Systems Security Instructions (NTISSIs), National COMSEC instructions and all applicable NSA and department policies. AT&T's COMSEC Custodian personnel will be qualified and trained by the NSA COMSEC. AT&T currently manages many encryption devices for multiple government sponsors in accordance with these policies, both on-site and within an AT&T [redacted] in the [redacted]

1.6.1.3.a.2 Anti-virus(Tiers II→IV)

These MTSS capabilities are all covered under the antivirus portion of the response for Tier II and can be replicated to an on-site configuration and management for Tiers III and IV with modifications for the security requirements of each individual Tier. (For more details on MTSS, refer to Section 1.6.5, Anti-Virus Management Service.

1.6.1.3.a.3 Firewalls (Tiers II→IV), Packet Filtering (Tiers II→IV), and Proxy Server (Tiers II & III)

These MTSS capabilities are all covered in more detail in Section1.6.2, Managed Firewall Services) portion of the response for Tier II. They can be replicated to an on-site configuration and management for Tiers III and IV with modifications for the security requirements of each individual Tier.

1.6.1.3.a.4 Agency Dedicated Help Desk (Tiers I→IV)

Help desk will be provided by a 7x24 tier 1 security staff that is capable of assisting Agencies with their security requirements.

1.6.1.3.a.5 Intrusion Detection/Prevention (Tiers II→IV)

AT&T will manage both premised based HIDs and network based NIDs for Tier II as specified in the IDPS response and provide the same facilities to Tier III and Tier IV when the appliances and management have to be located on site. For more detail, refer to Section 1.6.3, Intrusion Detection and Prevention Service.

1.6.1.3.a.6 Incident Response (Tiers II→IV)

AT&T will support all the security monitoring and reporting requirements for Tiers II to IV by using the AT&T Aurora platform both in an onsite requirement (Tiers III & IV) and as a service for Tier II. (For more detail. Refer to Section 1.6.6, Incident Response Service).

1.6.1.3.a.7 Network Isolation (Air Gap)(Tier IV)

AT&T will use physically separate network devices for Tier IV network enclaves to prevent connectivity to a network of a lesser security level.

1.6.1.3.a.8 NSA Approved Multi-level Security Solution (Tier III→IV)

AT&T will provide the technology to implement security mechanisms that allow the exchange of data residing on networks of different classification levels. Safeguards and countermeasures will be taken to verify that data is traversing connections between Secret and below networks and to adhere to the strictest security standards and procedures.

Using NSA-approved mechanisms, AT&T will provide the [redacted] This high assurance multilevel solution is the only available NSA-approved mechanism that provides the exchange of electronic mail (e-mail) between a High Assurance Tier-3 network and a Protected Tier-2 enclave.

The [redacted] provides specific filters [redacted] in accordance with the security policies of the Tier-3 enclave . The [redacted] supports Standard Mail Transport Protocol (SMTP), X.400 messaging and X.500 directory protocols (as required by DMS).

The [redacted] is the system component used to support the [redacted] requirement to support the exchange of electronic messages between security enclaves. Developed under the National Security Agency's Multilevel Information Systems Security Initiative (MISSI), the [redacted] verifies compliance with the Joint Staff's Secret and Below Interoperability (SABI) approach for messaging.

The [redacted] comprises four primary components: [redacted]

[redacted]

The [redacted] allows users to send and receive electronic mail messages. The data sensitivities expected to be processed by the [redacted] up to the Secret level. The [redacted] will allow the bi-directional flow of unclassified X.400 and SMTP messages. By policy, the X.500 directory shadowing is allowed to flow only from low to high.

[redacted].

As an adjunct to the [redacted] AT&T will use [redacted]. An organization can easily transfer large quantities of any type of data allowed by the site's security policy, including imagery, maps, documents, email and even databases. The data can be in any format, variable or fixed. It can be from any operating system such as UNIX® or Microsoft Windows.®

It supplements features that are integral to the [redacted] highly [redacted] operating environment, which include role-based administration (RBAC), mandatory access controls (MAC), use of least privilege and removal of the super-user root account. In addition to these features, [redacted] provides other security safeguards, including embedded virus scanning and advanced kernel-level Internet Protocol (IP) packet filtering.

