1.4.16 Converged IP Service (CIPS) [C.2.7.11]

Using the solution for converged Internet protocol (IP) services (CIPS), Agencies will be able to combine their access and transport operations for voice, video, and data transport using the AT&T IP virtual private network (VPN) products combined with the IP-Centrex solution. These products provide full-featured, business-grade telephone service over IP, and Agency data transport over a single-managed IP network for a high-quality operation at a lower cost.

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

1.4.16.1.a Approach to Service Delivery

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

The AT&T converged Internet protocol (IP) services (CIPS) is a combination of AT&T Virtual Private Network VPN (AVPN) services and the AT&T IP-Centrex offering. In addition to the IP-Centrex interoperability, the CIPS will also interoperate with onsite IP telephone switch systems, such as the Cisco Call Manager or Avaya IP-ready private branch exchange (PBX) systems. The IP-Centrex product supports IP telephones and offers Agencies a full set of PBX like features without the installation or maintenance of a PBX system.

As shown in **Figure 1.4.16.1-1**, using the AVPN, Agencies can build private networks that tie locations together, provide access to the Internet, use other legacy networks, and access VoIP services. Quality of service (QoS) is provided and controlled using a combination of Class of Service (CoS) packet marking, differentiated service priority routing, and multiple protocol label switching (MPLS). In addition, Agencies have the ability to monitor use.

Figure 1.4.16.1-1: CIPS Network Consists of VPN Services and Specialized Gateways. *Using AVPN, Agencies can transport video, access the Internet or other networks, and connect to VoIP services. Using the network based VPN service as a basis for CIPS allows each Agency location to connect in an any-to-any fashion and use the connectivity and services needed to accomplish Agency missions. The VPN service also provides CoS- based routing, which is maintained across specific gateways as needed.*

The approach to CIPS is described in **Table 1.4.16.1-1**.

SERVICE DELIVERY APPROACH	DESCRIPTION
Standards Compliance	• The service is delivered based on a set of IETF, ITU-T, IEEE and NIST standards
Multi-protocol Label Switching (MPLS) enabled VPN	• AT&T's AVPN solutions provide Agencies with IP/MPLS-enabled network-based VPN that extends quality of core network to customer premises equipment (CPE).
Managed service	[redacted]
Integrated security	• Security is built into every part of AT&T network. This whole network approach to security makes every part of Agencies operation more secure. • Defined security policies and practices the safe guard denial of service attacks, intrusion, and invasion of privacy • For a detailed discussion of our security architecture, refer to Section 1.3.1.
Large footprint	• The VPN service is available in over 48 countries and non-domestic locations.
Class of service routing	• Time-sensitive data, such as voice and video, are assigned a higher class of service as they enter VPN and are given routing priority in network. • Provides end-to-end quality within VPN or when using the AT&T VoIP network to gain access to public switched telephone network (PSTN).
VoIP Ready CPE and network	• The VPN and termination routers are VoIP ready. • Can be configured with local area network (LAN) interfaces to connect to IP telephones, IP PBX systems, to traditional PBX systems, or combinations of communications systems.
IP Centrex Service	• Features and services that are usually provided by onsite PBX are now available from IP Centrex within AT&T VoIP network. • Allows Agencies to deploy phones and add features without having to purchase or maintain PBX system.
Service management portal	• Agencies are able to monitor and manage AT&T IP VPN and VoIP services using AT&T's **Business**Direct® web portal.
Can be integrated with other AT&T VoIP products	• VoIP service can be combined with VoIPTS to create mixed use environment or to augment features of existing PBX.

Table 1.4.16.1-1: CIPS Is Created Using Several Integrated Network Features and Components. *Using the AT&T VoIP network, coupled with the VPN services, Agencies receive a service that is complete and reliable.*

The AT&T VoIP/IP Centrex offer provides complete PBX-like features to session initiation protocol (SIP)-based telephones at Agency locations through the VPN link and a set of VoIP gateways. PSTN access, including fully functional 911, E911, operator/directory services, and [redacted] are part of the service. Complete information on the VoIP and IP-Centrex service is provided in Section 1.4.15, IP Telephone Service (IPTelS).

1.4.16.1.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).

The advantages of the CIPS are from the ability to use the fully managed VPN service for multiple Agency applications. **Table 1.4.16.1-2** describes the major benefits of the CIPS.

SERVICE DELIVERY APPROACH	BENEFITS	FEA FACILITATION
Multi-protocol Label Switching (MPLS) Enabled VPN	• The IP/MPLS based AVPN solutions provide Agencies with service agnostic transport • Supports quality of service routing that extends to the CPE • Provides any-to-any connectivity within the VPN with no need for PVCs • Takes full advantage of the high bandwidth AT&T core network	FEA Link: TRM/Service Access and Delivery/Service Transport/Supporting Network Services
Managed service is monitored by AT&T	• Service is offered to Agencies as fully managed service. • AT&T Network Operations Center (NOC) and product management operations center monitor the service for alarms, errors, security, packet forwarding performance problems, and usage issues.	FEA Link: TRM/Component Framework/Data Management/Reporting and Analysis
Integrated Security	• Security is built into every part of AT&T network. • The whole network approach to security makes every part of Agencies operation more secure. • For a detailed discussion of our security architecture, refer to Section 1.3.1.	FEA Link: TRM/Component Framework/Security
Large VPN Footprint	• The VPN service is available in over 48 countries and non-domestic locations.	FEA Link: TRM/Service Access and Delivery/Service Transport/Service Transport
QoS is geared toward packet voice	• CIPS is has been designed to carry time-sensitive traffic, such as VoIP and video. • Agencies receive the best possible call quality though VoIP specific routing	FEA Link: TRM/Service Access and Delivery/Service Transport/Supporting Network Services
VoIP Ready Network and CPE	• Agencies are better able to transition to VoIP through systems that support multiple topologies.	FEA Link: TRM/Service Interface and Integration/Interface/Service Delivery
Service Management Portal	• Agencies are able to manage and track their own service usage. • Service statistics are available on access as well as links into control and provisioning of IP-Centrex service. • Refer to Section 1.4.16.2.b for more information.	FEA Link: TRM/Component Framework/Data Management/Reporting and Analysis
Can be integrated with other AT&T VoIP products	• AT&T CIPS allows Agencies to take advantage of new VoIP technology and off the shelf IP Phones without building unique solutions or dedicated networks. • The service can be combined with other VoIP to create mixed use environment or to augment features of existing PBX.	FEA Link: TRM/Service Interface and Integration/Enterprise Application Integration

