1.3.3.d Approach to Incorporate Emerging Technology [L.34.1.3.3.d]

(d) Describe the approach for incorporating into the offeror's network, infrastructure enhancements and emerging services that the offeror believes are likely to become commercially available in the timeframe covered by this acquisition, including a discussion of potential problems and solutions. [L.34.1.3.3.d]

[redacted]

To support this transformation, the AT&T network will require key infrastructure enhancements, and new services and capabilities during the Networx acquisition timeframe. This network transformation must be completed without service-impacting risks and without jeopardizing network reliability and functionality.

1.3.3.d.1 Approach for Enhancing the Network Infrastructure

[redacted]

[redacted]

When emerging technologies mature and become the new core, older technology interfaces are migrated to the edge for continued product support.

[redacted]

[redacted] **Figure 1.3.3.d-1** shows the flow of emerging technologies.

Figure 1.3.3.d-1: [redacted] **for** [redacted] **and** [redacted]

[redacted]

[redacted]. Table 1.3.3.d-1 [redacted].

APPROACH FOR ENHANCING THE NETWORK INFRASTRUCTURE

Approach	Description
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 1.3.3.d-1: Key Network Enhancements and Emerging Services. [redacted]

[redacted]

1.3.3.d.2 Approach for Enhancing the Operational Support Systems

The operational support systems (OSS) infrastructure must be modified to accommodate emerging capabilities too. As with the network infrastructure, the introduction of emerging technology should not impact the capabilities of the existing network operations systems. The

Changes to the OSS are limited to the EMS and provisioning system.

Network Operations team must continue to operate, administer, monitor, manage, and provision the network during the deployment of emerging technology or services. [redacted] **Figure 1.3.3.d-2** [redacted]

Figure 1.3.3.d-2: Approach for Operations System Enhancements. [redacted]

Table 1.3.3.d-2 summarizes AT&T's approach for incorporating enhancements to the OSS that are required to introduce emerging technology to the network.

APPROACH FOR OPERATIONS SYSTEMS ENHANCEMENTS	
Approach	***Description***
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 1.3.3.d-2: OSS Enhancements for Emerging Technology. [redacted]

[redacted]

1.3.3.d.3 Approach for Enhancing the Security System

Introducing emerging technology into the network creates the potential for security threats. These potential security threats must be identified, quantified, and mitigated prior to technology introduction. Otherwise, the service provider puts at risk the service quality and performance of the new technology and, potentially, the rest of the network.

Emerging technology insertion creates a security threat to the network.

To prevent an emerging technology or service from impacting the security of the existing network infrastructure, AT&T follows a rigorous process prior to network introductions. **Table 1.3.3.d-3** summarizes AT&T approach for securing emerging technology.

APPROACH FOR NETWORK SECURITY ENHANCEMENTS

Approach	Description
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 1.3.3.d-3: Approach for Network Security Enhancements. [redacted].

1.3.3.d.3.1 Two-Stage Security Introduction Process

Emerging technology requires the development of new security capabilities that are introduced in conjunction with the emerging technology. The new security technology is not integrated into the existing security platform. As the emerging technology is integrated into the core network, the associated security package is integrated into the network security infrastructure as described in **Figure 1.3.3.d-3**.

Figure 1.3.3.d-3: Approach for Security System Enhancements. [redacted]

1.3.3.d.4 Infrastructure Enhancements and Emerging Technologies

Emerging technologies anticipated during the Networx Contract time frame.

Many new technologies and services have emerged during the FTS 2001 contract timeframe such as VoIP and WiFi. AT&T anticipates many technologies will also emerge during the Networx contract timeframe. AT&T recognizes the importance of embracing emerging technologies to remain competitive from a service and cost perspective. **Table 1.3.3.d-4** summarizes the infrastructure enhancements and emerging technologies anticipated to impact AT&T's network during the Networx contract timeframe.