The system implements a heterogeneous virus scanner that simultaneously scans for UNIX, Amiga®, Macintosh®, Windows 95/NT® and MS-DOS®

viruses that perform denial of service and back door attacks, plus hostile Java applications and applets and OLE/VB5 macro viruses. [redacted] automatically transfers to a pre-designated high-side server any files determined to be free of viruses. The system scans files for viruses as each file is transferred from one level to the other. [redacted] automatically deletes any virus-laden file, whether it is embedded in an executable file or as a macro in a Microsoft Office® product.

[redacted] is the first commercial product selected by the NSA for product assessment. Along with the NSA assessment, operational systems worldwide—which include [redacted]—have received approval from the Defense Intelligence Agency (DIA) and the Secret and Below Interoperability (SABI)/Defense Information Security Network (DISN) Security Accreditation Working Group (DSAWG). It has been granted SABI Reference Implementation (SRI) status. [redacted] has undergone the DoD Information Technology Security Certification and Accreditation Process (DITSCAP), the standard process for security certification and accreditation of DoD IT Systems, as well as Director of Central Intelligence Directive (DCID) 6/3, the managing directive for computer security for the Federal Intelligence Community.

1.6.1.3.a.9 Premises-based VPN (Tiers II→IV)

AT&T will provide AT&T s eVPN service for premise based VPN devices. The security of this service will be monitored by the Incident Response team using the [redacted] platform, either at an AT&T site or onsite for the tiers of higher security level . Refer to section 1.4.12 , Preside Based IP for a more detailed discussion of that service's security features.

1.6.1.3.a.10 Secure Managed Email (Tiers II→IV)

AT&T will provide MTSS with a fully compliant secured email service that can functionally be migrated to service Tier II and Tier IV requirements. (For more detail on MTSS, refer to Section 1.6.8, Secure Managed Email Service.)

1.6.1.3.a.11 Security Certification Support (Tiers II→IV)

AT&T will provide full support for the C&A process across all the tiers with a staff of information assurance professionals that are fully familiar with all the federal regulations, guidelines, and certification processes required for all tiers.

1.6.1.3.a.12 Security Maintenance (TIERS II→IV)

All the security maintenance requirements for MTSS are met under one or more of the services and/or capabilities provided in this RFP response. **Table 1.6.1.3-1** is a matrix which maps each requirement to the corresponding component of MTSS which meets it.

		MFS	VSS	AVMS	MEAS	SMEM	C&A	INRS	HELP DESK NOC
a	[redacted]	✓	✓	✓					
b	[redacted]	✓		✓		✓		✓	
c	[redacted]	✓				✓			✓
d	[redacted]	✓		✓	✓	✓			✓
e	[redacted]			✓					
f	[redacted]								✓
g	[redacted]		✓					✓	
h	[redacted]	✓	✓	✓		✓		✓	
l	[redacted]	✓		✓	X	✓		✓	✓
j	[redacted]							✓	
k	[redacted]							✓	

Table 1.6.1.3-1: Requirement to the Corresponding MTSS Component. *All Agency security maintenance requirements for MTSS are met.*

1.6.1.3.a.13 Vulnerability Scanning (Tiers II→IV)

AT&T utilizes the industry-leading [redacted] scanning tool as the cornerstone of its Tier II service and will deploy the same capabilities and equipment on-site for Tier II and IV solutions. (For more detail on MTSS, refer to Section 1.6.4, Vulnerability Scanning Service.)

1.6.1.3.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 established requirements are sufficient to provide a service that will proactively protect the Agency's valued assets by determining if vulnerabilities exist in their infrastructure.

1.6.1.3.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 MTSS upon contract award without modifications to the network or operational support systems.