Table 1.4.16.1-2: CIPS Benefits come from Several Network Sources. *The benefits received by the Agencies are designed into the VoIP network.*

Single access strategies are easier to manage and grow than multiple access strategies. This service is also monitored in the AT&T NOC as well as in the product management operations center for alarms, errors, security, packet forwarding performance problems, and usage issues. Service statistics are available to Agencies on the CIPS use, as well as available links into the control and provisioning of the IP telephone service. The network's performance is also guaranteed through Service Level Agreements (SLA).

1.4.16.1.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 projects.

Table 1.4.16.1-3 lists the top eight service delivery risks and our mitigation strategy. As with all large, combined services 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	ISSUE	MITIGATION
Requirements changes	Requirements changes before and after service delivery contribute to budget overruns, schedule slips, and missed expectations.	• Obtain pre-project understanding of requirements through detailed analysis • Establish strong change management processes • Conduct continuous communications with GSA and Agencies.
Complete and accurate +Location information	Often, location information is not accurate and site Point-of-Contacts (POCs) are no longer valid.	Review and verification of location information with Agency Program Management Office (PMO) and site POC.
Business disruption	In our experience, all Agencies are concerned about business disruption when moving to a managed service. Adequate planning can minimize this risk.	• Develop engineering design that considers equipment replacement, concurrent operations, and bake-in period • Lab test all service delivery processes and procedures • Possess detailed backout procedures

RISK	ISSUE	MITIGATION
		• Conduct delivery activities during no-business hours, as directed by Agency site POC.
Schedule slippage	Many issues can contribute to schedule slippage; having a detailed project schedule can minimize this risk.	• Develop detailed project schedule • Identify activity dependencies and resource allocation • Use jeopardy escalation processes liberally.
Training	The new service could require some specific training on use of features.	AT&T Government Solutions provides familiarization and feature training on a case-by-case basis. In addition, Agency telephone system administrators can receive support to assist with changing aspect of automatic call distribution and private dialing plans. This support helps Agencies realize full potential of their new telephone service.
Performance issues	By adding new applications in a converged environment, traffic patterns will change, possibly contributing to performance degradation.	• Provide design and engineering services to ensure that traffic patterns are understood • Offer managed network service to provide appropriate level of performance management to identify issues and forecast potential issues.
Access	An increase in number of telephones or increase in telephone or data transport usage could oversubscribe transport. This could cause transport needs, which might not be met during high-call volume or data intensive functions.	AT&T works with Agency to design access with correct amount of overhead bandwidth to provide that services will operate at acceptable level of quality. Reassessment can be provided as needs of Agency change. Agencies have access to usage data through web portal so that they can track growth.
LAN configuration	Agencies will be required to manage their LANs with high-availability, security, and usage of telephone network, compared to LANs that are used only for data.	AT&T provides design and engineering solutions for Agency LANs through Customer Specific Design and Engineering Solutions (CSDES) (Section 1.5.8).

Table 1.4.16.1-3: Planning and Training can be Issues with VoIP. *AT&T provides services on an individual case basis to help Agencies with problems that can occur when deploying CIPS.*

1.4.16.1.d Network Architecture Synchronization

(d) Describe the synchronization network architecture to support the offeror’s access and transport networks.

Synchronization begins with the primary reference radio signal broadcast by the Federal Government. The AT&T digital hierarchy then derives its clock from a series of [redacted] primary clocks with rubidium oscillator-based time standards with an accuracy of 1x10^{-13}. CIPS derives its synchronization from the synchronous optical network (SONET) infrastructure on which those services ride. Network synchronization is provided at each central office on T1 facilities. More detailed discussion is provided in Section 1.3.6.1, Network Architecture Synchronization.

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

1.4.16.2.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.

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.

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 (TTR)	Without dispatch	4 hr	[redacted]
	With dispatch	8 hr	[redacted]
[redacted]			

Table 1.4.16.2-1: AT&T's Performance Levels Exceed Minimum Requirements. *The performance of the network supports applications such as VoIP.*

Table 1.4.16.2-1 lists typical core month-by-month network performance, as compared to the requirements set forth in the RFP.

The use of MPLS exclusively in the AT&T VoIP core, combined with high-capacity inter-router links, gives VoIP packets 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 good sound quality and high call-completion rates. AT&T VoIP network call quality, as compared to a typical IP network, such as the Internet, is shown in **Figure 1.4.16.2-1**.

The combination of performance parameters in the AT&T VoIP network helps produce a level of VoIP call satisfaction that has a mean opinion score (MOS) of 4.0 or higher for G.711 codecs.

