1.4.15 Internet protocol Telephone Service (IPTelS) [C.2.7.10]

AT&T Internet protocol (IP) Telephone Service (IPTelS) provides a secure Voice over Internet protocol (VoIP) telephone service with features that exceed those found in the traditional public switched telephone network (PSTN). This product offers the capabilities of VoIP today, with the quality Agencies can count on, from a system that has been architected for the future.

1.4.15.1 Technical Approach to Transport/IP/Optical Service Delivery [L.34.1.4.1]

1.4.15.1.a Approach to Service Delivery [L.34.1.4.1.a]

(a) Analyze the service requirements specified in this solicitation and describe the approaches to service delivery for each service. [L.34.1.4.1.a]

With the adoption of VoIP in business enterprises, the solutions for small to medium enterprise applications may not necessarily be best served using traditional or IP PBX technology. With that in mind the AT&T Voice Dynamic Network Applications (DNA) IP Centrex service has been created. This service offers Agencies a full set of PBX-like calling features and functions using network based VoIP call switching and IP-ready telephones that have many desirable business phone features. To better support Agencies in the VoIP transition, the AT&T VoIP architecture retains special features in the public switched telephone network (PSTN), such as 911 access and private dialing plans. **Figure 1.4.15.1-1** shows the basic IPTelS architecture with both the Agency and PSTN interconnects.

Figure 1.4.15.1-1: AT&T VoIP Product Access. [redacted]

The AT&T approach to IPTelS, described in **Table 1.5.15.1-1**, is for a system of application intelligent servers and routers that provide the AT&T IP-based voice service that is similar to PSTN functionality using the benefits of an IP network. Using the self-contained, network-based VoIP approach, Agencies need only to connect to the customer edge router to gain access and operate their IP telephones with a full set of calling features over IP. This approach also lends itself to PBX convergence with other IP voice-based products, such as telecommuting.

SERVICE DELIVERY APPROACH	DESCRIPTION
Standards compliance	The service is delivered based on the applicable set of IETF, ITU-T, IEEE and NIST standards
Class of service (CoS) routing with MPLS	Differentiated service (DiffServe) routing is combined with the multiprotocol label switching (MPLS) network core to provide PSTN-like voice quality

The AT&T standardized VoIP distributed architecture supports common functions and provides call completion quality	• Distributed, high-availability service nodes provide good call completion rates
	• DNA network centralizes common core functions, based on the session initiation protocol (SIP), allowing users to share services across different access networks such as:
	  ◦ Call control, E.164 to IP translation and gateway access
	  ◦ IP Centrex – Provides PBX-like service over the network
	  ◦ PSTN access

Provides complete PSTN access	• Access to PSTN is built into DNA network. • Network performs E.164 to IP translation • Provides inbound and outbound calling • Access operator service and directory assistance access • Fully functional 911/E911 interconnect and [redacted] • Access to international calling available
IP Centrex uses IP telephones supporting a wide range of PBX like features as well as VoIP only features	• The full functionality of PBX, with over [redacted] style and telephone network features is hosted inside AT&T VoIP network. • Service is integrated with VoIP network that offers both private call routing for virtual private voice networks (VPVN) and public dial routing worldwide. • Service supports next-generation SIP phones with large programmable liquid crystal display (LCD) panels and soft keys. These phones are more intuitive and easier to use than their PBX connected counterparts [redacted] • All features and functionality are controllable through AT&T **Business**Direct®, allowing Agencies to manage their own service, as needed.
Widely Available	Service is available in over [redacted]
The service is access-agnostic and supports station mobility	The Service is access independent and can be accessed using dedicated VPN, cable or digital subscriber line (DSL), [redacted] • Provides home PBX functionality from a variety of locations • Allows for mobility between different access methods used by an Agency • Using station mobility and the administrative portal, moves, adds, and changes can be made by Agency workers without consulting onsite telecom specialists

SERVICE DELIVERY APPROACH	DESCRIPTION
Uses low bandwidth codecs	Low bandwidth codecs reduce bandwidth needs, which lowers cost
Secure and reliable	• Service is built on top of AT&T's reliable IP network • The service is secured by both AT&T standard security practices and authentication and control built into SIP and the border control elements • Defined security policies and practices the safe guard denial of service attacks, intrusion, and invasion of privacy.

Table 1.4.15.1-1: The approach to IPTelS provides access, features, and flexibility. *The AT&T IPTelS offer includes full PSTN access, over [redacted] calling features, web access, and quality calling over an MPLS VPN.*

As shown above, VoIP call processing and routing is performed in a secure and specialized environment through the connection of call-routing service nodes to the AT&T MPLS core. Other advanced services, such as the unified messaging services (UMS), are also connected to the core network and are managed by the service-creation systems. This combination of applications and service-creation systems allows custom solutions to be created by the user. The web portal allows users and Agency administrators to manage and create their own calling solutions.

In addition, the AT&T-dedicated MPLS VoIP network is more resilient to circuit outages than its circuit-switched counterpart or other VoIP networks. Using a network, such as the Internet, for VoIP telephone service presents a much higher security risk and cannot guarantee call quality or dependability.

1.4.15.1.b Benefits to Technical Approach [L.34.1.4.1.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.34.1.4.1.b]

AT&T's Networx services and IPTelS, 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 1.4.15.1-2** describes each service in relation to FEA, summarizes its contribution, and/or provides an example of how it facilitates FEA implementation.

SERVICE DELIVERY APPROACH	BENEFIT	FEA FACILITATION
Class of service (CoS) routing with MPLS	Combination of multiprotocol label switching (MPLS) network and CoS-based priority routing provides PSTN-like voice Quality over VoIP	Agencies can transition to VoIP and remain aligned with the industry without sacrificing call quality. FEA link: TRM/Service Access and Delivery/Service Transport
Standardized VoIP distributed architecture supports common functions and provides call completion quality	• The service provides call completion rates that are comparable to the PSTN both inbound and outbound • The network takes care of 100% of the E.164 to IP translations taking the complexity of VoIP away from Agencies • IP Centrex, Unified Messaging, Voice Mail, and IP Conference Calling can be bundled in custom packages giving Agency users only the service they require	The common, standardized distributed architecture supports additional functions across multiple network applications. Example: A web-enabled calling platform for Government assistance portals. FEA Link: TRM/Component Framework/Business Logic/Platform Independent
Provides complete PSTN Access	• Allows calls to function in both directions as integrated part of PSTN. • Links to services, such as 911, E911, and Communications Assistance for Law Enforcement Agencies (CALEA), all automatically included.	Agencies will be fully interconnected to the existing worldwide PSTN FEA Link: TRM/Service Access and Delivery/Delivery Channels/Extranet
IP Centrex uses IP telephones supporting a wide range of PBX-like features as well as VoIP only features	• Agencies receive service they would expect from an onsite PBX • Agencies do not need to purchase telecommunications equipment, such as PBXs or voice messaging systems. • No specialized PBX administration costs, potentially reducing headcount • Next-generation IP telephones are more intuitive and require less training	Agencies receive the latest in VoIP technology and capability without purchasing equipment that can become obsolete. FEA Link: TRM/Service platform and Infrastructure/Infrastructure/Embedded Technology Devices
Wide availability	Gateways are deployed throughout network, providing access to local calling in over 100 MSAs in the CONUS area.	Agencies direct local access covering over 90% U.S. population. FEA Link: TRM/Service Access and Delivery/Service Transport
Access agnostic	Service can be accessed using several methods including: • Dedicated VPN for Agency office • Broadband cable or digital subscriber line (DSL) connection for telecommuting • From hotel or business as traveling user	Station mobility supports Agencies in a variety of both on-site and off-site locations. FEA Link: TRM/Service Access and Delivery/Access Channels/Other Electronic Channels
Uses low bandwidth codecs	Low bandwidth codecs reduce bandwidth needs, which lowers cost	Agencies bandwidth requirements are reduced using VoIP. FEA Link: Budget/performance Integration
Secure and reliable	• Providing service in combination of VPN access and VoIP core service networks provides better security and reliability than using the Internet for VoIP • Agency telephone traffic is not placed in vulnerable networks that have no performance guarantees	The service is provided in a secure network so Agencies do not need to worry about transitioning to VoIP. FEA Link: TRM/Component Framework/Security

