1.4.13 Network-Based IP Virtual Private Network Service (NBIP-VPNS) [C.2.7.3]

Agencies establish low-risk, highly secure, and highly reliable intranet, extranet, and remote access connectivity solutions on a global basis with Network-Based IP Virtual Private Network Service (NBIP-VPNS). Agencies are provided with a high-quality MPLS backbone, multiple levels of management and support, a full spectrum of leading privacy and security standards, flexible access arrangements, and a monitoring and management portal widely recognized as an industry-leading service.

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

1.4.13.1.a Approach to Service Delivery

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

AT&T offers the complete package-plenty of IP VPN choices, a rock solid backbone, tier one operations and management support and a new set of SLAs that are the best in the industry.

--Forrester Research
September, 2004

With geographically dispersed locations, an increasing number of remote workers, and the need to establish secure connectivity with external partners, Agencies need to provide secure and reliable communications through public and private networks that support a wide range of access speeds and access options. To effectively and efficiently accomplish these mission and business goals, the industry is transitioning from complex and inflexible legacy networks to virtual private networking capabilities. Virtual Private Networks (VPNs) support traditional private network requirements and applications over a shared and public carrier infrastructure. VPNs will help Agencies capitalize on the cost- effectiveness and ubiquity of public networks such as the

Internet and the Public Switched Telephone Network (PSTN). AT&T, with its leadership in the VPN space in general and the NBIP-VPNS space in particular, provides solutions for access, reach, reliability, performance, and security that best meet Agency requirements for intranet, extranet and remote access applications.

AT&T ranked as the top provider for VPN sales, with almost double the percentage of its nearest competitor.

--Forrester Research
September, 2004

In an effort to set new industry standards for the efficiencies and performance capabilities gained through the use of IP-based VPN technologies, AT&T designed and deployed its NBIP-VPN service as a component of a comprehensive converged VPN framework. This framework is displayed in **Figure 1.4.13.1-1** below.

Presenting NBIP-VPN within a larger VPN framework helps Agencies seamlessly and efficiently establish enterprise-wide IP-based networking and security solutions that maximize connectivity and information sharing while minimizing waste and information barriers. This becomes especially true over the lifetime of Networx as IP becomes the networking protocol of choice and IP-based VPNs become the means by which communication and security services are established. Of equal importance to the networking aspects of VPN convergence, Agencies also realize significant benefits through the integration of back-office and operational support systems as well.

Agency networks that operate a number of VPN technologies should be operationally supported through a single set of ordering, billing, inventory, and performance management Agency-facing systems. This will provide the Agency's ability to cost effectively and efficiently align its networking technologies with its business and mission goals and federal mandates.

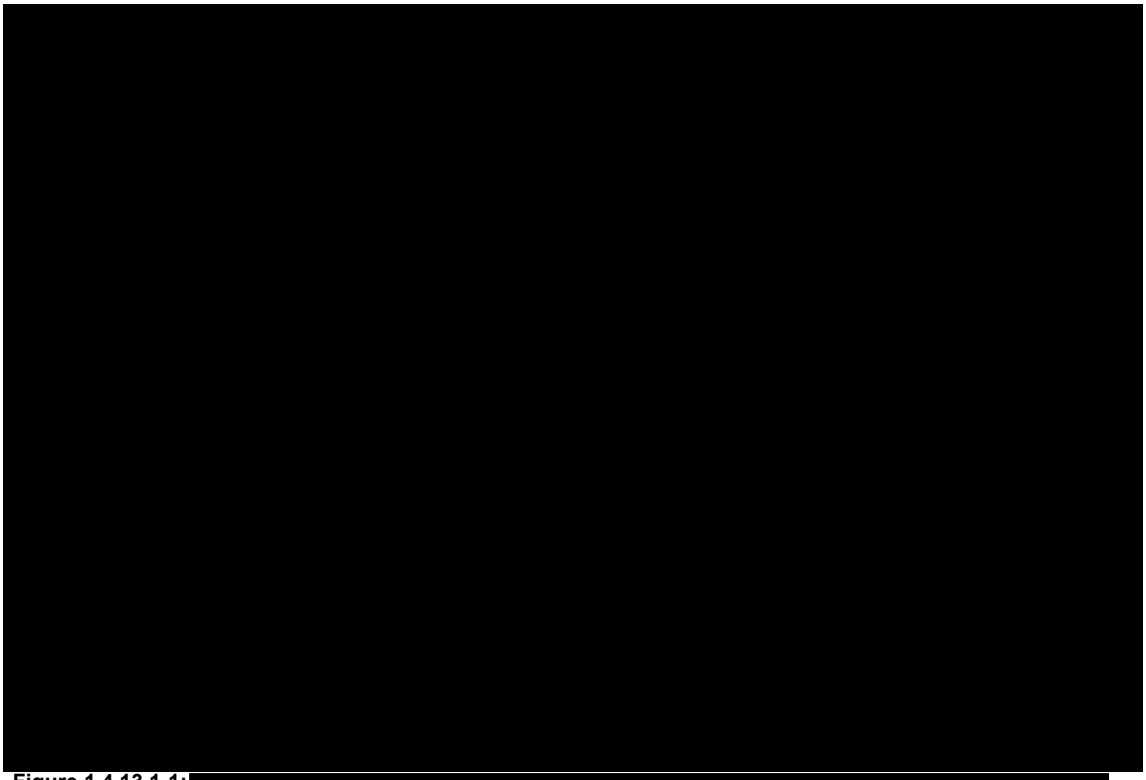


Figure 1.4.13.1-1:

The AT&T approach of integrating specific VPN technologies under a single VPN framework provides Agencies with the means of providing its end-users with a unified experience, regardless of how and where they access Agency resources.

In addition to unifying the various VPN services under one higher VPN umbrella, AT&T has also chosen MPLS as the underlying network for its Services over IP (SoIP) convergence strategy.

Figure 1.4.13.1-2 below provides a high-level representation of AT&T's approach to using MPLS as a convergence platform for all voice, data, and video traffic streams and across all AT&T services.

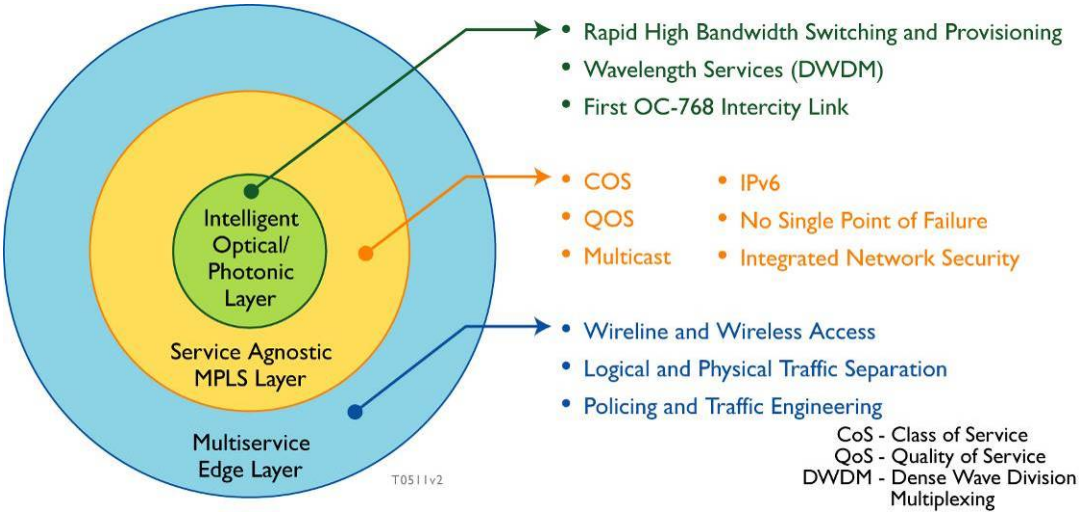


Figure 1.4.13.1-2: MPLS as Convergence Platform. [redacted]

NBIP-VPNS is a component of the Multi Service Edge (MSE) layer that uses the underlying service-agnostic MPLS layer. NBIP-VPNS provides intranet and extranet functionality to Agencies while MPLS provides NBIP-VPNS with transport and a set of ancillary services as depicted in **Figure 1.4.6.1-1**.