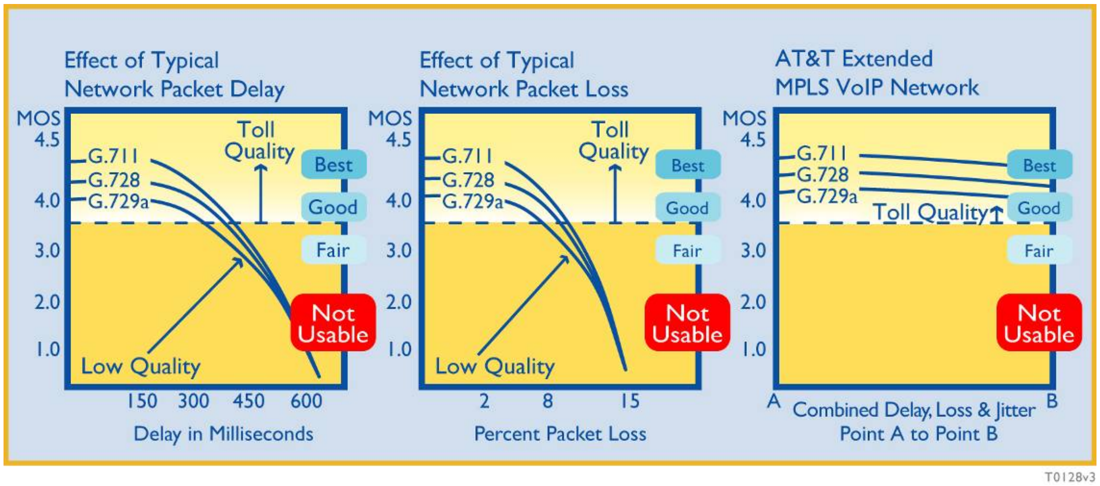

Figure 1.4.16.2-1: AT&T VoIP High-Quality Performance. *Excessive packet loss, delay, or jitter can affect overall call quality. The AT&T VoIP network carefully controls impairments to supply a higher quality VoIP service.*

1.4.16.2.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. 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 data would follow. **Table 1.4.16.2-2** outlines the methods used to measure the various IP key performance indicators.

KEY PERFORMANCE INDICATOR	APPROACH TO MONITORING AND MEASURING
Ability to measure network and service specific metrics	Using the Product Management Operations and Support System (PMOSS), AT&T monitors both network metrics and service metrics and correlates those metrics to a specific service and service event (e.g. a telephone call).
Availability measured (service delivery point [SDP]-to-SDP)	Measurement is performed in both the core network and in the edge and VPN networks.

KEY PERFORMANCE INDICATOR	APPROACH TO MONITORING AND MEASURING
Time to Restore (TTR)	AT&T One Ticket System (AOTS) performs the following functions: • Captures trouble ticket data for all services, including voice services • Provides TTR to Government through AT&T **Business**Direct portal.
[redacted]	ITU-T G.107-based call quality measurement systems are used to provide quality measurements on a call by call basis.

Table 1.4.16.2-2: Monitoring and Measuring CIPS. *Agencies can easily manage the CIPS service with easy to access and use data delivered through the AT&T **Business**Direct web portal.*

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 1.4.16.2-2**.

Figure 1.4.16.2-2: Management Network [redacted]

Using the dedicated management network service, performance is monitored and displayed in units that are appropriate for each product. Agencies are provided access to the performance data, using links within the AT&T **Business**Direct portal. For additional details, see Section 1.3.2.c.

1.4.16.2.c Performance Level Improvements

(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.

The AT&T core network is based on MPLS routing between all entry and exit points and includes the network based VPN products as well as the VoIP core network. 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 1.4.16.2-3** 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]

Table 1.4.16.2-3: [redacted] Performance Specifications. [redacted]

Using the MPLS core network with the above set of packet performance criteria, VoIP calls can rival the quality of PSTN calls and video is transported cleanly. In VoIP, this quality applies to both the speech quality and call completion rate, as 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 network 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.

1.4.16.2.d Rationale and Benefits for Additional Performance Metrics

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

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 **1.4.16.2-4**.

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

PROPOSED KPI	DESCRIPTION OF PROPOSED KPI	BENEFIT OF PROPOSED KPI
R-Factor	Single performance metric that captures VoIPTS quality by measuring three network performance metrics: network latency, packet loss, and jitter.	• Provide both aggregate and call-by-call view of VoIPTS quality • Single performance indicator provides service quality • Easily translates to mean opinion score (MOS) voice quality scale

Table 1.4.16.2-4: Performance Level Improvements. *Incorporating the proposed KPI into the VoIPTS provides comprehensive performance monitoring, allowing Agencies to migrate to performance-based contracts sooner.*

R-Factor is the specified output for the ITU-T G.107 packet voice measurement standard that quantifies quality based on three major network factors: (1) *latency*, which measures one-way transit across the network; (2) *packet loss*, which includes late and lost packets, and (3) *jitter*, which is the inter-arrival rate between voice packets. These three factors are measured as a function of their additive effects on the codec in use to determine relative voice quality. R-Factor is highly correlated with mean opinion score (MOS), another industry voice quality standard (**Figure 1.4.16.2-7**).

Figure 1.4.16.2-3: Call [redacted]

By monitoring the call quality, more information is gained about actual call performance than by just monitoring packet loss, jitter, and latency independently. In addition, monitoring call quality at every edge point gives a directional indicator as to which network or component is at fault for a poor quality call.

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

1.4.16.3.a Service Description

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

CIPS is a VPN and VoIP combined service that allows Agencies to interconnect sites, connect to the Internet and extranets, and transport time-sensitive packet traffic such as voice and video. **Figure 1.4.16.3-1** shows the basic configuration of a CIPS network and its key components.

The VPN portion of the service is based on MPLS, which allows the network to transmit standard IP-based data packets from any location to any location on a short, predetermined path without using private virtual connections (PVC). This gives Agencies a network that acts like a dedicated, purpose-built IP network with any-to-any connectivity within the VPN.

Figure 1.4.16.3-1: [redacted] **and** [redacted]

Agencies looking for simplified, fully meshed communications and the ability to use a variety of VoIP and video services, have a simple solution that gives them the private network needed with access to external networks, such as the AT&T dynamic network application (DNA), for services such as VoIP.