Table 1.4.15.1-2: Agency Benefits from AT&T VoIPTS. *The AT&T VoIP network provides a high level of security and provides a superior level of performance. An Internet-based calling service cannot provide such superior service.*

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

- 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 can assist specific departments and Agencies to meet mission and business objectives through a comprehensive IPTelS offering.

1.4.15.1.c Major Issue to Service Delivery [L.34.1.4.1.c]

(c) Describe the problems that could be encountered in meeting individual service requirements, and propose solutions to any foreseen problems. [L.34.1.4.1.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 selects a service provider that brings the depth and background to minimize an Agency's risk during transition. Our experience has enabled us to develop proven methods, processes, and procedures to mitigate risk in the simplest to the most complex projects.

Table 1.4.15.1-3 presents six risks involved with transitioning to IPTelS. As with all large projects, we enter each of these risks and others (after identification and characterization) into our risk-tracking database, and immediately take steps to mitigate them before they become an issue. Because risk management is more effective when all stakeholders are active in the process, AT&T engages the GSA, the client Agency, and other Government solution partners for success with risk mitigation activities.

RISK	RISK DESCRIPTION	RISK MITIGATION
Implementation/ transition	In our experience, all Agencies are concerned about business disruption when moving from traditional PBX to an IP PBX environment. Adequate planning can minimize this risk.	• Develop engineering design that considers equipment replacement, concurrent operations, and brake-in periods • Lab test all service delivery processes and procedures • Possess detailed back-out procedures • Conduct delivery activities during non-business hours, as directed by the Agency site point-of-contact (POC).
Lack of standards	No specific standards cover VoIP interconnection for all PBX systems.	• VoIP network has been designed with a SIP-based core and has protocol conversion built into network. • Until a single set of protocols becomes accepted, support for differing protocols is through transformation at the VoIP network edge.
Local area network (LAN) configuration	Converting to VoIP transport could require some Agency LAN and firewall changes.	• AT&T can provide Agencies with onsite assessment and engineering solutions that support Agency missions, while assisting in transition to VoIP.
Training	New service can require some specific training on use of features.	• AT&T Government Solutions provides familiarization and feature training on a case-by-case basis. • Agency telephone system administrators can receive support to assist with the changing aspect of automatic call distribution and private dialing plans. • Support helps Agencies realize the full potential of their new telephone service.
Access capacity	Lack of bandwidth in VoIP access system can affect overall call quality.	AT&T provides access engineering recommendations; Agencies receive correct amount of access for their service.
Security	VoIP is an IP service and can be vulnerable to the typical attacks and transmission anomalies in Internet.	• AT&T does not dump Agency VoIP traffic onto the Internet for transport. • AT&T provides VoIP services over a network that is dedicated to VoIP that is guarded by strict security practices.
Product longevity	New products are often eclipsed by the next generation of service leaving early adopters with useless equipment	Since the AT&T IPTelS service is completely network based, and is served over standard routing equipment, any improvements or generational changes are made in the AT&T network.

Table 1.4.15.1-3: Planning and Training Manage VoIP Issues. *AT&T provides services on an individual case basis to help Agencies with problems that can occur when deploying IPTelS.*

AT&T has taken steps to identify risks and provides mitigation for risks that are associated with its VoIPTS service offer. AT&T is committed to service excellence and will work with the Agency to identify and resolve potential problems that may occur during service delivery.

1.4.15.1.d Network Architecture Synchronization [L.34.1.4.1.d]

(d) Describe the synchronization network architecture to support the offeror's access and transport networks. [L.34.1.4.1.d]

AT&T is a leader in the area of network synchronization, by virtue of our active role in the international and domestic standards organizations and our existing industry-unique dedicated timing and synchronization network for distributing Stratum 1-traceable timing to our own national and international telecommunications networks.

Synchronization for access and transport networks begin with the Federal Government's cesium-based standard signal that is distributed to a series of [redacted] AT&T derives synchronization from those GPS systems as the primary clock source. As a backup AT&T deploys rubidium oscillator-based clocks, which have an accuracy of $1x10^{-13}$ (Stratum 1). IPTelS derives its synchronization from the synchronous optical network (SONET) infrastructure on which those services ride.

AT&T has a primary reference clock in every node, which is more reliable under dual and multiple failure conditions. This makes our timing/synchronization network truly unique in the industry, with unparalleled performance. A more detailed discussion on network synchronization is provided in Section 1.3.6.1, Network Architecture Synchronization.

1.4.15.2 Satisfaction of Transport/IP/Optical Performance Requirements [L.34.1.4.2]

1.4.15.2.a Service Quality and Performance [L.34.1.4.2.a]

(a) Describe the quality of the services with respect to the performance metrics specified in Section C.2 Technical Requirements for each service. [L.34.1.4.2.a]

AT&T will meet or exceed the mandatory performance metrics of Latency [200 ms AQL], Jitter [10 ms AQL], and Grade of Service (packet loss) [0.4% AQL] as defined in Networx Universal RFP Section C.2.7.10.4.1. To support Agency VoIP services, the AT&T network is built to perform at a level of quality that is required for acceptable voice quality, along with reliable call completion rates; network impairments are controlled network wide. **Table 1.4.15.2-1** lists typical core month-by-month network performance, as compared to the requirements set forth in the RFP.