[redacted]

[1] *Access technologies such as Frame Relay, ATM, and Point-to-Point Protocol.*

[redacted]

[2] *Another term commonly used is "peerless IP".*

[redacted] Agencies are thus relieved of creating these solutions as would be necessary operating networks with no connectivity to other networks. This, in turn, minimizes resource inefficiencies and waste in accordance with Federal Enterprise Architecture (FEA) guidelines.

Figure 1.4.13.1-3 displays the overall NBIP-VPNS service architecture, as well as detailing other elements of the service. AT&T will provide Agencies with a comprehensive NBIP-VPN service that is inclusive of a number of critical network and service elements that are all provided and managed by a single full-service provider.

AT&T's approach to delivery of NBIP-VPNS is based upon a number of broad factors that reflect AT&T's experience in providing large-scale enterprise networking solutions to large Government entities and enterprises. **Table 1.4.13.1-1** summarizes this approach.

Figure 1.4.13.1-3: NBIP-VPNS Architecture. *Agencies can take advantage of the available service elements to create a high-quality and secure NBIP-VPNS.*

SERVICE DELIVERY APPROACH	DESCRIPTION
Global MPLS footprint	• Seamless MPLS network in 60+ countries • More than 1500 MPLS service nodes • Carries more than 4300 terabytes of data traffic including 2400 terabytes of IP traffic per business day
Comprehensive end-to-end managed solutions	• Complete NBIP-VPN infrastructure management: [redacted] • Web-based service and lifecycle management: [redacted]
Flexible network access	• Analog voice • ISDN • Ethernet • Broadband (xDSL and cable) • Private Line: DS0 to OC-48 • IP over SONET: OC-3 to OC-48 • Wireless (Wi-Fi and broadband wireless) • Satellite
Standards Support	Applicable NIST, FIPS, and IETFRFC Standard Support
Support for complete set of Agency site types	• Remote access • Intranet • Extranet
Double Prong Security Model	• Integrated Network Security: [redacted] • Dedicated Security Services: AT&T provides dedicated security services such as managed firewall and managed intrusion detection to provide Agencies with maximum security protection.
High Reliability NBIP-VPN Services	AT&T NBIP-VPNS support a wide range of redundancy and resiliency options: • Access redundancy – dual and fully diverse access circuits to the AT&T MPLS network • SED redundancy • Backbone node redundancy • ISDN backup • Dial-up failover for remote access users • Redundant Network Operation Centers (NOCs)
Service Metrics	Comprehensive set of proactive and reactive performance metrics: [redacted]
Support for Service convergence	• NBIP-VPN can be integrated with AT&T VoIP services • SED devices managed to support traffic classification based upon class of service (CoS) • MPLS backbone support for multiple real-time and non real-time traffic types

Table 1.4.13.1-1: Service Approach. *Agencies receive greater flexibility, connectivity, and productivity with high-quality NBIP-VPN services and a comprehensive service delivery approach.*

As **Table 1.4.13.1-1** above illustrates, AT&T's NBIP-VPN service is designed and deployed with the goal of providing high-

AT&T was rated as "Top Global Service Provider" of IP VPNs.

--Telemark Research 2004, 2003, and 2002

quality, secure, flexible, and technologically superior solutions to a diverse user base on a global basis. This approach has earned AT&T the industry's leadership position in IP VPN enterprise networking solutions.

1.4.13.1.b Benefits to Technical Approach

(b) Describe the expected benefits of the offeror's technical approach, to include how the services offered will facilitate Federal Enterprise Architecture objectives (see http://www.whitehouse.gov/omb/egov/a-1-fea.html).

AT&T's Networx services in general and NBIP-VPN services in particular support the Government's vision of transformation through the use of the Federal Enterprise Architecture (FEA) to verify that technologies contribute to mission performance. **Table 1.4.13.1-2** describes each service-delivery approach element in relation to FEA and summarizes its contribution and/or provides an example of how it facilitates FEA implementation. AT&T is aligning its product and service components to be easily integrated, commonly manageable, and usable. This applies across Government functions, horizontally and vertically, as well as between levels of government.

SERVICE DELIVERY APPROACH	BENEFIT	FEA FACILITATION
Global MPLS footprint	NBIP-VPN services available to all Agency locations through one seamless network	As a component of TRM/Service Access and Delivery/Service Transport, allows agencies to maximize communication and collaboration while minimizing service interruption.
Comprehensive end-to-end managed solutions	Agencies relieved of daily device management activities	As a component of TRM/Component Framework/Data Management, allows Agencies to minimize waste and duplication by dedicating more of valuable internal resources to their core missions.
Flexible network access Support for complete set of Agency site types	Agency workers, teleworkers, and mobile users all gain flexible, secure, and efficient access to Agency critical data	As a component of TRM/Service Access and Delivery/Access Channels, allows increased sharing and collaboration between same-Agency employees and between agencies. Agencies also realize significant cost savings through reduced infrastructure due to a larger population of teleworking employees.
Double-throng Security Model	Agencies receive a highly secure NBIP- VPN service with continuous and real-time visibility of threats	As a component of TRM/Component Framework/Security, allows Agency e-commerce and e-business functions to remain intact in the event of major threats to the Internet.
High Reliability NBIP-VPN Services	Ability to design and deploy mission critical IP-based networking solutions	As a component of TRM/Service Access and Delivery/Access Channels, allows agencies to increase communication and collaboration while minimizing service delivery costs.
Strict Service Performance Guarantees	End-to-end service assurance for access into agency critical resources	As a component of TRM/Service Access and Delivery/Service Transport, allows Agencies to maximize communication and collaboration while minimizing service interruption.

SERVICE DELIVERY APPROACH	BENEFIT	FEA FACILITATION
Support for Service convergence	Agencies may easily and reliably migrate to VoIP based services and Services over IP (SoIP)	As a component of TRM/Service Interface and Integration/Integration, allows Agencies to better share information and reduce duplication as many functions and services become "available over a common and open IP-based architecture.

Table 1.4.13.1-2: Agency Benefits and FEA Facilitation. *Agencies can receive products and services components that are easily integrated, commonly manageable, and aligned to support FEA objectives and meet FEA guidelines.*

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

- 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 deliver Performance Reference Model (PRM) line-of-sight linkage to mission performance and ultimate accomplishment.
- AT&T operates as an innovative partner through Networx to help achieve the vision of the FEA to enhance Agency mission performance.

In addition to the benefits and FEA facilitations cited earlier, AT&T can provide Agencies with additional services that complement NBIP-VPNS. These services include hosting, content delivery, managed security, and storage services. Agencies are therefore provided with comprehensive, end-to-end enterprise networking solutions that maximize end-to-end service performance and security.

1.4.13.1.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 that brings the depth and background to minimize an Agency's risk during transition. Our experience

has enabled us to develop proven methods, processes, and procedures applicable from the simplest to the most complex projects. **Table 1.4.13.1-3** lists the top eight service delivery risks and our mitigation strategy. As with all large NBIP-VPNS 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
Business disruption	Business disruption associated with outsourcing key IT and networking functions to a managed services provider.	
Requirements changes	Requirements changes before and after service delivery contr bute to budget overruns and missed expectations.	
Incomplete and inaccurate location information	Location information often is not accurate and site POCs are no longer valid.	
Schedule slippage	Many issues can contribute to schedule slippage. Examples include local access provider access-circuit provisioning delays, delays due to poor project planning, and delays due to inside wiring issues.	
Equipment functionality problems	It is not uncommon for premises equipment to fail to live up to manufacturer's claims and deliver functionality that customer expects.	
Inadequate Global Coverage	Risk to on-time and on-budget implementation for a large agency with many sites scattered throughout the world.	