The MPLS-enabled VPN uses multiprotocol-internal border gateway protocol (MP-iBGP) to exchange customer-specific routing information. MP-iBGP enables VPN specific characteristics to be transported end-to-end between MPLS-enabled routers. The MPLS-based VPN enforces traffic separation among Agencies by assigning a set of customer ports to a unique virtual network routing and forwarding (VRF) table. Only pre-assigned ports are allowed to participate in the VPN. These participation ports can include other Agency locations as well as such services as VoIP and secure Internet access. The combined VPN and VoIP service also includes the service elements listed in **Tables 1.4.16.3-1** through **1.4.16.3-4**.

VPN FEATURES

Service Element	Description	Benefits to Agency
Transport independent	Provides secure any-to-any connectivity using MPLS technology independent of access technology.	Agencies can use this service for connectivity to many networks and services: • Interoffice data VPN • Voice Networking • ATM/Frame Relay • Internet Access
QoS routing for time-sensitive traffic	Using CoS marked packets, VPN service routes higher CoS packets with higher forwarding priority	Agency voice and video traffic is delivered with the quality required to use each service.
Gateways to and from VPN	Provides gateways to other networks, such as Internet and VoIP networks, including PSTN gateways on VoIP network.	The service is secured without requiring PVCs or cumbersome encryption schemes
Interfaces	• 802.3 10/100/100 Mbps Ethernet • 802.3 10GbE Ethernet	Agencies can select the interface and bandwidth needed to support the Agency's functions and missions

Table 1.4.16.3-1: VPN Service for CIPS. *Agencies can use the VPN service for VoIP service and a variety of data applications.*

VOIP NETWORK FEATURES

Service enabling device (SED) support	Supports different telephone devices, including SIP IP telephones, IP and traditional PBX systems, and analog terminal adapters (ATA).	Agencies can use a variety of devices to provide workers with the communications capabilities needed to accomplish their missions
PSTN access	Offers nationwide PSTN access for incoming and outgoing calls, with IP to PSTN address conversion built into network. Local number assignment [redacted]	Agencies can make or receive calls without changing dialing plans or calling habits of workers
911 support	Access to public safety answering point (PSAP) location with proper data exchange [redacted].	Agencies will not need to alter their calling habits or create new work around scenarios for emergency situations
Operator services (OS) and directory assistance (DA)	OS and DA access is built into VoIP network.	Agencies will not need to alter their calling habits and can continue to use local informational services.
CALEA Support	[redacted]	[redacted]

Table 1.4.16.3-2: VoIP Features to Augment the VPN. *Using AT&T's full-featured VoIP service allows Agencies to provide workers with telephones having business features without having to deploy PBX equipment.*

ONLINE SUPPORT TOOLS

Enhanced customer reporting	[redacted] • Site-to-site performance and reliability – delivery reports by cos [redacted]	Agencies can manage their own serivce using the same data that AT&T uses in the NOC [redacted] work centers

ONLINE SUPPORT TOOLS		
	[redacted] VoIP Reporting	
VPN snapshot	Topology Maps	Agencies can view their network topololgy, understand management data, and plan for augmentations.
Electronic (MACD)	Provides the ability for the customer to perform electronic moves, adds, changes and delets (MACD)	Agencies can manage and augment their service without time consuming third party involvement.

Table 1.4.16.3-3: Online Support for VoIP Management. *Agencies will be able to manage their CIPS service using a variety of tools and data that are accessed through the Business Direct portal.*

SECURITY		
Network-based firewalls	VPN service works in conjunction with AT&T network-based firewall services that protect against attacks, intrustion, worms, and viruses	• Agencies networks are secured without having to install and maintain security devices • Security system sensitive protocols are more easily transported throughout the VPN
Secure and reliable	AS layer provides secure environment with network and system redundancy for all AS processors. Processors are monitored by AT&T 24x7 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 • Data transport to servers and applications is dependable

Table 1.4.16.3-4: VPN Service Security. *Agencies can count on the security of the VPN-based services as AT&T follows strict security guidelines for network based products.*

Refer to Section 1.4.13 for more information on the AT&T network-based VPN service.

The VoIP service is based on the AT&T IP Centrex offer and is built into the VoIP network. As part of the VoIP network; the IP Centrex, IP conferencing, and VoIP messaging advanced service modules provide the basic calling features for VoIP customers. The basic calling features are listed in **Table 1.4.16.3-5.**

BASIC CALLING FEATURES				
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]	[redacted]

Table 1.4.16.3-5: Basic Calling Features. [redacted]

The VoIP service network is accessible from the VPN service and contains four distinctive layers (**Figure 1.4.16.3-2**). These four layers control access, provide security, route calls to and from the PSTN, and apply features to the telephone service.

Figure 1.4.16.3-2: [redacted] **Operating Areas.** [redacted]

For more information on the IP telephone service features, refer to the description of IP telephone service in Section 1.4.15 and associated J tables.

1.4.16.3.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.

This service will exceed the basic telephone service requirements outlined in the RFP. The telephone service offered in CIPS will match the full set of requirements outlined in Section 1.4.15, IP Telephone Service (IPTelS), and associated J tables.

1.4.16.3.c Service Delivery Network Modifications

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

No modifications to the AT&T VPN or voice DNA network are required to provide Agencies with a high-quality converged voice and data service.

1.4.16.3.d Transport/IP/Optical Service Experience

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

[redacted]

Table 14.16.3-6 cites examples of AT&T's ability to deliver managed services.

Large Manufacturing Customer

CLIENT NEED	SOLUTION	CREATE VALUE
[redacted]	[redacted]	[redacted]

Large Travel Company

CLIENT NEED	SOLUTION	CREATE VALUE
[redacted]	[redacted]	[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Table 1.4.16.3-6: Experience Delivering Converged Services. *AT&T measures success by our ability to deliver solutions to our customers that create value to their business.*

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

1.4.16.4.a Network Traffic Utilization

(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 buildout contemplated.