KEY PERFORMANCE INDICATOR (KPI)	SERVICE LEVEL	PERFORMANCE STANDARD (THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL *
CONUS Round Trip Latency	Routine	200 ms	[redacted]
End-to-End Packet Loss	Routine	0.4%	[redacted]
Availability	Routine	99.6%	[redacted]
	Critical	99.9%	[redacted]
Packet Jitter (Network)	Routine	10 ms	[redacted]
Time to Restore	Without Dispatch	4 hr	[redacted]
	With Dispatch	8 hr	[redacted]

[redacted]

Table 1.4.15.2-1: AT&T's Performance Levels Exceed Minimum Requirements. [redacted]

The use of MPLS exclusively in the AT&T VoIP core, combined with high-capacity inter-router links, provides VoIP packets with very good routing performance characteristics. Coupling the high-capacity efficient network with high-availability VoIP call processing equipment provides Agencies with a VoIP service that has both good sound quality and high call-completion rates. A comparison of AT&T's VoIP network call quality to a typical IP network, such as the Internet, is shown in **Figure 1.4.15.2-1**.

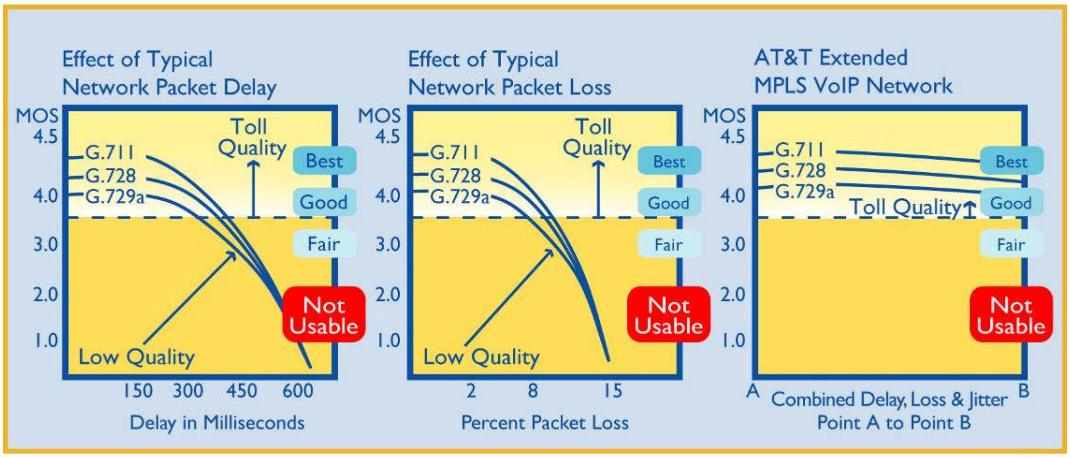

Figure 1.4.15.2-1: AT&T Network Performance over Typical VoIP Networks. *AT&T VoIP network carefully controls impairments to supply a higher quality VoIP service in terms of delay and packet loss.*

The combination of performance parameters in the AT&T VoIP network helps produce quality VoIP call satisfaction of mean opinion score (MOS) [redacted]

1.4.15.2.b Approach to Monitoring and Measuring Performance [L.34.1.4.2.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.34.1.4.2.b]

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. To provide the Agencies with the most accurate representation of the service performance, AT&T has deployed a separate service performance measurement infrastructure to collect network performance information. AT&T's measurement methodology, therefore, more closely captures the real performance that end users experience by measuring the data path that is very similar to the paths that the end user at a would follow. **Table 1.4.15.2-2** outlines the methods used to measure the various IP key performance indicators.

Key Performance Indicator (KPI)	Approach to Monitoring and Measuring
Ability to measure network and service specific metrics	[redacted]
Availability measured (service delivery point [SDP]-to-SDP)	[redacted]
Time to Restore (TTR)	[redacted]
R-Factor measures call performance	[redacted]

Table 1.4.15.2-2 Monitoring and Measuring IPTelS. *Agencies can easily manage the IPTeLS service with data delivered through the AT&T* ***BusinessDirect*** *web portal that is easy to access and use*

In the AT&T VoIP network, call quality and network transport quality are monitored at each network element using task-specific element management systems (EMS), as shown in **Figure 1.4.15.2-2**.

Figure 1.4.15.2-2: Management Network [redacted]

[redacted]

1.4.15.2.c Performance-Level Improvements [L.34.1.4.2.c]

(c) If the offeror proposes to exceed the Acceptable Quality Levels (AQLs) in the Key Performance Indicators (KPIs) required by the RFP, describe the performance level improvements. [L.34.1.4.2.c]

The AT&T core VoIP network is based on MPLS routing between all entry and exit points. The performance characteristics of MPLS, combined with high-capacity router-to-router links, create a high-performance network that exceeds the minimum performance levels requested in the RFP.

Table 1.4.15.2-3 lists the key AT&T network performance targets, as compared to the RFP performance targets, and denotes the percentage improvement over the Networx performance threshold marks.

METRIC	NETWORX AQL THRESHOLD	PROPOSED SERVICE QUALITY LEVEL*	IMPROVEMENT PERCENTAGE
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]			

Table 1.4.15.2-3: [redacted] **Performance Specifications.** *Using MPLS and a large footprint topology, the AT&T VoIP core network performs at levels that provide call quality that rivals the public switched network (PSN).*

Using the VoIP core network with the above set of packet performance criteria, VoIP calls can rival the quality of PSTN calls. This quality applies to both the speech quality and call completion rate, because the network performance criteria apply to both the talk-path network and the call-setup and signaling network. A network that degrades the signaling path in favor of the talk path can cause incomplete and dropped calls. AT&T provides complete call quality through networks that support high call completion rates and call sound quality.

End-to-end VoIP performance depends on both core network performance and access network performance. AT&T staff members calculate the customer-access bandwidth requirements, based on recommended site-specific services and usage. For Agencies to receive the needed levels of performance, the AT&T site-specific bandwidth recommendations for access arrangements must be followed.

1.4.15.2.d Rationale and Benefits for Additional Performance Metrics [L.34.1.4.2.d]

(d) Describe the benefits of, rationale for, and measurement of any additional performance metrics proposed. [L.34.1.4.2.d]

AT&T is the only carrier that offers R-Factor that is an industry standard VOIP performance measure that is equivalent to mean opinion score (MOS).

AT&T uses the ITU-T G.107 call quality measurement system to measure the quality of each call in the VoIP network as it passes into or out of the core. The output is expressed in the standard R-Factor output scale. AT&T proposes the R-Factor performance metric as summarized in **Table 1.4.15.2-4**.

PROPOSED KPI	DESCRIPTION OF PROPOSED KPI	BENEFIT OF PROPOSED KPI
[redacted]	[redacted]	[redacted]

Table 1.4.15.2-4: Performance Level Improvements. [redacted] (**Figure 1.4.15.2-3**).

Figure 1.4.15.2-3: Call [redacted]

[redacted]

1.4.15.3 Satisfaction of Transport/IP/Optical Service Specifications [L.34.1.4.3]

1.4.15.3.a Service Description [L.34.1.4.3.a]

(a) Provide a technical description of how the service requirements (e.g., capabilities, features, interfaces) are satisfied. [L.34.1.4.3]

The VoIP services are all built on the AT&T services over IP (SoIP) architecture shown in **Figure 1.4.15.3-1**. The VoIP/SoIP architecture uses the upper layers of the network architecture to create the different VoIP services that are available. The VoIP products are the first complete products to take advantage of the overall AT&T network convergence plan (SoIP). More information on SoIP and the convergence plan is provided in Section 1.3.3(b-d).