RISK	RISK DESCRIPTION	RISK MITIGATION
Ability to customize	As Agency networks and NBIP-VPN requirements differ, Agencies require broad solutions that allow for customization and flexibility	[redacted]
Cyber Security Threats	Security threats in the form of worms, viruses, and other threats that emanate from the Internet may cause severe damage to Agency critical resources.	

Table 1.4.13.1-3: AT&T Service Delivery Lessons Learned and Risk Mitigation Strategies. *Agencies benefit from lessons learned and experience implementing NBIP-VPN services, which ultimately minimize service delivery risks.*

As evidenced from **Table 1.4.13.1-3**, several program, implementation, and network risks exist that may hinder an Agency's ability to deliver high-quality and low-risk NBIP-VPN services to its users. Agencies can build upon AT&T's capabilities as a full-service network provider to mitigate these risks and deliver uncompromised NBIP-VPNS to Agency end users.

1.4.13.1.d Network Architecture Synchronization

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

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 which is distributed to a series of Global Positioning Satellites (GPS) systems. AT&T derives synchronization from those GPS systems as the primary clock source. [redacted]

[redacted]

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

1.4.13.2.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.

High-quality NBIP-VPN services require deployment over a robust and high-performance IP network. Agencies are able to deploy quality NBIP-VPN solutions because AT&T strives to lead the industry in the quality of the IP network as AT&T service types converge onto a common IP/MPLS backbone network. **Table 1.4.13.2-1** depicts the service performance metrics Agencies will obtain for NBIP-VPNS:

KEY PERFORMANCE INDICATOR (KPI)	SERVICE LEVEL	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Latency (contiguous United States [CONUS])	All	70 ms	[redacted]
Latency (outside contiguous United States [OCONUS])	All	150 ms	[redacted]
VPN Availability	Routine	99.9%	[redacted]
	Critical	99.99%	[redacted]
Time to Restore (TTR)	Without Dispatch	4 hr	[redacted]
	With Dispatch	8 hr	[redacted]
[redacted]			

Table 1.4.13.2-1: Performance Metrics for NBIP-VPNS. *Agencies will have access to a high-quality NBIP-VPN service designed to meet all Government KPI and AQL requirements.*

[redacted]

Figure 1.4.13.2-1 illustrates how AT&T compares with other service providers in the number of network Points of Presence (POPs)[3]. A higher number of POPs translates into improved performance levels as access lines become shorter and the access network is minimized. [redacted] By minimizing this access and interconnecting with the high speed POP directly, Agencies receive much better performance levels and reliabilities.

2. The AT&T backbone network presents the industry lowest end-to-end packet latencies. Latency is one of the most important metrics that reflect the quality of the underlying IP network. [redacted] **Figure 1.4.13.2-2** illustrates how packet delay compares between several large IP networks.

[redacted]

Figure 1.4.13.2-1: Network Reach Comparison. *With the highest number of high- speed POPs in the underlying backbone network, Agencies interconnect with the network globally and achieve much improved performance levels.*

Figure 1.4.13.2-2: IP Network Latency Comparison. *A lower and consistent latency translates to improved end-to-end quality for agency applications and is the basis for successfully converging agency applications onto a common IP infrastructure. Reference: each company's web site.*

3. AT&T offers the following AQL's for performance, provisioning, and maintenance. **Table1.4.13.2-2** illustrates how the AT&T AQL's compare with competitors.

DEDICATED INTERNET ACCESS AQLS	AT&T	CLOSEST IDENTIFIED COMPETITOR*
Latency (ms)		
Within Region US		
Within Region Asia Pacific (AP)		
Between Regions AP – EMEA		
Data Delivery		
Within region Europe		
Between Regions US to Other		
Service Availability (End-to-End)		
Provisioning (Days)		
Time to Repair		

Table 1.4.13.2-2: AT&T AQLs vs. Competition. *Agencies receive best possible service with industry-leading AQLs. AT&T AQL's are realistic and not based upon creative marketing or accounting practices.*

Best-in-industry AQL's will allow AT&T to deliver superior NBIP-VPNS solutions.

AT&T is really raising the bar with these SLAs. This is a comprehensive and aggressive move to challenge the industry's traditional methods of measuring performance in a way that is meaningful to customers and meeting their business objectives. It will be harder for competitors to be vague about their SLA commitments when AT&T's are out there in bold print"

--Kate Gerwig, Current Analysis

1.4.13.2.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. Every element of the NBIP-VPN service, including the infrastructure components of the underlying AT&T Internet backbone are monitored using a task specific Element Management System (EMS) shown in **Figure 1.4.13.2-3**

Figure 1.4.13.2-3: Management Network

Table 1.4.13.2-3 below outlines the methods used to measure the various NBIP-VPN key performance indicators.

KEY PERFORMANCE INDICATOR	APPROACH TO MONITORING AND MEASURING
Latency (CONUS and OCONUS)	
VPN Availability	
Time to Restore (TTR)	

Table 1.4.13.2-3: Approach to Monitoring and Measuring NBIP-VPNS. *Agencies are provided the methodologies to ensure proper measurements of the KPIs in the RFP.*

The first time the service is provided through the Networx contract, the performance must be verified. The KPIs will be monitored to certify that the service performance complies with the AQL. [redacted] The service verification process is presented in greater detail in Section 1.3.2.d, Approach to Perform Service Delivery Verification.

Agencies will benefit from AT&T's approach to monitoring and measuring the NBIP-VPNS KPIs by having comprehensive methods and procedures for monitoring and measuring KPIs.

1.4.13.2.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.

Agencies will benefit from enhanced service performance when the NBIP-VPNS service provider exceeds the stated KPI performance thresholds. **Table 1.4.13.2-4** summarizes the proposed improvements to the KPI performance thresholds, and the benefits that Agencies will experience through the higher service performance.

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

Table 1.4.13.2-4: Performance Level Improvements. [redacted]

1.4.13.2.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 proposes the additional KPIs listed in **Table 1.4.13.2-5** as enhancements to the Government's set of NBIP-VPN KPIs.

PROPOSED KPI	DESCRIPTION OF PROPOSED KPI	BENEFIT OF PROPOSED KPI

Table 1.4.13.2-5: Performance Level Improvements.

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

1.4.13.3.a Service Description

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

AT&T will satisfy all the service requirements through the technological capabilities of the backbone IP/MPLS network, the geographic reach and access flexibility of NBIP-VPN solutions, and a host of network-based services and applications. In addition, NBIP-VPN requirements will be satisfied through

gateway services between the IP/MPLS network and other public networks, strong layered security, complementary managed services that augment NBIP-VPNS, and superior support services backed by AQL guarantees. Through the combination of NBIP-VPN components, AT&T can provide Agencies with customized and secure solutions for intranets extranets, and remote access. **Table 1.4.13.3-1** provides a detailed description of the elements of the AT&T IPS service and their associated Agency benefits.