Per the usage numbers supplied by the GSA for Networx, calculation of the total equivalent numbers of DS0s and peak bandwidth consumption is provided in **Table 1.4.16.4-1**.

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]
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]

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

Table 1.4.16.4-1 [redacted]

The AT&T IP network supports the transport and delivery [redacted] The additional load that would be added to the network for CIPS [redacted] 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.

1.4.16.4.b System Robustness and Resiliency

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

Rigorous engineering practices and measurements of the network allow Agencies to obtain a scalable, reliable service to build and operate their mission-critical applications. IP service and backbone capacity planning within the IP network are driven by three main factors (**Table 1.4.16.4-2**).

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	Capacity for planned technology migrations and insertions are built into system before migration is started.
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 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 1.4.16.4-2: Key Capacity Planning Factors. *Network capacity buildout is based on both predictive and measured data. AT&T strives to provide 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.

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

1.4.16.5.a Approach to Optimizing IP-based and Optical Services

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

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.

1.4.16.5.b Network Architecture Optimization

(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.

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.

1.4.16.5.c Optimizing Engineering Techniques

(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).

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.

1.4.16.5.d Vision to Implement Service Internetworking

(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.

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.

1.4.16.6 Narrative Text Requirement

1.4.16.6.1 Non-Domestic Coverage [C.2.7.11.1.3]

The contractor shall provide CIPS for domestic locations and it is optional for non-domestic locations.

The CIPS service from AT&T is provided in domestic locations where AT&T will either provide NANP telephone number assignment or use local number portability (LNP) to move number routing to the proper carrier. All CIPS data services are available in domestic locations as well. AT&T will also provide optional coverage for non-domestic locations and supports the VPN service to those locations that can be used for CIPS. Due to the licensing and regulations of non-domestic locations, numbers, and dialing plans for non-domestic locations are limited to extensions of covered North American Numbering Plan (NANP) domestic locations. On a case-by-case basis, custom SEDs that support non-domestic numbering plan call termination into foreign postal, telephone, and telegraph (PTT) or carrier through traditional interconnects (e.g., E-1 integrated services digital network (ISDN) links) can be engineered into the service. For coverage information of non-domestic locations and capabilities, refer to Section 1.3.4.

1.4.16.6.2 Routing Priority [C.2.7.11.1.4 (2)]

The following Converged IP Services capabilities are mandatory unless marked optional.
2. The contractor shall provide a routing prioritization scheme or class of service to distinguish between applications that require real-time (or high priority) treatment over near, or non real-time applications.

The access links for the AT&T VoIP services are constructed using VPNs that are carried to the network [redacted]

The CoS is typically assigned, as listed in **Table 1.4.16.6-1**.

Once classified, the network routers act on the marked packets, according to

CLASS OF SERVICE

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

Table 1.4.16.6-1: [redacted] **of** [redacted] *with a higher priority.*

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.

their level of criticality. [redacted] **Figure 1.4.16.6-1** depicts the classification of packets and the DiffServe routing engine process.

Figure 1.4.16.6-1: VoIP Packets [redacted]

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

1.4.16.6.3 SEDs and Gateways [C.2.7.11.1.4 (5)]

The following Converged IP Services capabilities are mandatory unless marked optional.
The contractor shall provide gateways and/or service enabling devices, where required, (a) for protocol conversions, (b) to interface with the contractor's CIPS network or (c) for access to external networks.

Protocol conversion, gateways, and access to external networks are built into the network-based VPN service. **Table 1.4.16.6-2** lists gateways that could be part of an Agency VPN plan.

DEVICE	FUNCTION
Customer edge (CE)	Routing interface is included to allow customer networks and protocols to interface with AT&T MPLS routing infrastructure.
Border edge (BE)	Provides access to VoIP network, performs protocol conversion, and applies VoIP security.
ATM/Frame gateway	Supplies protocol conversion and gateway services from MPLS to asynchronous transfer mode (ATM) or frame relay. This works in conjunction with CE.
Internet gateway	Provides gateway services from MPLS to Internet. This works in conjunction with IP interfaces on CE as well as network-based security products and systems.

DEVICE	FUNCTION
Provider edge (PE)	Provides on-ramp from access network to MPLS core.

Table 1.4.16.6-2: Access Diversity with VPN Services. *The variety of gateways supplies Agencies with access to several network types.*

Figure 1.4.16.6-2 shows the placement of the gateways and protocol converters within the VPN model.

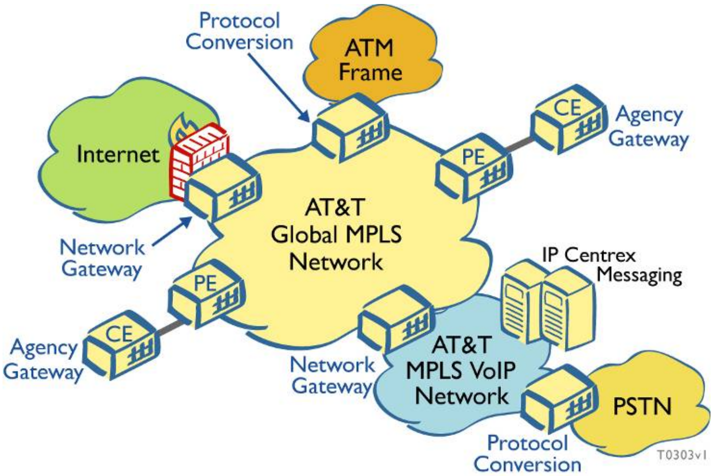

Figure 1.4.16.6-2: Gateways Provide Access to Other Networks. *Using the AT&T VPN service, Agencies have access to gateways that include VoIP networking and Internet.*

1.4.16.6.4 Network Capacity [C.2.7.11.1.4 (6)]

The following Converged IP Services capabilities are mandatory unless marked optional.
6. The contractor shall ensure adequate network capacity to deliver CIPS service for the subscribing Agency.