As shown in **Figure 1.4.15.3-1**, there are four layers that support the VoIP telephone service: (1) Access, (2) Border Edge, (3) VoIP network, and (4) **Tables 14.15.3-1** through **14.15.3-4** describe the functions and benefits of each layer and the advanced services they support**.**

Figure 1.4.15.3-1: Systems Supporting AT&T's VoIP Network. *Agencies using the AT&T VoIP telephone service receive a full set of features supported by four service creation layers.*

Layer 1, Access, provides access to customers, partners, and the PSTN. The VPN services, the links to the PSTN, and the peering to other VoIP networks are all constructed with security and quality of service as priorities (**Table 1.4.15.3-1**).

LAYER ONE - ACCESS		
Feature	***Description***	***Benefit***
VPN	Access is through VPNs that use MPLS provide quality packet delivery and security	• Agencies receive a service that is comparable to the service received from the PSTN.
Class Of Service routing	CoS is created for all traffic to and from the customer premises equipment (CPE); the VoIP packets are routed in the highest priority queue, which helps create a consistent packet delivery end-to-end.	• Agency routers provide the first point of routed packet QoS so networks that don't provide priority for VoIP packets are not traversed. • Provides PSTN like quality enhancing Agency communications
Managed access	Access service is monitored and managed by AT&T to provide consistent	• Agencies do not need to manage routers, access circuits or security configurations. AT&T

LAYER ONE - ACCESS		
	results and fault management.	manages those as part of the VPN service
VoIP-specific CPE	Access termination equipment is specially optioned to handle VoIP calling systems and configured to perform well in a VoIP environment.	• Agency routers provide the first point of routed packet QoS so networks that don't provide priority for VoIP packets are not traversed. • Provides PSTN-like quality enhancing Agency communications
Extranet tunnels	Tunnels through IP extranets allow Agency users to access the service from locations outside the office.	• Agency workers can telecommute or use their office telephone number and features while in a hotel or on other business broadband networks.
Station mobility	Stations register with nearly any assigned IP address while retaining their E.164 telephone number, providing station mobility	• Station mobility allows the use of extranet tunnels as stated above • Station mobility simplifies office moves
Interfaces	Ethernet RJ-45 Analog – Two wire (Telcordia SR-TSV-002275)	• Agencies can use r IP-ready telephones, soft phones on a PC, or standard analog phones and devices such as fax machines.

Table 1.4.15.3-1: Layer 1 Access Strategies.. *The access provided to customers, partners, and PSTN strategies play an important role in the quality if VoIP services.*

Layer 2, Border Edge, provides gateways that allow secure access to the VoIP core transport and switching network. At the edges of the network are the customer-facing BE devices, the PSTN gateways (network gateway BE [NGBE]), and other access gateways (such as the IP gateway [IPBE]), as listed in **Table 1.4.15.3-2**.

LAYER TWO - BORDER EDGE		
Feature	***Description***	***Benefit***
Network Security	BE, [redacted] acts as a security device by tracking call setup information and only allowing call traffic to authorized end points.	The service is secure and protected from: • Denial of Service Attacks • Theft of, or unauthorized use • Intrusion • Eavesdropping
Network Address Translation	Portion of BE's ALG function is to perform as a network address translator to interconnect calls from differing IP networks.	• Agencies can use the service from networks with differing IP numbering schemes • Agencies can retain the use of translated networks
Multiple Protocol Support	Along with the security and address translations, the SIP BE, MEGACO BE [redacted] provide signaling protocol conversion so that differing Agency devices can access the service.	• The service supports SIP phones directly • The service can also be integrated with other topologies that use other protocols and switching mechanisms such as PBX equipment.
Call Quality Measurement Points	Every BE, including the NGBE, provides a quality control check point, measuring call quality in and out of the core network.	Agencies can see, by logging into AT&T **Business**Direct, the quality of each call inside the VoIP network.
PSTN Interconnect	PSTN gateway (NGBE) converts VoIP into a traditional, circuit-switched voice and provides an appropriate ingress/egress point for voice traffic. It works in conjunction with the call control engine (CCE) and a signal system 7 (SS7) gateway to ensure calls continue to route properly, once they are passed to the PSTN.	• Agencies receive full access to the PSTN • PSTN calling is inbound and outbound • The PSTN interconnect will support the majority of calls • Agencies do not need to change their calling habits to use VoIP

LAYER TWO - BORDER EDGE		
Special Services Interconnects	Other access gateways include access to [redacted] services and links to different public safety answering points (PSAPs) for 911 call handling.	• Access to 911 and other local services is properly executed so Agencies won't need a procedural work around [redacted]

Table 1.4.15.3-2: Layer 2 Gateway Security. *The border between the VoIP domain and the remaining networks is secured by gateways called border elements.*

Layer 3, VoIP network core, is based on the CCE, which routes VoIP calls within the high-capacity, MPLS-based IP network. This network provides security and quality for the VoIP customer (**Table 1.4.15.3-3**).

LAYER 3, VOIP CORE		
Feature	***Description***	***Benefit***
Core provides quality over wide reach	VoIP core provides direct local number access to CONUS PSTN reach that exceeds [redacted]	Agencies can use this service with their existing local numbers in a large number of locations.
Core is routing interconnected with AT&T TDM voice network	[redacted] CONUS PSTN locations is carried by AT&T to local handoff over traditional trunking.	Inbound and outbound call coverage is [redacted] of the CONUS calling areas.
Class of Service is maintained in core	CoS routing is maintained through core using MPLS.	Call quality is similar to the PSTN.
Scalable call routing infrastructure	CCE call routing engine uses SIP signaling that matches the PSTN's E.164 telephone number routing hierarchy for scalability and complete PSTN interoperability.	Agencies will receive a service that maintains its high level of quality as the service grows.
[redacted]	CCE provides access to special call routing functions that provide call routes, such as 911 and [redacted]	Agencies do not need to change their calling habits or use work-arounds for emergencies.
High quality packet routing	VoIP core provides very low latency and high-packet delivery reliability for overall quality service. (Refer to Section 1.4.15.2.c for actual performance metrics.)	Call completion rates and call quality will be comparable to the PSTN based telephone services.

Table 1.4.15.3-3: Layer 3 Highly Scalable Call Control. *Call routing and access to the PSTN are facilitated by the VoIP core components.*

Layer 4 Advanced Services (AS), are general computing devices running in a highly available configuration. These processors create features that comprise the different types of VoIP product offers, as listed in **Table 1.4.15.3-4**.

LAYER 4, ADVANCED SERVICES (AS)		
Feature	***Description***	***Benefit***
Works with CCE	CCE in VoIP network core consults advanced feature servers for line treatments on call-by-call basis.	Advanced services such as unified messaging can be easily included in an Agencies VoIP service suite.