SERVICE REQUIREMENT	DESCRIPTION	BENEFITS TO AGENCY
Tunneling	IP Security (IPSec), Secure Sockets Layer (SSL), Layer 2 Tunneling Protocol (L2TP), Point-to-Point Tunneling Protocol, GRE over IPSec, VRF aware IPSec	• Highly secure solutions • Solutions based upon latest security standards • Business-level encryption as well as NSA type-1 encryption • Support for SSL allows Agencies greater implementation flexibility • VRF aware IPSec allows multiple Agencies share common infrastructure
Encryption	Site to site encryption: DES, 3DES, AES.	
Authentication	X.509 certificates, RADIUS, SecureID, LDAP, SafeWord, Defender, Others on a custom basis	
Multi-VRF solutions	[redacted]	Agencies may easily apply multiple QoS policies tailored to individual Agency groups and application classes
Co-location	Co-location can be designed based upon each agency's specific requirements for equipment, space and security. Current AT&T co-location options include: • AT&T POP Space – Provide the highest levels of security • AT&T Internet Data Center (IDC) – Provides access to managed hosting services and high-speed Internet access	• Highly secure and reliable infrastructure • High bandwidth Internet access without the need for costly access circuits
IPv6 Support	[redacted]	Quicker IPv6 adoption and associated address, security, and quality benefits
Quality of service (QoS)	For AT&T managed SEDs, end-to-end QoS is provided through traffic classification and prioritization at the SED device (CE router), the Provider Edge (PE router), and core (P routers). For Agency managed SEDs, AT&T provides QoS for all network devices (PE and P). Per-flow QoS is currently being tested but not commercially available.	Agency real-time applications receive required performance and availability metrics
Congestion avoidance	[redacted]	Agency applications perform at consistent quality levels during congestion

[4] *AT&T is also an active participant in the Moonv6 project which was launched as a collaborative effort between Industry, Academic, and Government entities to further advance IPv6 research, advancement, and deployment.*

SERVICE REQUIREMENT	DESCRIPTION	BENEFITS TO AGENCY
Layered security services	Security features include • Anti-virus management • Intrusion detection and prevention • Managed firewall • Vulnerability scanning • Network integrated security through the backbone IP/MPLS network	• Defense-in-depth • Maximum security protection • Ability for Agencies to tailor security solutions according to needs and budgets
Proactive management	AT&T's NBIP-VPNS are managed on a 24x7x365 basis via two fully redundant Network Operations Centers (NOCs). Devices under AT&T management are proactively polled for availability, delay, and performance data. Agencies are also provided with a web-based management tool for near real-time topological and graphical view of Agency network performance with color coded status and links into the ticketing and status systems	• Higher levels of service availability and reliability. • Enhanced vis bility of network health status.
Design and engineering	Agencies may receive customized NBIP-VPN solutions that meet Agency-specific requirements: • Design, configure, install & test custom solution components • Integration consulting services and Proof of Concept service • AT&T Labs and AT&T Government Solutions offer extensive expertise in helping Agencies customize NBIP-VPN networking solutions	Agencies will be able to deploy highly customized solutions that best meet Agency networking and mission needs
Response to requests	Web-based tool that provides Agencies with ability to issue Move, Add, Change, Delete (MACD) requests	Quick and error-free response to Agency requests
Secure routing	AT&T supports static and dynamic routing to provide full routing capability on the VPN platform	Routing transparency for agency sites that participate in the VPN
Class of service (CoS) support	AT&T can provide Classes of Service categorized by the type of traffic as shown in **Table 1.4.13.3-2**.	Agencies can prioritize traffic by integrating time-sensitive applications, i.e. Voice over IP (VoIP), over the NBIP-VPNS.
High availability options for service enabling devices (SED)	AT&T provides resiliency options to provide automatic failover in the case that the primary NBIP-VPNS connection fails as outlined in **Table 1.4.13.3-4**.	Agencies will have maximum uptime even with a failure to their primary NBIP-VPNS connection.
Internet gateway service	• Internet gateway services allow Agencies access to the Internet through unique packet filtering and address translation. • Supported through network-based firewall	• Filtering and address translation helps protect users from unauthorized access by unwanted sources without use of firewall or proxy server. • Enables Agencies to access intranet, Internet, and extranet applications from single connection.
Service interworking	AT&T can interwork with the following access services into NBIP-VPNS: • Asynchronous Transfer Mode Service (ATMS) • Frame Relay Service (FRS) • Private Line Service (PLS)	Allows Agencies to interconnect between Agency sites served via ATM, frame relay, private line and/or Ethernet services.

SERVICE REQUIREMENT	DESCRIPTION	BENEFITS TO AGENCY
Key management	• Support for X.509 digital certificates • Customized complex multilayer key management • Full management through AT&T Managed Token Security Service • More sophisticated token management provided through the AT&T Government Solutions PKI center for sensitive Government Agencies	Agencies can control the use of shared keys within their NBIP-VPNS and not have to rely on a third party to provide the shared keys.
[redacted]	[redacted]	[redacted]

Remote access service	• AT&T's NBIP-VPN Remote Access (ANIRA) provides remote access capabilities to NBIP-VPNS.
	• Provides connectivity to NBIP-VPN via:
	  • Analog dial (6000+ global POPs in 120 countries)
	  • WiFi (9200+ hotspots in 35 countries
	  • DSL (95 MSAs, 1000 US cities, 9 countries)
	  • Wired Ethernet (1700+ locations in 18 counties)
	  • Cellular GPRS in Europe and PHS in Japan
	  • Agency provided broadband, wireless, Ethernet, and dial
	• Supports full service interworking through network based gateway services.
		• Agencies may provide NBIP-VPNS to a broad base of site and user types
		• Allows remote users seamlessly communicate with all Agency network access types through network based gateway services

Table 1.4.13.3-1: NBIP-VPNS Service Description. *By combining standard NBIP-VPNS service features, Agencies can design and implement a secure, robust and high quality VPN solution.*

As indicated in **Table 1.4.13.3-1**, Agencies receive fully compliant NBIP-VPN services with a range of capabilities that may be used to construct sophisticated and customized VPN solutions with varying levels of technical and operational requirements.

1.4.13.3.a.1 Class of Service (CoS)

AT&T supports [redacted] today with the ability to expand as Agency application support needs expand. In addition, AT&T currently supports [redacted] that allow Agencies to optimize SED and access resources based upon the mix of applications used by each Agency. The classification of traffic is defined at the edge of the network by the Agency SED (CE router). The Agency SED uses this classification to differentiate the traffic and prioritize the applications before transmission through the network.

Table 1.4.13.3-2 provides an overview of the [redacted] as well as examples for the use of each class.

TRAFFIC CLASS	TRAFFIC TYPE	SUGGESTED EXAMPLES
[redacted]	[redacted]	[redacted]

Table 1.4.13.3-2: Class of Service Categories. [redacted] **Table 1.4.13.3-3**.

[redacted] The objective is to optimize the access link usage as well as the service offered to the different types of applications.

DESCRIPTION	PARAMETERS
Application traffic assigned to a class on Agency router	• Origin IP address • Input interface • Port number • Application protocol • Classification/setting of IP precedence bits/marking
Traffic conditioning techniques	• Classification/setting of IP precedence bits/marking • Traffic policing and traffic shaping • Queuing mechanisms • Congestion control

Table 1.4.13.3-3: Techniques for Managing Application Traffic. [redacted]

1.4.13.3.a.2 High Availability Options for SEDs

AT&T provides four configurations of resiliency options to provide automatic backup in the unlikely event of a primary connection failure. **Table 1.4.13.3-4** describes the different configurations in further detail.

RESILIENCY OPTION	DESCRIPTION
[redacted]	[redacted]

Table 1.4.13.3-4: Resiliency Options. [redacted]

In addition to the high availability options listed above, AT&T can provide Agencies with customized features such as redundant processor cards, non-stop forwarding, and hitless IOS upgrades. These additional features can be provided to critical routers as well as non-router devices such as switches, firewalls, caches, antivirus servers, intrusion detection devices, VoIP gateways, VoIP gatekeepers, and VoIP call managers.