INFRASTRUCTURE ENHANCEMENTS AND EMERGING TECHNOLOGIES

Emerging Technologies	*Description*
[redacted]	[redacted]

INFRASTRUCTURE ENHANCEMENTS AND EMERGING TECHNOLOGIES

[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 1.3.3.d-4: Key Network Enhancements and Emerging Services. [redacted]

1.3.3.d.5 Problems and Solutions with Emerging Technologies

Emerging technology and services must be introduced into the network carefully to mitigate potential problems. Stability, reliability, and security of the emerging technology and of the existing network must be evaluated prior to introduction, and potential issues must be identified and resolved. The benefits of emerging technology can only be realized when it operates safely and securely as planned. To facilitate this result, AT&T has identified the following general problems and solutions, as summarized **Table 1.3.3.d-5**.

Emerging technologies

EMERGING TECHNOLOGIES PROBLEMS AND SOLUTIONS

Issue	*Description and Solution*
Emerging technology is not always reliable and stable	[redacted]

EMERGING TECHNOLOGIES PROBLEMS AND SOLUTIONS	
	[redacted]
Emerging technology is a security risk to the Network	[redacted]
Emerging technology must be operational	[redacted]

Table 1.3.3.d-5: Problems and Solutions with Introducing Emerging Technologies. [redacted]

1.3.3.d.5.1 AT&T One Process Phase Gate Approach

To minimize the risks and maximize the value of emerging technology, AT&T follows a rigorous technology/service introduction process called the One Process Phase Gate Approach. [redacted] (**Figure 1.3.3.d-4** and **Table 1.3.3.d-6**).

Figure 1.3.3.d-4: AT&T One Process [redacted]

The culmination of the Approach is the introduction of emerging technology to the network. The introduction is closely monitored to minimize risk to the other services.

[redacted]

Phase	Description
Concept Phase	[redacted]
Feasibility Phase	[redacted]
Design Phase	[redacted]
Development Phase	[redacted]
Service Testing Phase	[redacted]
Introduction Phase	[redacted]

Table 1.3.3.d-6: [redacted] Approach. *This comprehensive and phased approach for securing emerging technology reduces associated risks.*

In summary, the risks associated with emerging technology are reduced by AT&T's strategic approach. [redacted]

1.3.3.e Approach to Ensure Converged Service Quality [L.34.1.3.3.e]

(e) Describe the approach for network convergence. In particular, describe how the approach ensures service quality over the converged network for data, voice, video, and multimedia. [L.34.1.3.3.e]

The AT&T has a two-fold strategy for network convergence: building a service oriented architecture and handing and routing of application-specific packets in the network.

1.3.3.e.1 Standardized Service Delivery Platform

An emerging technology that AT&T envisions will be developed is the SoIP service delivery platform (SDP). The SDP acts as a common framework to perform functions required to create, register, provision, and manage new IP-based services that are required by the Agencies. The SDP comprises the OSS system for service ordering and provisioning, the Services over IP Layer (SoIP) for service creation, and the Application Aware Networking (AAN) layer for network resource allocation. **Figure 1.3.3.e-1** presents the SoIP SDP architecture that includes the VoIP products that AT&T offers today.

Figure 1.3.3.e-1: SoIP Service Integration in SDP. *New services become available in the IP network when Application Aware networking service creation layers are added to the OAM&P network and modular service elements placed in the IP network.*

The AT&T SDP provides a plug-and-play environment so that emerging IP-based applications services do not require a separate, unique development process. Among the reusable application elements are software logic, modules, processes, and server technology. The AT&T SDP provides fast, flexible mechanisms to create new services that integrate with the underlying network and drastically shorten the service development cycle.

The AT&T SDP is implemented as a SOA. The interfaces between the SDP components (OSS, SoIP and AAN) are standard web services interfaces. The SOA enables SoIP applications to be written using standard web services protocols such as XML and Simple Object Access Protocol (SOAP) and to be loosely coupled to each other as needed.