Layer 4, Advanced Services (AS)		
Secure and reliable	Application server (AS) layer provides secure environment with network and system redundancy for all AS processors. Processors are monitored by AT&T 24x7x365 to ensure reliable operation.	• Call completion rates are high and special services are routinely available • Agencies can count on the service being available in the same way they depend on the PSTN
Special controls for call flow	Agency users can control action of CCE through configuration of advanced services, using their telephone or web and service-creation environment.	• Agencies can create call controls that help support their work flow. • Find-me and other multiple network services are available and can be customized
Easily augmented	AS are based on software so the feature set is easily augmented, as compared to PSTN and dedicated hardware switching.	• Agencies are not stuck with on site systems and equipment that can become obsolete. • The service will be upgraded as the VoIP industry grows
No vendor locks on features	Number of and type of AS servers in network is virtually unlimited, so there is no vendor lock on services that exist in PSTN.	• New service paradigms are implemented at a much lower cost • Blended services with both network based and Agency based equipment are possible • Integration between computing and telephone systems is possible
Feature servers	AS layer provides special feature servers, such as IP Centrex, which provides common calling features [redacted]	Basic business calling functions are available without purchasing a PBX: [redacted]
Multiple feature sets are available	AS processors are used to create features that are commonly in PBX systems, as well as new VoIP-only features, such as [redacted] and remote-integrated automatic call distributor (ACD).	• Agencies can manipulate their calling features form their station or form a web portal • Integration with computing such as a desktop PC is possible.
Sip based call routing allows new features	Additional services that require mid-call switching are available through special AS systems to create features, [redacted]	• Agency workers can be more mobile while retaining communications availability through find and follow features • Unified messaging (UMS) allows Agency workers to traverse other phone networks without leaving the UMS application
Contains service creation layer	Allows functions such as web accessible service manager and administration manager. Also allows for customer-enabled provisioning of new or expanded service.	• Existing VoIP services are made accessible through the web portal using the service creation layer • New services and functions are made available to Agencies through the web portal • Agencies will be able to combine different network based services into a single service.

Table 1.4.15.3-4: Layer 4 Special Calling Features and Messaging. *The AS layer provides a location within the secure VoIP network for special call processing, such as IP Centrex and unified messaging, to operate. The virtual common repository allows services from multiple vendors and custom applications for individual Agencies or users to be more easily added to the network.*

[redacted] AT&T takes care of the details and complexities of running a scalable and secure telephone system. Therefore, Agencies can concentrate on their own missions.

1.4.15.3.b Attributes and Values of Service Enhancements [L.34.1.4.3.b]

(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. [L.34.1.4.3.b]

Additional features offered by the AT&T voice DNA service, as compared to the requirements in the RFP, are listed in **Table 1.4.15.3-5**. This list of additional features is expected to increase over time as the VoIP services become more prevalent in the industry.

Network Features		
Service Enhancement	**Description**	**Benefit**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
Station Features		
Service Enhancement	**Description**	**Benefit**
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

	NETWORK FEATURES	
	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
	SIP FORKING FEATURES	
Service Enhancement	***Description***	***Benefit***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 1.4.15.3-5: Additional Features in IP Centrex Service. *Agency users can take advantage of these additional features using the AT&T Voice DNA service. Because this is a new product, this list of extra features is expected to grow.*

1.4.15.3.c Service Delivery Network Modifications [L.34.1.4.3.c]

(c) Describe any modifications required to the network for delivery of the services. Assess the risk implications of these modifications. [L.34.1.4.3.c]

No modifications to the AT&T voice DNA network are required to provide Agencies with a high-quality VoIP service.

1.4.15.3.d Transport/IP/Optical Service Experience [L.34.1.4.3.d]

(d) Describe the offeror's experience with delivering the mandatory Transport/IP/ Optical Services described in Section C.2, Technical Requirements. [L.34.1.4.3.d]

AT&T possesses years of experience offering voice service to both Government and commercial entities. This experience has given us the ability to engineer and deliver services that create value to our customers. **Table 1.4.15.3-6** cites two examples of AT&T's ability to deliver managed services.

[redacted]		
Client Need	Solution	Create Value
[redacted]	[redacted]	[redacted]
[redacted]		
Client Need	Solution	Create Value
[redacted]	[redacted]	[redacted]

Table 1.4.15.3-6: Experience Delivering IP Telephony Services. *AT&T measures success by our ability to deliver solutions to our customers that create value to their business.*

1.4.15.4 Robust Delivery of Transport/IP/Optical Services [L.34.1.4.4]

1.4.15.4.a Network Traffic Utilization [L.34.1.4.4.a]

(a) Given the offeror's current network capacity and utilization, explain how the offeror will support the Government requirements specified in the traffic model. Describe the impact on capacity and utilization, as well as any infrastructure build out contemplated. [L.34.1.4.4.a]

Per the usage numbers supplied by the GSA for Networx VoIP products, calculation of the total equivalent numbers of DS0s and peak bandwidth consumption is provided in **Table 1.4.15.4-1**.

Contract Year	Subscriber Numbers[1]	VPN Ports[2]	DS0 Count	Bandwidth Mbps[3]	% Total AT&T IP Capacity[4]
1	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
2	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
3	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

CONTRACT YEAR	SUBSCRIBER NUMBERS[1]	VPN PORTS[2]	DS0 COUNT	BANDWIDTH MBPS[3]	% TOTAL AT&T IP CAPACITY[4]
4	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
5	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
6	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
7	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
8	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
9	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
10	[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

[redacted]

Table 1.4.15.4-1: Usage Calculations based on Networx Usage Estimates Provided by GSA. *Overall usage of the network for IPTelS is a very small portion of the AT&T network capacity. The overall high capacity of the AT&T network will provide Agencies with a high QoS.*

The AT&T IP network supports the transport and delivery of over 2.2 petabytes of traffic at less than 40 percent peak usage. The additional load that would be added to the network for CIPS is less than 0.0001 percent of the total traffic. The overall AT&T network capability to move very large amounts of data at low usage will provide Agencies with dependable packet delivery for the life of the contract.

1.4.15.4.b System Robustness and Resiliency [L.34.1.4.4.b]

(b) Describe the measures and engineering practices designed to provide robustness of the access and backbone networks, ensure resiliency, and plan for growth. [L.34.1.4.4.b]

Rigorous engineering practices and measurements of the network allow Agencies to obtain a scalable, reliable service to build and operate mission-critical applications. IP service and backbone capacity planning within the AT&T IP network are driven by three main factors (**Table 1.4.15.4-2**).

MAJOR CAPACITY PLANNING FACTORS	
Business Planning	Annual business planning forecasts of all existing and new AT&T services that use IP backbone network and connected service give combined prediction of use.
Technology Migrations	Planned technology migration and insertion capacity is built into system before migration starts.
Historic Growth	Historic traffic growth of existing services, as measured over time, allows for buildout, based on increasing use by AT&T customers.
TYPICAL APPLICATION OF FACTORS	
Call Loads	Call loads to incumbent local exchange carriers (ILECs), competitive local exchange

MAJOR CAPACITY PLANNING FACTORS	
	carriers (CLECs), and other inter-exchange carriers (IXCs) are all tracked on a trunk group basis and have additional capacity added based on three principles above.
Use of a Service	Each of above principles is also applied to components and systems that constitute service such as VoIP.