1.4.13.3.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.

In addition to the standard services, Agencies can enhance their NBIP-VPNS with additional features and capabilities for an additional fee. AT&T proposes the attributes in **Table 1.4.13.3-5** as service enhancements.

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

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

Table 1.4.13.3-5: Service Feature Enhancements. *Agencies can enhance their NBIP-VPNS by subscribing to the service enhancements.*

[redacted]

1.4.13.3.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.

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

1.4.13.3.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.

AT&T Networx Team offers Agencies extensive experience providing managed services that create value to our customers to both in Government and commercial entities. This experience has given us the ability to engineer and deliver NBIP-VPN services. Three examples of AT&T Team's ability to deliver these services are listed in **Table 1.4.13.3-6**.

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

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

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

Table 1.4.13.3-6: Experience Delivering Managed Services. *AT&T has an extensive history in providing hosting services to both Government Agencies as well as commercial customers.*

AT&T's vast experience in providing broad and large-scale NBIP-VPN services will help meet the NBIP-VPN needs of Agencies, regardless of Agency size, location base, or mission requirements.

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

1.4.13.4.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 build out contemplated.

To assess the impact of the Agencies NBIP-VPNS traffic on the AT&T network, the forecasted traffic in the Networx hosting model has been compared against the scale of AT&T's IP/MPLS network. As **Table 1.4.13.4-1** shows, [redacted]

CONTRACT YEAR	TRAFFIC MODEL TOTAL NBIP-VPNS TRAFFIC (GBPS)	TRAFFIC MODEL TOTAL TRAFFIC (TB/DAY) @ 100% UTILIZATION (NOTES1,2)	AT&T TOTAL MPLS NETWORK TRAFFIC (TB/DAY)-NOTE 3	TRAFFIC MODEL TO AT&T TRAFFIC RATIO (%)
1	[redacted]	[redacted]	[redacted]	[redacted]
2				
3				
4				
5				
6				
7				
8				
9				
10				

CONTRACT YEAR	TRAFFIC MODEL TOTAL NBIP-VPNS TRAFFIC (GBPS)	TRAFFIC MODEL TOTAL TRAFFIC (TB/DAY) @ 100% UTILIZATION (NOTES1,2)	AT&T TOTAL MPLS NETWORK TRAFFIC (TB/DAY)-NOTE 3	TRAFFIC MODEL TO AT&T TRAFFIC RATIO (%)
[redacted]				

Table 1.4.13.4-1: Network [redacted]

As evidenced by the Table above, no additional network build-out will be contemplated.

1.4.13.4.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.

Network access robustness and resiliency is provided through access circuit redundancy, device (CPE) redundancy, and access POP redundancy. POP redundancy includes physical POP diversity (i.e., Agency sites receive dual access circuits to two AT&T POPs) as well as redundancy access within the POP itself (i.e., two access circuits terminate within the same POP but at two separate edge devices).

Network backbone IP robustness and resiliency is provided through superb network reliability and availability measures and by adhering to a rigorous network design process. **Table 1.4.13.4.-2** summarizes these two points.

ROBUSTNESS & RESILIENCY FACTOR	DESCRIPTION
High reliability	This is facilitated through: • No single point of failure anywhere in the core architecture. • All backbone nodes located within highly reliable and secure AT&T central offices. [redacted]
Rigorous network design process	[redacted]

ROBUSTNESS & RESILIENCY FACTOR	DESCRIPTION
	[redacted]

Table 1.4.13.4-2 Robustness and Resilience in the AT&T Backbone. [redacted]

Another key component of the AT&T backbone network and its resiliency is the fact that the MPLS core network does not contain any Internet routes (Internet-route free core). As routing tables grew in size in recent years following tremendous growth of the Internet, routers became increasingly unstable. This included core high-performance routers. AT&T recognized this problem early and designed a tiered structure with the intention of having the core carry no Internet routes. This has added significantly to the stability and performance predictability of the AT&T core MPLS network.

Agencies will also benefit through AT&T's rigorous capacity planning process, which allows AT&T to maintain the flexibility of the IP/MPLS network to accommodate planned and sudden increased traffic loads. A description of the AT&T capacity-planning process in outlined in Section 1.4.13.4.B.1 below.

1.4.13.4.b.1 Capacity Planning

Backbone capacity planning within the backbone IP/MPLS network is a result of three main drivers, as summarized in **Table 1.4.13.4-3.**

MAJOR CAPACITY PLANNING DRIVER	DESCRIPTION
Forecasts	Annual business plan forecasts of all existing and new AT&T services that use the IP backbone network.
Planned events	Planned technology migrations and insertions

MAJOR CAPACITY PLANNING DRIVER	DESCRIPTION
Historic traffic growth	Historic traffic growth of existing services as measured over time. This growth reflects changes in usage patterns of existing users as well as the Internet at large. [redacted]

Table 1.4.13.4-3: Capacity Planning. *Agencies benefit from a comprehensive capacity planning framework.*

The scale and size of the AT&T IP/MPLS network today is testimony to the successful capacity planning process employed by AT&T.

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

1.4.13.5.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.

Engineering optimization of the IP-based and optical services is described in Section 1.3.6.2.a.

1.4.13.5.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.

1.4.13.5.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 multiservice edge (MSE) platforms is described in Section 1.3.6.2.c.

1.4.13.5.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.

1.4.13.6 Narrative Requirements

A technical resource available to AT&T corporate is AT&T Labs. This organization plays a key role certifying interoperability of all existing access types, interfaces, products, and services before they are connected with the AT&T network. Compliance to the narrative text requirements for subsections C.2.7.3.3.1 (1) through C.2.7.3.3.1 (3) are listed in **Table 1.4.13.6-1**.

UNI TYPE	INTERFACE/ ACCESS TYPE	NETWORK-SIDE INTERFACE	PROTOCOL	COMPLY
C.2.7.3.3.1 (1)	Ethernet Access	• 1 Mbps to 10 GbE • 10GbE (Optional)	IPv4/IPv6 over Ethernet	✓
C.2.7.3.3.1 (2)	Private Line Service	• DS0 • Fractional T1 • T1 • T3 • Fractional T3 • OC-3c • OC-12c • OC-48c • OC-192c	IPv4/v6 over PLS	✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓ ✓
C.2.7.3.3.1 (3)	IP over SONET Service	• OC-3c • OC-12c • OC-48c • OC-192c	IP/PPP over SONET	✓ ✓ ✓ ✓

Note 1: IPv6 when commercially available by the offeror.

Table 1.4.13.6-1: Compliant with Intranet and Extranet NB IPVPN Interfaces. *Agency intranet and extranet interface requirements are fully met with IP over Ethernet.*

Compliance to the narrative text requirements for subsections C.2.7.3.3.2 (1) through C.2.7.3.3.2 (7) are listed in **Table 1.4.13.6-2**.

UNI TYPE	INTERFACE/ACCESS TYPE	NETWORK-SIDE INTERFACE	PROTOCOL	COMPLY
C.2.7.3.3.2 (1)	Voice Service	Analog dialup at 56 Kbps	Point-to-Point Protocol, IPv4/v6	✓
C.2.7.3.3.2 (2)	DSL Service	xDSL access at 1.5 to 6 Mbps	Point-to-Point Protocol, IPv4/v6	✓
C.2.7.3.3.2 (3)	Cable high-speed access	320 kbps up to 10 Mbps	Point-to-Point Protocol, IPv4/v6	✓

UNI TYPE	INTERFACE/ACCESS TYPE	NETWORK-SIDE INTERFACE	PROTOCOL	COMPLY
C.2.7.3.3.2 (4)	Multimode/Wireless LAN Service	Section C.2.14.3.3.1 MWLANS User-to-Network Interfaces		✓
C.2.7.3.3.2 (5)	Wireless Access	Section C.2.16.2.3.3.1 Wireless Access Arrangement Interfaces		✓
C.2.7.3.3.2 (6)	Satellite Access	Section C.2.16.2.4.3.1 Satellite Access Arrangement Interfaces		✓
C.2.7.3.3.2 (7)	Circuit Switched Data Service	• ISDN at 64 kbps • ISDN at 128 kbps • ISDN dial backup at 64 kbps • ISDN dial backup at 128 kbps	Point-to-Point Protocol, IPv4/v6	✓ ✓ ✓ ✓

Note 1: IPv6 when commercially available by offeror.