Overall network bandwidth capabilities are described in Section 1.4.16.4.a as well as in Section 1.3.2.c. In addition to the overall network capacity, Agencies have control over their own access capacity through the selection of several rate- shaping plans (**Table 1.4.16.6-3**), which are created by the systems described in Section 1.4.16.2. Table 1.4.16.6-3 lists the typical VPN

BANDWIDTH SELECTION

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

Table 1.4.16.6-3: Support Options for Multimedia Transport. *Agencies can select the bandwidth needed for each CoS to pass data, make calls, and conference in video.*

CoS data allocation amounts for high and low multimedia usage. Depending on the access bandwidth available and the applications support needed, CIPS can be tailored to Agency needs.

AT&T engineering will assess the needs of the Agency and make recommendations as to the total bandwidth need and the CoS priority percentage configuration. These settings and bandwidths can be reassessed and modified over time to suit changing Agency needs and missions.

1.4.16.6.5 Utilization Statistics [C.2.7.11.1.4 (8)(b)]

The following Converged IP Services capabilities are mandatory unless marked optional.
b. Utilization statistics

Usage statistics for the CIPS are collected and correlated with the EMS elements and [redacted], as described in Section 1.4.16.2.b. Usage statistics data is available for Agencies through the AT&T **Business**Direct portal. Typically available statistics are listed in **Table 1.4.16.6-4**.

PERFORMANCE INFORMATION AND USAGE STATISTICS

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

PERFORMANCE INFORMATION AND USAGE STATISTICS	
[redacted]	[redacted]

Table 1.4.16.6-4: [redacted] of [redacted]

An example of the concurrent or simultaneous calls available as AT&T **Business**Direct output is shown in **Figure 1.4.16.6-3**. The number of calls is given in time of day slots and equates to specific call bandwidth usage.

Figure 1.4.16.6-3: The AT&T BusinessDirect [redacted]

1.4.16.6.6 Active Directory [C.2.7.11.1.4 (13)]

The following Converged IP Services capabilities are mandatory unless marked optional.
13. The contractor’s CIPS shall be compatible and interoperate with Agency provided Active Directory services.

Components of the AVPN service and the IP-Centrex offer are not direct participants in an Active Directory network. The AVPN service supports and transports any Active Directory messages between networked sites. [redacted]

1.4.16.6.7 Agency Firewalls [C.2.7.11.1.4 (14)]

The following Converged IP Services capabilities are mandatory unless marked optional.
14. The contractor shall verify with the Agency that the Agency firewall is compatible with this service.

In AT&T's premise-based firewall services, [redacted] These firewalls represent the most commonly deployed types of firewalls. AT&T has tested and approved [redacted] managed firewalls for use with VoIP (**Table 1.4.16.6-5**). Work continues in AT&T Labs to test and approve other existing and future firewall types for use with VoIP services.

Other factors that need to be considered are call and data volume versus firewall sizing, site specific configurations, and possible network address translation (NAT) configurations. AT&T offers Agencies onsite firewall assessment and configuration through its Customer Specific Design and Engineering Services (CSDES) offer, which is discussed in Section 1.5.8.

TESTED/COMPATIBLE FIREWALLS	
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	
[redacted]	[redacted]

Table 1.4.16.6-5: Three Common Types of Firewalls Interoperate with VoIP. *AT&T has tested and approved firewalls and configurations to operate with VoIP services. Testing additional firewalls and configurations is a continuing effort.*

1.4.16.6.8 Security Safeguards [C.2.7.11.1.4 (15)]

The following Converged IP Services capabilities are mandatory unless marked optional.
15. 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 briefly outlined in **Table 1.4.16.6-6**.

ELEMENT	FUNCTION
Separation	Customer traffic is separated using MPLS VPNs.
Automation	Automated perimeter security tools protect the MPLS core.
Monitoring	IP traffic monitoring provides early warning of Internet viruses and worms.
Control	Strict operational security controls are enforced in the MPLS core and on-service

ELEMENT	FUNCTION
	application platforms.
Testing	Testing, auditing, and reviewing all maintain 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 1.4.16.6-6: AT&T Uses Seven Distinct Areas and Functions To Provide Security Across Its Networks. *These pillars of security are part of the best practices that keep Agency systems and transmissions secure.*

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 1.4.16.6-4**).

Figure 1.4.16.6-4: SIP [redacted] for [redacted]

1.4.16.6.9 Security Practices [C.2.7.11.1.4 (15)]

The following Converged IP Services capabilities are mandatory unless marked optional.
15. The contractor shall ensure security practices and policies are updated and audited regularly.

[redacted] who are responsible for network and systems security and who perform the functions listed in **Table 1.4.16.6-7**.

ACTION	ACTIVITY
Standards work	Following standards, tracking threats, and making industry-wide recommendations
Design	Making security a requirement to be designed into every component of every product
Management	Managing security best practices in service deployment
Testing	Laboratory testing systems for vulnerability
Monitoring	Monitoring system against threats or changes in operation that could indicate 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 1.4.16.6-7: AT&T's Security Personnel Functions. *Using a proven set of actions, AT&T provides Agencies with up-to-date security for the products they use.*

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

1.4.16.6.10 Denial of Service [C.2.7.11.1.4 (15)(a)]

The following Converged IP Services capabilities are mandatory unless marked optional.
a. Denial of service – The contractor shall provide safeguards to prevent hackers, worms, or viruses from denying legitimate CIPS users and subscribers from accessing CIPS.