1.3.3.e.1.2 Standardized Network Application Infrastructure

AAN provides a network-based computing infrastructure to run SoIP applications servers and other web application servers. AAN's objective is to link customer application requirements with the optimized networking, processing, storage, and security resources. This standardized computing environment allows AT&T to provide a common resource layer that will be shared by different IP-based applications, accelerate service introduction, and reduce service costs and risks. **Figure 1.3.3.e-2** shows the basic operation of the AAN architecture.

Figure 1.3.3.e-2: AAN Packet-based Routing. *By acting at the edge of the MPLS network, special edge devices read the contents of packets from specific applications or network functions and modify the IP routing to include servers in the path that augment the service.*

1.3.3.e.2 Standardized Service over IP Infrastructure (SoIP)

Given the explosive federal and commercial customer's demands for IP-based service (voice, video, multimedia and others) and applications, AT&T is developing a common SoIP infrastructure. **Figure 1.3.3.e-3** shows a service network representation of the SoIP architecture.

Figure 1.3.3.e-3: Network Representation of the SoIP Architecture. *Services such as VoIP and IP video-conferencing are available in the high-performance MPLS core using protocol-specific routing systems and service-specific feature controllers. Back-end systems and the Web portal create the services from different routers and feature controllers.*

The main goal of the AT&T SoIP infrastructure is to provide a single, common, and shared infrastructure for all existing and evolving IP-based services. Many common elements of this infrastructure (e.g., border elements, call admission control (CAC), signaling gateway, call control elements, common network functions, media servers) will be reused for different IP services, reducing the development cycle and increasing service consistency and quality. Additionally, AT&T's SoIP is access-agnostic, supporting all common access technologies.

Session Initiation Protocol (SIP) is the primary internal signaling protocol used by the SoIP Infrastructure components to initiate service sessions. However, the SoIP infrastructure will support other existing session protocols, such as SIP, H.323, SS7, IGMP, and MEGACO, for creating IP-based services.

1.3.3.e.3 Converged Quality of Service

AT&T's Global IP Core Network Infrastructure is based on MPLS technology that provides an end-to-end framework to support CoS/QoS packet routing.

At the edge of the network, DiffServ packet classifications are mapped to MPLS labels through the use of the Experimental (EXP) field in the MPLS header. This field is used to specify the per-hop behavior of the packet within the network, such as scheduling and drop preference parameters. The Type of Service (ToS), or CoS, is maintained throughout the network and is delivered to the exiting access system as shown in **Figure 1.3.3.e-4**.

Figure 1.3.3.e-4: CoS is maintained end-to-end. *Using available bit space in MPLS to mark CoS outside of the IP header allows the IP based CoS to be maintained end-to-end.*

In this network architecture, traffic classification for prioritization starts at the Agency's router, which identifies application traffic flows by application or protocol type and assigns them to a specific network class. This traffic mapping is performed by the premise router/switch by setting either the IP Precedence or DiffServ bits in the ToS byte of the IP Header for each application traffic flow, as shown in **Figure 1.3.3.e-5**. The MPLS-enabled network will look at the IP Precedence or DifferServ bits of the incoming traffic and prioritize the traffic based on those settings.

Figure 1.3.3.e-5: Differentiated Services Code Point (DSCP) Bits. *The DSCP bits within the IP packet are assigned by the premise router/switch. ToS bits 2, 3, and 4 are used to identify service types at the edge. Once set, the DSCP bits are not changed by the MPLS network.*

From this packet marking within the IP header, AT&T recognizes four (4) distinct classes of service at the service edge for subscriber traffic (**Table 1.3.3.e-1**). These service classifications cover data types from time-sensitive traffic, such as VoIP-RTP and streaming video, to non-time-sensitive data, such as batch processing and web browsing.