Table 1.4.13.6-2: Compliant with Remote Access NB IPVPN Interfaces. *Agency Remote Access interface requirements are fully met through support of dial, broadband, circuit switched, and wireless interfaces.*

Agencies will benefit from the role of AT&T Labs by verifying interoperability of access types and interfaces with Agency equipment. Agencies will be able to use existing equipment with AT&T's NBIP-VPNS.

1.4.13.6.1 Application Level QoS Support

The contractor shall support one or more of the following application level QoS objectives, as required in J.2.1, J.2.2, and J.2.3 for Geographic Coverage: a. Intserv model for selected individual flows; b. Diffserv model for aggregated flows.

AT&T supports the Diffserv model for aggregated flows supporting NBIP VPNS QoS objectives in all geographic coverage areas.

1.4.13.6.2 Standardized Modes QoS Support

The contractor shall support QoS in one or more of the following standardized modes: a. Best effort; b. Aggregate Customer Edge (CE) Interface level QoS ("hose" level); c. Site-to-site level QoS ("pipe" level); d. Intserv (RSVP) signaled; e. Diffserv marked.

AT&T supports the following standard QoS modes:

[redacted]

[redacted]

1.4.13.7 Stipulated Deviations

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

1.4.13.8 EMNS Enhanced Network-Based IPVPN

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

1.4.13.8.1 EMNS Enhanced Network-Based IPVPN - Service Description

The EMNS Enhanced NB-IPVPN service provides the advantages of a QoS-aware, any-to-any MPLS network and the privacy of encrypted, Agency-specific IPSec overlay meshes.

MPLS is the marriage of switching technologies with the scalability of IP, in a fully standards-compliant implementation. RFC-2547/4364 describes the MPLS implementation that AT&T has deployed worldwide. [redacted]

[redacted] Support for current and future applications is ensured by the multiple Class of Service (CoS) offerings. The CoS1 level is used for real time application such as voice over IP and video. The CoS2 level is used for critical data applications and is targeted at mission critical data applications. The CoS3 level is used for Agency data applications such as Human Resource web sites and Agency email.

[redacted]

CLASS OF SERVICE TYPE	DESCRIPTION
CoS-1	Voice over IP, video conferencing, etc
CoS-2	Non-real-time traffic requiring better than standard service, video streaming, SNA, and other Government enterprise-wide applications such as HR Connect, etc
CoS-3	Regular Agency traffic l ke email, http, ftp, etc.

Table 1.4.13.8-1: Class of Service Description. *The Enhanced Managed Network Service Network Based IPVPN supports three distinct Classes of Service that provide prioritized transport across the MPLS VPN network***.**

[redacted]

All legacy protocols are supported on a site-by-site basis. [redacted]

[redacted]

1.4.13.8.2 EMNS Enhanced Network-Based IPVPN – Remote Access Service Feature

Remote access into the EMNS Enhanced Network-Based IPVPN is provided with encrypted, multi-authenticated, non-repudiated and access-agnostic connectivity over the Internet. [redacted]

The service configurations for remote access provide the Agency with the option to purchase as follows:

- VPN Client only
- VPN Client w/ Bundled Nationwide Dial-up Access
- VPN Client w/ Bundled Nationwide Dial-up Access and Nationwide Broadband Wireless Access
- VPN Client only w/ Multipart Authentication
- VPN Client w/ Bundled Nationwide Dial-up Access w/ Multipart Authentication
- VPN Client w/ Bundled Nationwide Dial-up Access and Nationwide Broadband Wireless Access w/ Multipart Authentication
- Unbundled Nationwide Dial-up Access
- Unbundled Nationwide Broadband Wireless Access

1.4.13.8.3 EMNS Enhanced NBIPVPN – Service Quality & Performance

All EMNS sites belong to one of the two categories with each category of site requiring a different availability as follows:

- Category-1 Sites require ≥ 99.99% availability

- Category-2 Sites require ≥ 99.9% availability

Additionally, service quality and performance is further defined by Class of Service. **Table 1.4.13.8-2** depicts the service performance metrics Agencies will receive when they select EMNS Network Based IP-VPNS with CoS-1:

KEY PERFORMANCE INDICATOR (KPI)	SERVICE LEVEL	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Availability	CAT-2	99.9%	[redacted]
	CAT-1	99.99%	[redacted]
Latency (CONUS & OCONUS)	CoS-1	125 ms	[redacted]
Packet Jitter (CONUS & OCONUS)	CoS-1	25 ms	[redacted]
Packet Loss (CONUS & OCONUS)	CoS-1	0.1%	[redacted]
[redacted]			

Table 1.4.13.8-2: Additional Performance Metrics for EMNS Network Based IP-VPNS with CoS-1. *Agencies will have access to a high-quality NBIP-VPN service designed to support Voice over IP or Video Conferencing service performance requirements.*

Table 1.4.13.8-3 depicts the service performance metrics Agencies will receive when they select EMNS Network Based IP-VPNS with CoS-2:

KEY PERFORMANCE INDICATOR (KPI)	SERVICE LEVEL	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Availability	CAT-2	99.9%	[redacted]
	CAT-1	99.99%	[redacted]
Latency (CONUS & OCONUS)	CoS-2	175 ms	[redacted]
Packet Jitter (CONUS & OCONUS)	CoS-2	35 ms	[redacted]
Packet Loss (CONUS & OCONUS)	CoS-2	1%	[redacted]
[redacted]			

Table 1.4.13.8-3: Additional Performance Metrics for EMNS Network Based IP-VPNS with CoS-2. *Agencies will have access to a high-quality NBIP-VPN service designed to support Voice over IP or Video Conferencing service performance requirements.*

Table 1.4.13.8.1-4 depicts the service performance metrics Agencies will receive when they select EMNS Network Based IP-VPNS with CoS-3:

KEY PERFORMANCE INDICATOR (KPI)	SERVICE LEVEL	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Availability	CAT-2	99.9%	[redacted]
	CAT-1	99.99%	[redacted]
Latency (CONUS & OCONUS)	CoS-3	250 ms	[redacted]

KEY PERFORMANCE INDICATOR (KPI)	SERVICE LEVEL	PERFORMANCE STANDARD (LEVEL/THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Packet Jitter (CONUS & OCONUS)	CoS-3	45 ms	[redacted]
Packet Loss (CONUS & OCONUS)	CoS-3	2%	[redacted]
[redacted]			

Table 1.4.13.8-4: Additional Performance Metrics for EMNS Network Based IP-VPNS with CoS-3. *Agencies will have access to a high-quality NBIP-VPN service designed to support Voice over IP or Video Conferencing service performance requirements.*