1.6.1.3.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 Networx Team offers Agencies extensive experience providing MTSS that create value to our customers both in Government and commercial entities. This experience has given us the ability to engineer and deliver services. Two examples of AT&T Team's ability to deliver MTSS are listed in **Table 1.6.1.3-2**.

[redacted]

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

Table 1.6.1.3-2: Experience Delivering MTSS. *Success is measured by the ability to deliver solutions to Agencies that create value to their business.*

1.6.1.3.e Approach to Network Infrastructure Security

(e) For Managed Tiered Security Services (MTSS), describe the approach, process, and considerations for securing a network infrastructure. Based on the offeror's experience with the Tier 2 requirements specified in Section C.2.7.4, provide a discussion of how the offeror would investigate the requirements, design the solution, implement the plan, and deliver service that meets the Agency's performance requirements.

The approach taken in delivering Agency specific network infrastructure security draws on the Team's systems engineering and design experience. As part of the delivery process, the AT&T Team follows our standard process for design and engineering security solutions developed using best practices, sophisticated tools, and rigorous methodologies. These are applied from the initial receipt of a customer statement of work (SOW) to customer acceptance and final delivery . Our approach uses a phased approach that consists of (1) planning, (2) requirements, policy, and process preparation, (3) designing domain separation, (4) hardening infrastructure elements (5) layer 3 architecture, (6) implementation, and (7) certification and accreditation.

1.6.1.3.e.1 Security Planning

During the planning phase, a project manager is assigned to effectively manage requirements gathering and design tasks and sustain progress into baseline operations. The Project Manager directs activities, monitors progress, and manages risks to produce a quality deliverable to the Government. During this planning activity, AT&T performs the following functions: (1) identifies our team, (2) assigns roles and responsibilities, (3) establishes our project schedule, (4) defines our communications plan, (5) works with the Government to identify the locations to interconnect, and (6) establishes a monthly or weekly status meeting. The following are key work products that are developed during the project-planning phase of MTSS:

- Change control processes
- Change control register
- Meeting agenda
- Project schedule
- Project budget
- Agency governance model

- Meeting minutes
- Risk review gates.

1.6.1.3.e.2 Security Requirements, Policy, and Processes

Security begins with the development of the Agency's security requirements and policy that adhere to applicable security standards and practices . This family of policies and practices governs security in all services areas in everything from operating systems to facilities. Building on this foundation, security processes and policies will provide the framework, security is embedded in every step of deployment, network architecture, reviews, testing, monitoring, management, maintenance, and incident response . The requirements analysis addresses the items listed below:

- Schedule and costs constraints
- Standards and Agency security guidelines
- Security risks and vulnerabilities
- Network applications
- Network Topology
- Equipment and configurations
- Logical interconnection
- Physical security
- Authentication, access, and accounting
- Privacy
- Certification and accreditation
- Network operational models
- Continuity of operations.

The following methods are used to collect the security requirements, policies, and processes: (1) review of existing documentation, (2) user surveys, and/or (3) site surveys. The result of this activity will be a requirement, policy, and process documents customized for the Agency.

1.6.1.3.e.3 Domain Separation

Once all the requirements are documented the IT infrastructure is analyzed to identify domains . AT&T uses the principle of domain separation both for its internal networks and for managing customers' networks.

Domain separation verifies that communications between domains are allowed only as authorized, going through designated gateways, which can detect suspicious activity and block it, if necessary. If one domain is compromised in a security incident, domain separation protects the other domains from compromise and contains the incident, limiting the damage.

While networks and the Internet are generally perceived as enhancing connectivity and openness, in practice there is a real business need for controlling access to critical Government or enterprise applications such as human resources (HR) or payroll systems. Different systems and networks require different security characteristics, access needs, and user screening. An entity that comprises one or more systems and one or more networks, all with a common function, constitutes a domain.

Each domain will have a set of rules for communication within the domain and another set for communication outside the domain. This separation is achieved by using the principles of domain separation for systems and networks within the Agency.

The result is a security architecture that defines the domains, the appropriate separation, policies, and separation controls mechanisms (i.e. MFS, IDPS, and AVMS) between each of the domains.