CLASS OF SERVICE	SERVICE TYPE	DESCRIPTION OF SERVICE
CoS 1	Voice, video, multimedia	Time-sensitive traffic such as RTP streams. Signaling traffic for voice, video and multimedia are carried in CoS-1
CoS 2	Critical business applications	Transactional applications and other critical or urgent business, including near-real-time processing
CoS 3	General business applications	Database applications, commercial business applications
CoS 4	Other Data	All other data including file transfer, batch transfer, email, web browsing and database replication

Table 1.3.3.e-1: Class of Service Assignments. *Agency traffic is assigned to one of four service classes that map to Network Queues for traffic management. CoS-1 traffic is routed with high-priority data assigned to this queue, since it is generally time (packet-pacing)-sensitive and cannot be replicated by the sending application. CoS-4 data is easily resent by the applications and has little time sensitivity in its transport.*

AT&T is working on systems that would support an additional two tiers of service in the network. These additional tiers have not been fully defined at this time but will likely provide an additional business data class as well as a bandwidth scavenging data class for nonbusiness-related traffic.

As the data is exchanged from the access network to the MPLS core, each of the four service classes can be further divided into a consistent set of 25 traffic-management profiles. These customer selected profiles are then used to manage traffic congestion into and across the MPLS backbone. To accomplish this AT&T

maps the DSCP bits in the IP header, as described in **Figure 1.3.3.e-5**, into the MPLS header Experimental (EXP) bits. The EXP bits, shown in **Figure 1.3.3.e-6** are set to map the different classes of service to the different backbone queues. The 25 service profiles then perform policing on the packets based on profile filters and the percentage of data from each CoS in the access segment.

Figure 1.3.3.e-6: MPLS Header Encapsulation with Experimental (EXP) Bits Highlighted. *The EXP bits in the MPLS header represent a CoS and are assigned based upon the DSCP bit.*

EXP values are used to map the traffic into different queues on the backbone and to make discard decisions on encountering congestion in the network. When there is no congestion on the backbone trunks, there is no requirement for traffic management. During congestion on any queue and/or the trunks, the Weighted Random Early Detect (WRED) scheme is used to discard traffic in the queue (or trunk); the traffic with the lower EXP value has the higher probability of being discarded. **Figure 1.3.3.e-7** depicts traffic-routing management in the MPLS network.

Figure 1.3.3.e-7: MPLS Packet Priority Routing. *Using available network mechanisms, the MPLS network provides time-sensitive, traffic special routing to ensure reliable, well-paced delivery for higher service quality.*

In order to facilitate a better use of DiffServe in the core, AT&T is working with the IETF and other industry leaders to help develop the differentiated service traffic engineering (DiffServe TE) and differentiated service traffic engineering-maximum allocated resource (DiffServe TE-MAR) specifications. These priority schemes will be integrated in the network as they are completed and the routing processors are able to operate them without adverse impact on normal network operations.

Traffic in the AT&T backbone is seldom discarded for reasons of congestion. Given the high bit-clocking rate of the high-capacity links in the core network (which is OC-192 moving towards OC-768); individual packets of any type typically pass through any given routing point in less than 10 microseconds. This element alone creates a QoS in the core today that continues to be supported by the low-cost of increased backbone capacity.

Section 1.3.2.e further describes a high- level view of CoS and QoS operation and data stream management within the AT&T network architecture.

1.3.3.f Approach to Support Interoperability of IP and Public Switched Networks [L.34.1.3.3.f]

(f) Describe the approach to support and ensure interoperability between Internet Protocol (IP) networks and the Public Switched Telephone Network (PSTN), including the approach to map between IP and PSTN addresses. [L.34.1.3.3.f]

Using the AT&T VoIP products, Agencies can make and receive calls as they always have. The VoIP to PSTN interconnect facilities seamlessly map traditional Agency telephone numbers to the IP addresses of VoIP telephones and IP-enabled PBX systems. **Table 1.3.3.f-1** presents the basic elements used to completely interoperate with the PSTN and map IP addresses to E.164 numbers.