1.4.13.8.4 EIASS Gateway Feature

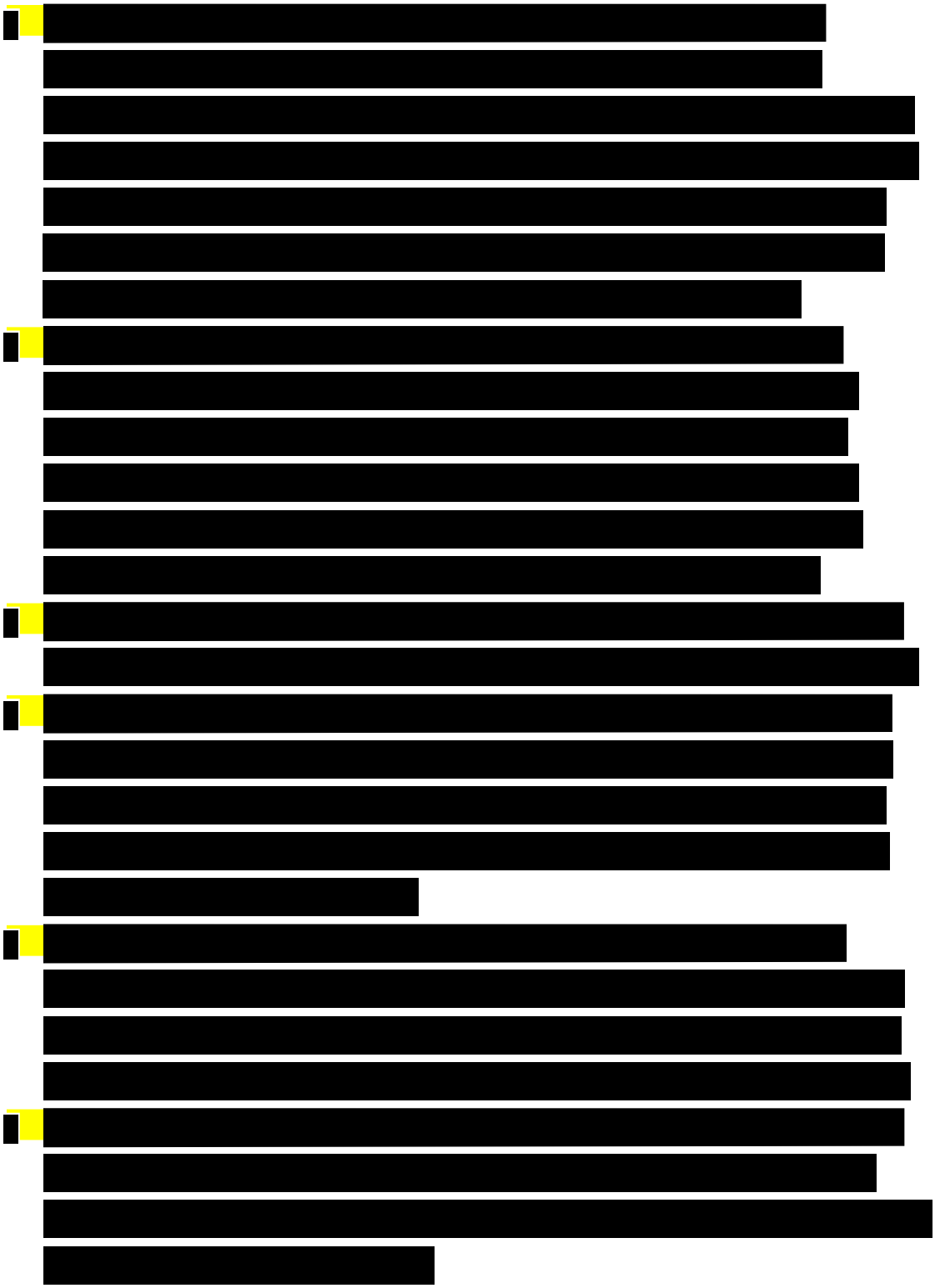
The Enhanced Internet Access Security Service (EIASS) provides Enhanced NBIP-VPNS customers with redundant secure Internet access gateways for Enhanced NBIP-VPNS sites to securely connect to the public Internet. The EIASS feature will be provided to every Enhanced NBIP-VPNS customer site deployment, as part of the overall Enhanced NBIP-VPNS solution.

In addition to providing secure Internet connectivity, the EIASS Gateway feature provides the option for the Enhanced NBIP-VPNS [redacted]

1.4.13.8.4.1 EIASS Gateway Feature – Service Description

Continually increasing and more sophisticated cyber security threats to government systems range from curious prowlers to savvy intruders, simple mischief to espionage. Based on the current threat environment, recent OMB mandates, and Agency-specified security requirements and policies, AT&T has developed the EIASS service to provide adaptive and comprehensive security architecture for Internet Access. The EIASS is designed to provide a robust security posture, providing the Enhanced NBIP-VPNS customer with a high level of security and privacy for its private VPN network.

The physical components that comprise the EIASS Gateway Feature are listed below:



1.4.13.8.4.2 EIASS Gateway Feature – Solution Components

The EIASS Gateway Feature is a managed solution. As a managed solution, there are multiple components that comprise the EIASS Gateway feature, as described below:

Design & Engineering

Working with the Enhanced NBIP-VPNS customer, AT&T will provide the design and engineering services required to deploy the EIASS Gateway. Design and engineering services include review of current network traffic, performance, transport, hardware and software components, and an overall evaluation of the network topology, configuration, addressing, bandwidth, availability, scalability, reliability, and disaster recovery requirements.

Establish EIASS Gateway Sites

Upon completion of the EAISS design and engineering solution, AT&T will establish the EIASS Gateway Sites in accordance with designed and engineered solution. AT&T will procure the necessary equipment, Internet service, collocation space and other required components of the EIASS Gateway. AT&T installs and configures the EIASS Gateway equipment at the designated collocation facilities, and connects the EIASS Gateway equipment to the public Internet and the Enhanced NBIP-VPNS Customer's VPN Network.

Configure and Provision EIASS Gateway Sites

Upon receipt of EIASS Gateway service order, AT&T will configure and provision the EIASS Gateway to provide secure Internet access to the Enhanced NBIP-VPNS customer. The configuration and provision activities include:

- Adding or removing logical Enhanced NBIP-VPNS connections to the EIASS Gateway
- Configuring Security Devices in accordance with the security policies jointly defined by the Enhanced NBIP-VPNS Customer and AT&T

[redacted]

- Document and inventory EIASS Gateway order configurations

[redacted]

Manage and Maintain EIASS Gateway Sites

Upon deployment of the EIASS Gateway, AT&T will provide ongoing management and maintenance of the EIASS Gateway. This includes management and maintenance of EIASS equipment, the associated Internet and customer VPN connections, and collocation space. The management and maintenance activities include fault management and trouble resolution, change management, upgrades and repairs to the components that comprise the EIASS Gateway.

[redacted]

1.4.13.8.4.3 EIASS Gateway Feature – Detailed Component Description

The EIASS Gateway feature is comprised of multiple networking and security components that perform specific roles in protecting the Customers network. A description of each EIASS Gateway component follows.

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

1.4.13.8.4.4 Out of Band Management (OBM) – Detailed Description

[redacted]

1.4.13.8.5 Trusted Internet Connection (TIC) Interconnect

[redacted] The TIC Interconnect infrastructure will allow access to an Agency's TIC, offering a secure, Agency policy compliant connection to its bureaus or subagencies. The key elements for an Agency's TIC Interconnect are:

- TIC Interconnect equipment will consist of a [redacted] (or equivalent) and two (scalable to four) redundant [redacted] (or equivalent) [redacted]
- [redacted] are referred to in Section [redacted] of AT&T's Networx Universal technical volume. The Agency bureau or subagency utilization of the TIC Interconnect [redacted].
- An Agency-[redacted] implementation will receive connectivity into that Agency's TIC Interconnect [redacted].
- The Ethernet ports [redacted]
- An Agency-[redacted] implementation will get connectivity to that Agency's TIC via the TIC Interconnect. AT&T will complete the Agency ordered [redacted] connection [redacted]
- The TIC Interconnect [redacted] will be configured for each Agency-[redacted] implementation.