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 thin 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 (**Figure 1.4.16.6-5**).

Figure 1.4.16.6-5: Invisibility to DoS Attacks. [redacted]

Using AT&T VoIP services, Agencies are also protected from internal threats by the VoIP-specific security architecture (**Figure 1.4.16.6-4**). In addition to the nine points of security outlined in the diagram, 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.

1.4.16.6.11 Intrusion Prevention [C.2.7.11.1.4 (15)(b)]

The following Converged IP Services capabilities are mandatory unless marked optional.
b. Intrusion – The contractor shall provide safeguards to mitigate attempts to illegitimately use CIPS service.

The security that is built into the AT&T network automatically protects against intrusion threats. The two main components of intrusion protection are the separation of networks and hardening of all network systems. The separation of networks acts to greatly reduce the number of possible potential risks to the number of elements within a subscribing Agency. The hardened systems are also a good security feature as they resist being used for intrusion attack launch points.

In addition to separation of networks and systems hardening, two more security features help resist intrusion. Each system that requires network access must pass AT&T security standards and is only accessed using terminal access controller access control system (TACACS+) and strong authentication rules. The border edge devices act to secure the network against intrusion as they allow only authenticated, VoIP signaling and service delivery point (SDP)-generated real-time protocol (RTP) to pass to authorized locations. For details on the trusted security domains and protections against intrusion, refer to Section 1.3.1.

1.4.16.6.12 Invasion of Privacy [C.2.7.11.1.4 (15)(c)]

The following Converged IP Services capabilities are mandatory unless marked optional.
c. Invasion of Privacy – The contractor shall ensure CIPS is private and that unauthorized third parties cannot eavesdrop or intercept CIPS communications.

The VoIP service standards organizations indicate that securing VoIP against eavesdropping should be accomplished using RTP stream encryption. However, the equipment industry has not been able to provide usable products with encryption in all aspects of a VoIP network.

With industry-standard deployment, VoIP achieves security against invasion of privacy 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 1.4.16.6-6**).

Figure 1.4.16.6-6: Like-for-Like Wiretap Resistance. *With the routing and LAN switching equipment secured in wiring closets, the potential wiretap points are limited to the same locations as a traditional telephone service. Proper LAN switch configuration must be maintained so that packets are delivered to only one unique mandatory access control (MAC) address in the LAN. The base functionality of a properly configured LAN switch eliminates the potential use of sniffing software to eavesdrop on a VoIP call.*

1.4.16.6.13 Encryption [C.2.7.11.1.4 (15)(d)]

The following Converged IP Services capabilities are mandatory unless marked optional.
d. Encryption and secure tunneling (VPN) at the Sensitive but Unclassified (SBU) through National Security Information (NSI) levels available under section C.2.10 Security Services and C.2.7.4 Managed Tier Security Services.

AT&T will offer a premises-based solution that will Internet protocol security (IPSec) encrypt all data traffic between locations while allowing unencrypted traffic, such as voice, to pass to a voice switching gateway. This is accomplished with our proposed converged solution.

Voice, although circuit switched, is not encrypted in “sensitive but unclassified” (SBU) solutions. Therefore, AT&T offers this same level of security in an SBU environment. If the Government requires voice encryption, AT&T has determined that security implementations between Government Agencies will vary. However, AT&T can develop a custom solution that will meet these requirements. This custom solution would consist of an IP PBX on the customer premises and premises-based encryption between locations.

1.4.16.7 Stipulated Deviations

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

1.4.16.8 CIPS with Managed Router Service

AT&T CIPS with Managed Router provides managed, “end-to-end” network VPN connectivity for Agencies who prefer complete vendor-provided solutions for their connectivity needs. [redacted] routers are provided by AT&T, configured by AT&T, installed at the Agency’s premises and monitored, managed, and maintained by AT&T. This service allows for additional managed application services such as VoIP to be added to the Agency network without providing additional termination equipment. [redacted]

Figure 1.4.16.8-1: [redacted]

In the CIPS with Managed Router configuration AT&T performs the configuration, management and maintenance function for the IP termination equipment. Out-Of-Band (OOB) access provides management [redacted]

1.4.16.8.1 Service Description

Under CIPS with Managed Router, AT&T provides, configures, monitors, manages and maintains the premise equipment necessary to use CIPS at each location in the Agency VPN, which generally consists of a router and a diagnostic modem. With CIPS with Managed Router, service demarcation occurs at the LAN port of the router. [redacted]

1.4.16.8.2 AT&T Monitoring, Maintenance and Management

[redacted] AT&T coordinates required software updates and configuration changes to AT&T routers. AT&T technicians work remotely with Agencies to diagnose failures and determine if AT&T routers should be replaced or repaired. The Agency installs replacement AT&T routers [redacted]

[redacted]

1.4.16.8.3 Implementation Support

CIPS with Managed Router includes on-line access to the [redacted] which provides detailed information about the installation and use of CIPS. AT&T will help Agencies prepare for installation and use of CIPS by providing Agency site configuration information to Agencies [redacted] AT&T will coordinate access line connection or ordering and installation of the access line and CIPS testing.

1.4.16.8.4 Availability and Service Interfaces

CIPS with Managed Router is a fully managed service inclusive of [redacted] as shown in **Table 1.4.16.8-1**. Under Networx, however, access CLINs are still required to be ordered**.**

SERVICE	SERVICE INTERFACES
CIPS with Managed Router	56Kbps to OC-48 (2.5Gbps)

Table 1.4.16.8-1: Domestic Port Speeds. *CIPS with Managed Router is available across multiple CIPS port speeds.*

CIPS with Managed Router service is available to Agencies located in all 50 states as well as Puerto Rico and the US Virgin Islands. CIPS with Managed Router supports the following Networx application layer services [redacted]

[redacted]

[redacted]

[redacted]

[redacted]

Additionally, CIPS with Managed Router can be configured to support Agency specific video applications with a router configuration for video specific CoS using Difserve.