DEVICES	FUNCTION	BENEFIT
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 1.3.3.f-1: Basic Network Elements for Mapping IP addresses to E.164 numbers. *Multiple network elements work together to complete the translation between IP address and E1.64 number.*

The E.164 to VoIP address mapping and call-routing strategy is described in **Figure 1.3.3.f-1**. [redacted]

Figure 1.3.3.f-1: AT&T's VoIP to PSTN interconnect. [redacted]

1.3.3.f.1 Registration and Device Location

[redacted]

[redacted] [redacted] The assignment of e.164 numbering is still governed by the North American numbering plan administration (NANPA) or local number portability (LNP) translation.

1.3.3.f.2 PSTN Call Routing and Handoff

A call coming from the PSTN to a VoIP phone starts out in the PSTN End Office (SSP). The call's signaling is routed through the PSTN using SS7 and the Signal Transfer Points (STP). [redacted]

1.3.3.f.3 Call Routing in VoIP

[redacted]

1.3.3.f.4 Setting up the Call's Talk Path

[redacted]

1.3.3.f.5 Number Assignments and Allocation

AT&T is a local switching entity, or CLEC [redacted] Using that carrier interconnect status as well as its long standing status as an Interexchange Carrier (IXC) numbers that are terminated within the AT&T VoIP network come from multiple sources.

- Numbers Assigned to AT&T as a CLEC by the North American Numbering Plan Administration (NANPA)
- Numbers Ported to AT&T using Local Number Portability (LNP)
- Numbers Assigned to other LECs and CLECs that follow the Terminating Switched Access Arrangement (TSAA) reroute rules for PBX connections

Using a combination of these typical number sources, AT&T is able to route Agency numbers through the VoIP network as part of the PSTN. This means that in using AT&T VoIP no concessions need be made, such as the loss of 911 services.

1.3.3.f.6 ENUM and its Evolution

[redacted] **Figure 1.3.3.f-2**, [redacted]

[redacted]

[redacted]

Figure 1.3.3.f-2: [redacted] interconnect carriers at the IP to IP level. [redacted]

[redacted] **Figure 1.3.3.f-2** [redacted]

[redacted]

1.3.3.g IPv4-to-IPv6 Migration Support [L.34.1.3.3.g]

(g) Describe the approach for IPv4-to-IPv6 migration. [L.34.1.3.3.g]

In July 2005, Karen Evans, the Office of Management and Budget's administrator for e-Government and information technology set a June 2008 deadline for civilian Agencies to add IPv6 technology to their network backbones. The civilian Agencies are right behind the Department of Defense, which has started the migration to IPv6 due to the June 2003 announcement to transition all inter- and intra-networking by FY 2008.

Clearly, the Federal Government will lead the migration to IPv6 in the United States.

The AT&T strategy to support and assist Agencies in their move to IPv6 networks and applications includes the use of test networks, the newest IPv6 routing platforms, and the AT&T MPLS IP-version agnostic routing core.

It has long been recognized that a larger number of unique IP addresses is needed to support the vast number of devices and services that use the Internet and its private network variations. Since emerging countries such as China have started using large blocks of IPv4 addresses, the supply of free unique IPv4 addresses is diminishing rapidly. The diminishing number of IPv4 addresses has prompted a worldwide use of NAT tools, which require special firewall-like devices to be employed and break the functionality of several peer-to-peer applications. In addition, IPv4 global routing has become disjointed and inefficient.

Deployment of IPv6 will increase the number of available addresses from IPv4's 4x10^9 to IPv6's 3.4x10^{38}. This very large number of addresses will supply every potential network device with a unique dedicated address. In addition, the IPv6 address space is broken into segments that provide for better inter-network routing and larger blocks of locally administered addresses. IPv6 header space and functionality is expanded over IPv4 as well.