Table 1.4.15.4-2: Key Capacity Planning Factors. *Network capacity buildout is based on both predictive and measured data. AT&T provides service from a network with more than enough capacity to do the job and grow.*

Because AT&T's IP backbone network is a two-tier architecture with an MPLS network core that does not contain any Internet routes (Internet-route free core), the IPTelS provided to the Agencies is secure, scalable, and reliable. As the number of Internet routes increased dramatically during the late 1990s, the stability of the IP backbone network was at risk. AT&T recognized this threat and engineered a two-tier architecture that moved the Internet routes to the edge routes, providing a stable, Internet-route-free MPLS core. This new core supports metered growth without the threat of being overloaded by outside or uncontrollable sources.

1.4.15.5 Transport/IP/Optical Service Optimization and Interoperability [L.34.1.4.5]

1.4.15.5.a Approach to Optimizing IP-based and Optical Services [L.34.1.4.5.a]

(a) Describe the offeror's approach for optimizing the engineering of IP-Based and Optical Services. [L.34.1.4.5.a]

A detailed discussion of our approach to optimizing the engineering of IP-based and optical services is provided in Section 1.3.6.2.a.

1.4.15.5.b Network Architecture Optimization [L.34.1.4.5.b]

(b) Describe how the offeror will utilize methods such as remote concentration, switching/routing capabilities, and high bandwidth transmission facilities to optimize the network architecture. [L.34.1.4.5.b]

Optimization of the network architecture through the use of remote concentration, switching/routing capabilities, and high bandwidth transmission facilities is described in Section 1.3.6.2.b.

1.4.15.5.c Optimizing Engineering Techniques [L.34.1.4.5.c]

(c) Describe the engineering techniques for optimizing access for improved performance or increased efficiency in areas where large concentrations of diverse customer applications exist (e.g., the use of multi-service edge platforms). [L.34.1.4.5.c]

Optimization of the access for improved performance or increased efficiency through the use of multi-service edge (MSE) platforms is described in Section 1.3.6.2.c.

1.4.15.5.d Vision to Implement Service Internetworking [L.34.1.4.5.d]

(d) Describe the offeror's vision for implementing service internetworking over a common infrastructure (e.g., IP-centric architecture). Include a view on network interoperability, control plane integration, and optical infrastructure support for IP-Based Services. Describe the benefits and rationale of the offeror's approach. [L.34.1.4.5.d]

The implementation of service internetworking over a common infrastructure – including network interoperability, control plane integration, and optical infrastructure support – is described in Section 1.3.6.2.d.

1.4.15.6 Narrative Text Requirement

1.4.15.6.1 Connection to the IP Network [C.2.7.10.1.3]

IPTelS requires a connection to the contractor's IP network.

The AT&T voice DNA services are provided over a managed IP VPN that helps control the quality of every call. The VPN and access uses MPLS to the customer edge (CE) router to maintain a superior quality of service. **Figure 1.4.15.6-1** depicts a typical managed access configuration for a combined VoIP and data access service.

Figure 1.4.15.6-1: Typical Dual Link and Router Option for Access and Redundancy. *Network access arrangements provide access to the AT&T VoIP network. Access arrangements are available in a variety of configurations, including single link and those using multiple access routers. The type of access network options can be varied, depending on Agency needs.*

VoIP services are also available by VPN tunnel connection through an IP extranet. Using this configuration, Agency workers can work from home over a cable or DSL broadband link, or from the broadband Internet connection provided by a hotel or other enterprise. Since the communications is encapsulated in an encrypted tunnel, and the tunnel is terminated on the AT&T VoIP network, the call security can be trusted. **Figure 1.4.15.6-2** shows extranet access on a secure IP tunnel.

Figure 1.4.15.6-2: IP Telephone Service from IP Extranets. *Users are not limited to accessing their station features only from a desk phone at the office. All of their station features are available by tunneling into the service from other broadband locations.*

Refer to Section 1.3.2 for more information on overall access arrangements, quality control mechanisms, and their configuration.

1.4.15.6.2 Routing 700 Number Calls [C.2.7.10.1.4 (2)(e)]

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:
2. The contractor shall provide the following minimum capabilities:
e. The contractor's IPTelS shall interoperate with non commercial, Agency specific 700 numbers

Along with the routing and handling of 700 number calls in the circuit switched voice products, the [redacted] service is a [redacted] telephone service and routes all IP-to-outgoing Agency 700 number calls to the appropriate carrier, as assigned by the carrier

CALL TYPE	HANDLED
PSTN-to-VoIP	Routed to and handled by the [redacted] call routing system. Passed to VoIP network to complete call.
VoIP-to-PSTN	Routed by VoIP network to Agencies preferred inter-exchange carrier (PIC). Carried by that PIC to endpoint network for translation.
VoIP-to-VoIP	VoIP-to-VoIP would be carried to [redacted] and hair-pinned back to VoIP.

Table 1.4.15.6-1: Call Type Routing for VoIP. *The carrier CIC is selected using the Agencies' preferred inter-exchange carrier (PIC) for 700 number services.*

identification code (CIC). **Table 1.4.15.6-1** describes how the 700 number calls are routed with respect to the VoIP service.

1.4.15.6.2.1 Incoming-to-VoIP

Calls made to a specific 700 number are routed to AT&T from another carrier or from the AT&T circuit switched voice service as part of the [redacted] code specific routing. Once it has been determined that AT&T is the carrier of termination, the call is translated to a specific public telephone number and routed appropriately. If the final call destination is located in the VoIP network, the circuit switched network passes the call to the VoIP network, using its public telephone number as the call destination.

1.4.15.6.2.2 VoIP-to-Outgoing

Calls to a 700 number made from AT&T VoIP telephones are first handled by the CCE and the IP Centrex systems. These systems determine which carrier should handle the call, based on Agency PIC information. The call is then passed to the appropriate carrier through the PSTN gateway. The call is handled by the selected carrier, based on that carrier's 700 code routing rules.

1.4.15.6.2.3 VoIP-to-VoIP

The VoIP network is a local exchange and does not route 700 numbers internally. However, calls to an AT&T-provided 700 number that are made from inside the VoIP network will be passed to the [redacted] within AT&T. These calls could be hair-pinned back into the VoIP network after number termination translation is completed.

1.4.15.6.3 PSTN Gateways [C.2.7.10.1.4 (3)]

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:
3. The contractor shall provide gateway's for interoperability with IPTelS and the PSTN, or with Agency UNIs.

Voice over IP services from AT&T are served over an access link that includes a VPN to the [redacted] through a [redacted] The VoIP network contains call-routing logic, advanced services features, and access to a [redacted] The traditional AT&T voice network to provide 100-percent PSTN coverage carries the remainder of the PSTN access.

Refer to Section 1.3.3.f for a more complete description of the AT&T VoIP to PSTN interconnect strategy.