1.41.6.8.5 Agency Responsibilities

AT&T will provide a total “end-to-end” managed solution. Service demarcation occurs at the LAN port of the router. Agencies have the following responsibilities in connection with CIPS with Managed Router::

- As part of the CIPS with Managed Router service, AT&T will provide an Agency with a managed router and, [redacted]

1.4.16.8.6 Features Available for CIPS with Managed Router

Class of Service (CoS)

CoS includes the standard four classifications that enable a network to support varied service levels and applications for many users. By selecting the appropriate classes relevant to specific needs, network managers can manage bandwidth and ensure that mission-critical applications do not suffer undue delays. The four general classes are:

- **CoS 1** [redacted]
- **CoS 2** [redacted]
- **CoS 3** [redacted]
- **CoS 4** [redacted]

[redacted]

[redacted] If the customer wants CoS, but does not select a CoS Profile, [redacted]

Alternate Backbone Node

The Alternate Backbone Node feature allows customers to request the Backbone Node to which their AT&T CIPS connection will terminate. [redacted]

CPE Redundant Configuration

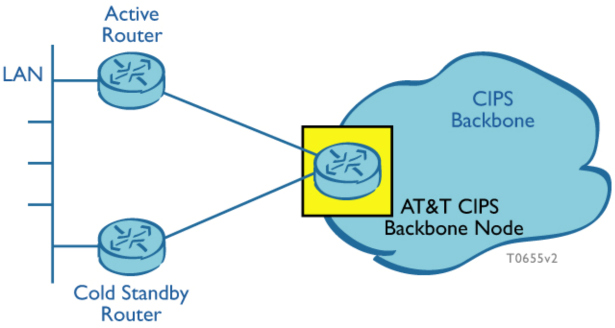

FIGURE 1.4.16.8-2: CPE REDUNDANCY. ***CPE REDUNDANCY PROVIDES AGENCIES WITH A CPE SOLUTION FOR RESILIENCY AND SURVIVABILITY TO THE IPS NETWORK.***

CPE Redundant Configuration provides a “Cold Standby” router configuration on the customer’s premises, as depicted in **Figure 1.4.16.8-2**. The Cold Standby is a fully configured and tested AT&T CIPS router and CSU/DSU.

CIPS Access Redundancy Option – Backbone Node Redundancy

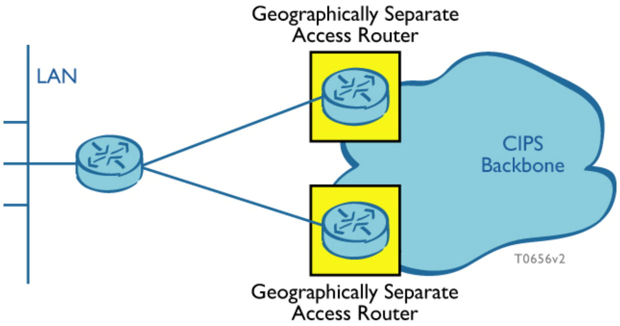
Geographically Separate Access Router
LAN
CIPS Backbone
T0656v2
Geographically Separate Access Router

FIGURE 1.4.16.8-3: BACKBONE NODE REDUNDANCY. ***BACKBONE NODE REDUNDANCY PROVIDES AGENCIES WITH HIGH SURVIVABILITY BY PROVIDING CONNECTIVITY TO GEOGRAPHICALLY DIVERSE ACCESS ROUTERS.***

Figure 1.4.16.8-3 depicts Backbone Node Redundancy where a group of circuits terminate on one or two different Agency routers and two different access routers that are located within two geographically separate AT&T [redacted] nodes. This option provides redundancy in: 1) logical path, 2) Agency router (if two are used), 3) access router and 4) AT&T [redacted] node connection. This eliminates the single point of failure for the circuit, Agency Router, access router and Backbone Node.

CIPS Access Redundancy Option – Access Router Redundancy

As depicted in **Figure 1.14.6.8-4**, Access Router Redundancy provides for a group of circuits terminating on one or two different Agency Routers and two different Access Routers within the same AT&T [redacted] Node. This eliminates the single point of failure of the circuit, Agency Router (if two are used) and Access Router. This option provides redundancy in: 1) logical path, 2) Agency router (if two are used) and 3) access router which all eliminate the single point of failure for the circuit, Agency router and access router. [redacted]

FIGURE 1.4.16.8-4: [redacted]

CIPS Access Redundancy Option – Automatic Load Balancing

Cannot be used with VoIP

Shown in **Figure 1.4.16.8-5**, a group of circuits terminate on two different Agency Routers and one Access Router. IP traffic is then load balanced across the two different Agency Routers to the Access Router. This option provides a logical redundant path to help eliminate the single point of failure for the circuits only. [redacted].

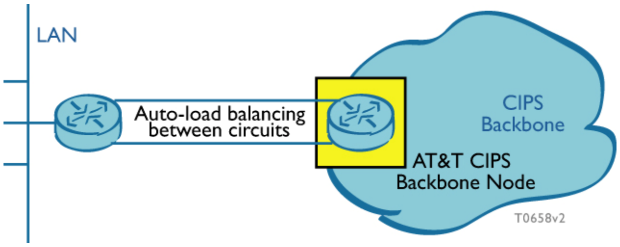

FIGURE 1.4.16.8-5: AUTOMATIC LOAD BALANCING. *AUTOMATIC LOAD BALANCING PROVIDES A LOGICAL REDUNDANT PATH TO THE CIPS NETWORK WHILE ALLOWING AN AGENCY TO UTILIZE BOTH ACCESS CIRCUITS.*