To support customers who want to transition to IPv6, AT&T has undertaken a set of tasks to ready the network for IPv6 support. **Figure 1.3.3.g-1** shows the AT&T migration to IPv6 in a logical set of steps from planning and testing through building and use. [redacted]

Figure 1.3.3.g-1: AT&T Lead in Transition to IPv6. [redacted]

1.3.3.g.1 AT&T's IPv6 Strategy

[redacted]

Figure 1.3.3.g-2 [redacted]

[redacted]

Figure 1.3.3.g-2: The AT&T MPLS core network [redacted]

[redacted]

1.3.3.g.1.1 Dedicated IPv6 Network Support

Direct, dedicated IPv6 access is provided to Agencies by supplying a connection to the IPv6 core via an IPv6 customer edge router. In this topology, IPv6 packets are routed in their native format through the Agency access network to the Agency local network. This access methodology will serve those users ready to become wholly dedicated to IPv6 on an Agency-wide basis.

1.3.3.g.1.2 Remote IPv6 Network Access

This topology is one that provides IPv6 packet routing that is tunneled through traditional IPv4 routing. This mechanism wraps each IPv6 packet in a complete IPv4 header and forwards it through the IPv4 network as normal. This IPv6 support methodology is similar to the Internet dial access that started in the early 1990s and continues today. Remote IPv6 tunneled access allows Agencies to operate an IPv6 local network that is connected to the IPv6 core through an IPv4 access strategy. The comparison of the dial access to the remote IPv6 tunneled access is shown in **Figure 1.3.3.g-3**.

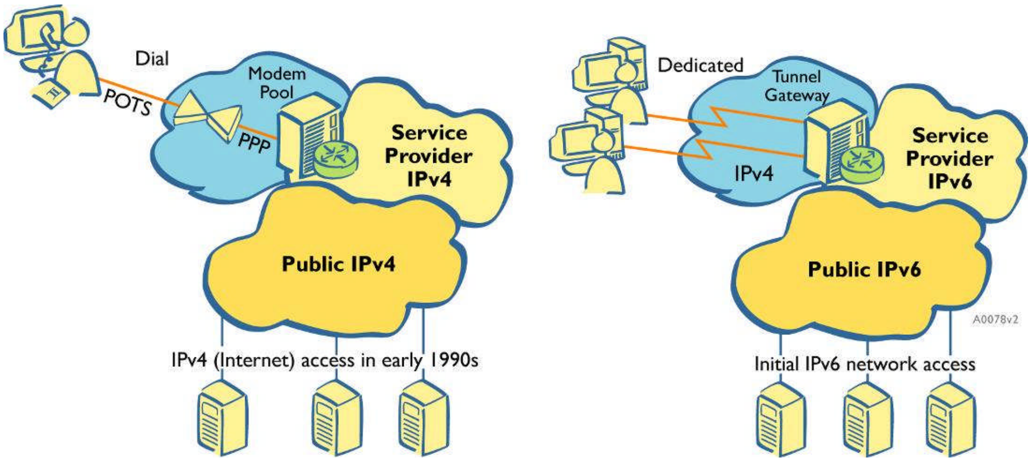

Figure 1.3.3.g-3: Initial IPv6 tunnel access is analogous to the dialup IPv4 access of the early 1990s. *The Point to Point Protocol (PPP) access to IPv4 networks in the beginning of the public access to Internet has a direct analogy to the use of IPv4 tunnels to access an IPv6 network. Both strategies employ a large existing network base.*

1.3.3.g.1.3 IPv6 VPN Options

[redacted]

[redacted]

[redacted]

1.3.3.g.1.4 IPv6 Translation Mechanisms

[redacted]

1.3.3.g.2 Beyond the Deployment

The IETF, Internet, and network providers envision IPv6 being an enabling technology. Along with the additional address space, the following offers are expected to become available once IPv6 is more widely deployed:

- Native security
- Mobility
- Anycast
- Peer-to-peer
- Applications Aware Networks

AT&T is dedicated to evolving its network to support its customers in the migration from IPv4 to IPv6. Through planning, testing, building, and support, Agencies will receive service from a network that is IPv6-ready when the time to migrate arrives.