1.4.15.6.4 Routing Priority [C.2.7.10.1.4 (5)]

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:
5. The contractor shall provide a routing prioritization scheme or class of service.

The access links for the AT&T VoIP services are constructed using VPNs that are carried to the network core with CoS markings for most packets. At the edge of the network, the packets are classified and marked by application type for differentiated routing in the network [redacted] (**Figure 1.4.15.6-3**).

Figure 1.4.15.6-3: Differentiated Services [redacted]

[redacted] typically assigned as follows:

[redacted]

[redacted]

[redacted]

Packet traffic is classified with the CoS tags at the customer premises router. The customer premises router, through extended access lists, identifies the voice traffic using the transmission control protocol (TCP), user datagram protocol (UDP), the network of origination, application port, or socket.

Once classified, the network routers act on the marked packets, according to their level of criticality. [redacted] **Figure 1.4.15.6-4** depicts the classification of packets and the DiffServe routing engine process.

Figure 1.4.15.6-4: VoIP Packets [redacted]

Unlike our competitors, AT&T provides CoS across our IP VPN, not just at the edge of the network. This offers true end-to-end QoS to our customers and provides a suitable environment for IP voice and converged services.

Refer to Section 1.3.2.e for more details on the overall network routing priority system used in the AT&T networks.

1.4.15.6.5 Station Mobility [C.2.7.10.1.4 (6)]

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:

6. The contractor shall provide the capability to support station mobility.

Table 1.4.15.6-2 lists the typical options used in supported mobility.

MOBILITY	
Inside Office	Allows users to move phones within office where new IP address could be required. This allows users to move their telephone, without technical support form telecommunications team.
On Cable and DSL	Networks that change their addressing dynamically are supported by VoIP system using station mobility.
For Traveling Users	Users can access VoIP network from broadband network at hotel or outside office.

Table 1.4.15.6-2: Mobility Options with IPTelS. *Users access service at the home office, working from home, or while on the road.*

Each station within AT&T voice DNA service is IP address agnostic. When a station first comes online, it registers with the VoIP network, using station-specific information, along with the locally assigned IP address. The IP address, which can be any address within the range of addresses for the VPN connected service, is associated with the station for the time it is registered with the network. Changes in address are simply reflected as changes in registration.

1.4.15.6.6 Agency Firewall Traversal [C.2.7.10.1.4 (8)]

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:
8. The contractor shall verify with the Agency that the Agency firewall is compatible with the contractors' service.

In processing packets for security, VoIP packets pose a particular problem in that the processing delay of the firewall can acutely affect the quality of the calls passing through it. Due to the industry move towards services over IP, many newer firewall devices are being produced with VoIP capabilities. Given the differences in existing and new firewalls, AT&T has tested the following brands and types of firewalls, shown in **Table 1.4.15.6-3**, and approved usable firewall configurations for VoIP applications.

AT&T will verify with the Agency that the premises-based firewall is capable of supporting our VoIP service. This will be accomplished at the requirements determination phase of the project. In addition to verifying and certifying the capability of the router, we will provide expert advice regarding firewall policies and configuration to verify that the firewall supports the VoIP functionality before implementation.

FIREWALL APPROVAL		
Manufacturer	***Model/Platform***	***Capability***
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]		

Table 1.4.14.6-3: Approved Firewalls Work with VoIP. *AT&T has tested several firewalls for use with the VoIP suite of products. Approved, managed firewalls allow VoIP packets to operate in the network without excessive delay or other impairment.*

1.4.15.6.7 Security Practices [C.2.7.10.1.4 (11)]

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:
11. The contractor shall ensure security practices and safeguards are provided to minimize susceptibility to security issues and prevent unauthorized access.

AT&T provides Agencies with the best possible IP network security using the seven elements listed in **Table 1.4.15.6-4**.

ELEMENT	FUNCTION
Separation	Customer traffic is separated using MPLS VPNs.
Automation	Automated perimeter security tools protect MPLS core.
Monitoring	IP traffic monitoring provides early warning of Internet viruses and worms.
Control	Strict operational security controls are enforced in MPLS core and on-service application platforms.
Testing	Testing, auditing, and reviewing all ensure security compliance.
Response	Proactive response teams trained in details of networks and security are deployed to places of potential attack or risk.
Innovation	AT&T funds extensive security research.

Table 1.4.15.6-4: AT&T Uses Seven Basic Security Elements to Provide Security across All Products. *Most security tasks or features fall within these seven core security concepts.*

Using these elements, along with monitoring and threat elimination tools, AT&T has been able to detect and stop attacks for its customers, while customers of other network providers simply had to weather the storm. (Refer to Section 1.3.1 for a complete description of these elements and the overall network security practices.)

In addition to the overall network security practices outlined above, AT&T secures IP and traditional PBX equipment with the SIP VoIP network security model (**Figure 1.4.14.6-5**).

Figure 1.4.15.6-5: AT&T Security Based on [redacted]

[redacted] provides proxy authentication for the Agency PBX. This allows Agencies to use the service securely, even if the equipment that possess is not an IP-ready PBX. Since the remainder of the VoIP network is a closed MPLS environment, Agencies do not need to monitor or manage the security aspects of the remainder of the network. Finally, AT&T monitors all of its IP networks for activity anomalies. This monitoring helps detect attacks and the setup of attacks before the actual attack occurs. This allows AT&T response teams to thwart most attacks before they affect the service. Refer to Section 1.3.1 for more information on attack mitigation through monitoring.

1.4.15.6.8 Security Updates [C.2.7.10.1.4 (11)]

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:
11. The contractor shall ensure security practices and policies are updated and audited regularly.

AT&T employs [redacted] who are responsible for network and systems security and who perform the functions listed in **Table 1.4.15.6-5**.

JOB SPECIALTY	JOB FUNCTIONS
Standards work	Following standards, tracking threats, and making industry-wide recommendations
Design	Ensuring that security is designed into every component of every product
Management	Managing security best practices in service deployment
Testing	Laboratory testing of systems for vulnerability
Monitoring	Monitoring system against threats or changes in operation that could indicate a new threat
Action	Managing threats and mitigating attacks through response team action
Assessments	Assessing new security threats and protection mechanisms for emerging products, such as VoIP

Table 1.4.15.6-5: AT&T Security Personnel Tasks. *The use of security professionals, along with designing security into every product, creates services that are secure when they are first deployed. Continuing vigilance keeps those products secure.*

Refer to Section 1.3.1 for an overall understanding of the AT&T security practices and how they are updated.

1.4.15.6.9 Denial of Service [C.2.7.10.1.4 (11)(a)]

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:
a. Denial of service – The contractor shall provide safeguards to prevent hackers, worms, or viruses from denying legitimate IPTelS users and subscribers from accessing IPTelS.

The primary defense against denial of service (DoS) attack, worms, viruses, and hackers is the separation of networks (outlined in Section 1.3.1). Using this separation scheme, the VoIP network, although interconnected to other networks on secure BEs, routes as an independent MPLS network. The core network is invisible to the Internet. In addition to being hidden from the Internet, customer networks cannot freely route to other customer networks, as depicted in **Figure 1.4.15.6-6**.