1.6.1.3.e.4 Hardening Infrastructure Elements

Network infrastructure security consists of both host-based and network-based security. The foundation of infrastructure security is a secure network equipment or server . All servers and network equipment are hardened per vendor, industry, and internal recommendations. Host-based agents continuously monitor the servers looking for unauthorized changes in software and configurations . In addition to hardening the network elements, AT&T will deploy a number of measures to protect against distributed denial of service (DDoS) attacks at the host and element level, at the network level, and at the service (application) level. These mechanisms consist of premises or network based firewalls and intrusion detection. One significant AT&T security innovation, AT&T Internet Protect, monitors IP traffic for new attacks caused by worms and viruses. All of these systems will be in place and are monitored 24x7 by senior security personnel.

1.6.1.3.e.5 Layer 3 Security

At the network edge, AT&T has established a rigorous set of security techniques and practices . AT&T has implemented IETF RFC 2547bis to assure the isolation and separation of VPNs . AT&T will design and implement the following measures to protect the shared infrastructure:

- Authentication
  - User Access – Provided through managed electronic authentication service (MEAS) for access to servers, VPN, or other domains.
  - Router Access – TACACS+ centralizes administration of users that have access to network elements. Thus, AT&T does not have to separately administer the users on each element. The TACACS+ security mechanism allows a separate access server (the TACACS+ server) to provide the services of authentication, authorization, and accounting independently. Each service can be tied into its own database or can use the other services available on that server or on the network.
  - Routing Protocol – BGP MD5 authentication is implemented on all access links. MD5 authentication on BGP routing verifies that route announcements for a given network (autonomous system) are being received from that network. MD5 prevents BGP resets from being received by an unauthorized source, thus helping to maintain network stability.

- Routing Controls
    - Route filtering - Route filters will be implemented on the routers in accordance with the Agency requirements.
    - Least Privilege – Infrastructure routers and Provider Edge (PE) interfaces are hardened by turning-off, or severely restricting, unnecessary protocols and ports.
    - Limits – Route dampening is used to limit the rate or total number of route-update transactions performed by a router
- Router, Firewall, IDS, and AVMS
    - Sizing – Equipment will be sized based upon numbers of policies, addresses, throughput requirements, and interfaces
    - Configuration – Equipment will be configured based upon software features, protocols, IP addresses, and availability and redundancy requirements.

1.6.1.3.e.6 Implementation

Agency security solutions are installed as detailed in the detailed architecture and design document. All equipment and services are installed using the engineering as-built drawings developed after the site survey. The onsite technician mounts the equipment, fastens the network and power cables, and powers the equipment. After verifying that the equipment functions properly, the technician contacts the program manager who coordinates with the network operations center for site testing, verification, and acceptance.

Based on site surveys and finalized site specifications, AT&T refines its acceptance test plan. After the installation, our team executes acceptance testing. Upon successful testing and acceptance, the security solution is turned over to AT&T's lifecycle team for ongoing management.

1.6.1.3.e.7 Security Certification and Accreditation

AT&T network security systems continually probe our networks, both internally and externally. We deploy an Ethical Hacking Team (or “Tiger Team”) that probes for security vulnerabilities, using the same techniques as a potential intruder. The team compiles and analyzes the test results, reports their findings to the organization that requested testing, and recommends measures to close the vulnerabilities that testing uncovered. In addition, on both our intranet and on the Internet, AT&T employs deception technology (in the form of “honey pots” that use AT&T-patented technologies) to look for potential subversive activity.

The AT&T Network Security Evaluation Program (SEP) evaluates the security of both existing environments and for new features that are to be delivered within AT&T. This verifies that security is embedded into the lifecycle process for all AT&T services. SEP and client organizations jointly develop a Custom Security Plan specific to the client’s environment as part of CSDES.

1.6.1.4 Narrative Requirements

Narrative Requirements not required in accordance with RFP Section C.2.7.4.3.1, C.2.7.4.3.2, and J.1.1.3(a).

1.6.1.5 Stipulated Deviations

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