Figure 1.4.15.6-6: Network Separation Security Defense. [redacted]

Using AT&T VoIP services, Agencies are also protected from internal threats by the VoIP specific security architecture (**Figure 1.4.15.6-5**). In addition to the nine points of security outlined in this graphic, AT&T also follows a strict practice of securing every system in the network through a process of system hardening, as described in Section 1.3.1.

1.4.15.6.10 Intrusion [C.2.7.10.1.4 (11)(b)]

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:
b. Intrusion – The contractor shall provide safeguards to mitigate attempts to illegitimately use IPTelS service.

The security that is built into the AT&T network automatically protects against intrusion threats. **Table 1.4.15.6-6** lists the separate major elements of intrusion control within the AT&T VoIP network. These security mechanisms work in conjunction with the security mechanisms in the VPN service that provides access to the VoIP network.

MECHANISM	EFFECT ON INTRUSION
Separation of networks	Separation of networks makes it impossible for someone on a public network, such as Internet, to access VoIP network or any of its customers. Customer networks are shielded from each other as well.
Secure border edge	Secure border edge device creates VoIP signaling control point that requires authentication to pass signaling data. Since unauthorized signaling is not passed to call control units in interior of VoIP network, coupled with network separation, signaling access is only granted to authorized VoIP users. Interior systems will only accept signaling form authorized interior systems. Border edge is authorized gateway to interior.
Systems hardening	Every system in VoIP network is hardened, removing all unused IP ports and unnecessary OS and program functions. This eliminates use of functional block as intrusion stepping stone.
Systems security standards	Every system in network is operated under strict set of AT&T security standards. Refer to Section 1.3.1 for a complete description of AT&T system security standards.
Strong authentication	All legitimate systems access is authenticated using strong authentication and [redacted]. This control mechanism prevents outside access and logs all access as well.
Monitoring	All VoIP systems are continuously monitored for any access violation. Access violations create alarms and energize action from incident response team.

Table 1.4.15.6-6: Mechanisms to Secure VoIP Systems. *Agencies can depend on the systems and procedures that AT&T uses to protect against intrusion.*

For further details on the trusted security domains and protections against intrusion, refer to Section 1.3.1.

1.4.15.6.11 Invasion of Privacy [C.2.7.10.1.4 (11)(c)]

Internet Protocol Telephony Service capabilities are mandatory unless indicated otherwise:
c. Invasion of Privacy – The contractor shall ensure IPTelS is private and that unauthorized third parties cannot eavesdrop or intercept IPTelS communications.

Network protection against eavesdropping is supplied by the standard VoIP security mechanisms (**Table 1.4.15.6-7**). These security mechanisms are linked in their effectiveness to the Agency LAN eavesdropping protections.

AREA OF NETWORK	SECURITY MECHANISM
Access	Secure managed VPN service eliminates access from outside sources. Transporting IP in MPLS makes address spoofing impossible.
Signaling	Signaling is secured in BE and will only forward packets to an authenticated partner system. All call handling platforms are located in VoIP core and are secured using AT&T's systems hardening and strong authentication methodology.
VoIP Core	VoIP core is 100% MPLS routed. No IP access exists in the core. Access to core routers and elements is strictly controlled. Physical security is strong and follows telephone systems standards.

AREA OF NETWORK	SECURITY MECHANISM
Agency LAN	Best security practices in Agency LAN will provide like-for-like eavesdropping security with traditional telephone service systems. Strong internal physical security is also required.

Table 1.4.15.6-7: Wiretap Protection Mechanisms. *Protection against eavesdropping in the network is provided by a solid VoIP security model and practices.*

The industry standard deployment strategy for privacy is to deploy VoIP in a way that achieves invasion of privacy security that is like-for-like with traditional telephone service. VoIP telephones are no more easily tapped than a traditional telephone. If an Agency uses a switched Ethernet environment, and adequate physical and systems management controls are placed on the LAN switch equipment, then the VoIP service is as secure against eavesdropping as a traditional telephone service (**Figure 1.4.15.6-7**).

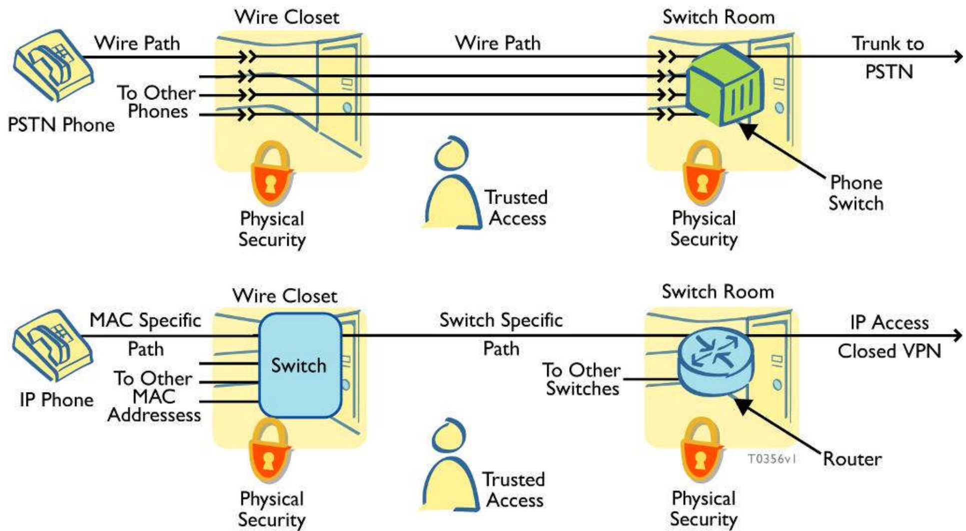

Figure 1.4.15.6-7: LAN Switch Configuration Protects VoIP Privacy. [redacted]

1.4.15.6.12 IP Telephony Service Interfaces [C.2.7.10.3.1 (1)]

UNI Type 1
Interface Type: Router or LAN Ethernet port: RJ-45 (Std: IEEE 802.3)
Payload Data Rate or Bandwidth: Up to 100 Mbps
Signaling Type: SIP, H.323, MGCP or
SCCP [Optional]

The Agency UNI Type 1, RJ-45 Ethernet 10/100, is provided as a standard interface on the SDP options listed below. The SDP is signaling independent and provides access to the first point of CoS routing and VPN termination. Router options are dependent on access methodologies, such as MPLS, asynchronous transfer mode (ATM), and frame relay. All configurations will be able to supply the 10/100 Mbps Ethernet interface in a signaling protocol agnostic manner. **Tables 1.4.15.6-8** and **1.4.15.6-9** list two examples of Ethernet interfaces available.

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

Table 1.4.15.6-8: T-1 Access and 100 Mbps Ethernet Port Interfaces.

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

Table 1.4.15.6-9: T-3 Access and 100 Mbps Ethernet Port Interfaces.

1.4.15.7 Stipulated Deviations

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