1.4.13.8.5.1 Agency Responsibilities

- The Agency is required to provide AT&T with a design document that sets forth the specific security controls applicable to the internet traffic which are intended to prevent unauthorized traffic [redacted]
- The Agency Program Management Office (PMO) will work with Agency Bureaus or subagencies to document their traffic flow requirements [redacted]
- For all orders,an Agency Bureau or subagency shall provide the following information at the time the order is placed:

  [redacted]

This Agency specific Traffic information is necessary for AT&T to correctly and securely configure the traffic flow [redacted]

1.4.13.8.6 Certification & Accreditation (C&A) at FIPS-199 High-High-High Impact Level

EMNS Enhanced NB-IPVPNS and EIASS service requires certification as a High-High-High system in accordance with Federal Information Processing Standards 199 (FIPS-199). As such, EMNS requires more stringent controls than FIPS-199 Moderate systems as well as more documentation and testing regarding those controls.

The Certification and Accreditation (C&A) at FIPS-199 High-High-High Impact Level is driven by requirements of the NIST 800-37 Special Publication that contains the process for certifying Government systems. AT&T will prepare

and submit the requisite documentation to the Government for certification and accreditation of the Government's systems for each ENMS Enhanced NBIP-VPNS site at the outset of the three year cycle which Federal Information Security Management Act (FISMA) mandates. At each Customer site where the ENMS Enhanced NBIP-VPNS and EIASS service is provided, the C&A at FIPS-199 High, High, High impact level [redacted]

In addition, the C&A process required for a High-High-High Impact Level addresses the more extensive test case development, C&A documentation development, results analysis, methods and procedures, and all required supporting documentation. In accordance with those requirements:

- AT&T will update the C&A supporting documentation as necessary [redacted]
- AT&T will update the relevant security documentation [redacted] FISMA, and OMB guidelines such as A-130.

In addition to the documentation, operational control processes and procedures will be put into place [redacted] The controls required to shift from FIPS-199 Moderate to FIPS-199 High [redacted] These controls are [redacted] NIST and EMNS Customer audit compliance and monthly reporting. There are three main categories of support that are required:

- IT Operations Support – needed to conduct information assurance activities [redacted]

[redacted]

- Network Engineering Support – needed to conduct frequent and automated WAN device configuration audits [redacted]
- Security Analyst Support – needed to analyze results of all IT and WAN configuration management, vulnerability scans, and security audits.

AT&T will provide Service Development Lifecycle (SDLC) support which is comprised of five phases:

1. Planning / Initiation
2. Acquisition / Development
3. Testing / Implementation
4. Operations / Management
5. Disposition

Planning/Initiation: Security authorization tasks should begin early in the SDLC, [redacted] and are important in shaping and influencing the security capabilities of the system. It is critical that the *security requirements* as determined by FIPS 199 be properly determined and planned in during this phase. [redacted]

Acquisition/Development: During the first part of the acquisition / development phase, system planners define the requirements of the system. [redacted] Therefore, security requirements should be developed

at the same time. Determining security features, assurances, and operational practices can yield [redacted] This information needs to be validated, updated, and organized into the detailed security protection requirements and specifications.

Testing and Implementation: The information system's security category (i.e., Low Impact, Moderate Impact, or High Impact) determines the intensity and rigor of the effort applied in executing/completing the other components. The set of baseline controls that result from applying the Security Control Selection component to a High Impact information system [redacted]

Likewise, the assessment of controls that takes place in the Security Control Assessment component [redacted]

The objectives of the security test and evaluation (ST&E) are to:

- Uncover design, implementation and operational [redacted]
- Determine [redacted] security mechanisms, assurances and other properties to enforce the security policy
- Assess the degree of consistency between the system documentation and its implementation.

High impact systems require detailed testing [redacted] Testing typically includes [redacted] In addition, [redacted]

Operations and Management: Many security activities take place during the operational phase of a system's life. In general these fall into three areas: (1) security operations and administration; (2) operational assurance; and (3) periodic re-analysis of the security.

Operation of a system involves many security activities that need to be performed to assure the information and information systems are protected. These activities [redacted] are some examples.

High impact system may require continual scanning and updating of scanning software that captures new vulnerabilities. Moderate system [redacted] but high impact systems are required to have this capability. High impact systems are required to [redacted] to maintain an up-to-date, complete, accurate, and readily available baseline configuration of the information system. High impact systems have much more rigorous controls for the handling and disposal of media than moderate systems.

Disposition: The disposal phase of the computer system life cycle involves [redacted]. The big difference [redacted] is in the degree of rigor in which the information [redacted]

AT&T is required to track and document [redacted] high impact systems that have been [redacted] Additionally, the equipment [redacted] must be periodically tested to assure that it is operating properly. Measures may also have to be taken for the

future use of archive data that has been encrypted, such as taking appropriate steps to ensure the [redacted].

AT&T will frequently update the C&A supporting documentation as necessary and prepare supporting artifacts and evidentiary material in response to Government inquiries.

In addition, the C&A process is required to be expanded to address the additional test case development, C&A documentation development, results analysis, methods and procedures, and required supporting documentation.

AT&T will put into place enterprise [redacted] management, vulnerability scanning, and automated audits to satisfy the additional control requirements. For example, depending on the particular needs and demands of a particular HHH system, AT&T may add the following technologies, or equivalents, to meet certain requirements:

- [redacted] for automated network configuration and change management, and audit support.
- [redacted] for IT configuration and change management, and audit support.
- [redacted] management software for centralized security event aggregation, correlation, and analysis.
- Enhanced Audit log management and analysis, as well as level 3 authenticators for local access

1.4.13.9 NBIP-VPNS Subrate Ports

NB-IPVPN Subrate Port service, as described in the following sections, provides Agency Customers with the benefit of obtaining a NBIP-VPNS dedicated port with a bandwidth that is less than the access circuit bandwidth. This allows Agency Customers to purchase a NBIP-VPNS dedicated port bandwidth that most closely matches their requirements. Without this capability, the Agency Customer would have to purchase a NBIP VPNS dedicated port bandwidth that is equivalent to the access circuit bandwidth.

1.4.13.9.1 Service Description

The primary NBIP-VPNS components are MPLS Ports. Networx NBIP-VPNS Subrate Ports provide port bandwidths that are less than the access circuit bandwidth. Additionally, NBIP-VPNS Subrate Ports may support several Layer 2 protocols such as Point to Point Protocol (PPP), Frame Relay (FR), and ATM. **Table 1.4.13.9-1** summarizes the NBIP-VPNS Subrate Port characteristics.

SUBRATE PORT BANDWIDTH	SUPPORTED L2 PROTOCOLS	ACCESS CIRCUIT TYPE
[redacted]	[redacted]	[redacted]

Table 1.4.13.9-1: [redacted]

The subrate port bandwidth specifies the maximum available bandwidth supported by the NBIP-VPNS Subrate Port.

1.4.13.9.2 Availability and Service Enabling Devices (SEDs)

The NBIP-VPNS Subrate Ports are available in the CONUS region. No SEDs are required to deliver the NBIP-VPNS Subrate Port service.

1.4.13.10 EMNS Fixed Site VPN Services

The Fixed Site VPN Services provides Government Agencies' remote sites/small offices with a comprehensive and fully managed, secure dedicated remote access solution for connection back to an Agency Hub Site / Internet Data Center (IDC), utilizing the AT&T global IP backbone and other third party Internet Service Providers (ISP) as the transport network.

In addition to providing secure connectivity via the public Internet, the EMNS Fixed Site VPN Services provides each remote site/small office with Out-of-Band Management (OBM) capabilities.

1.4.13.10.1 Service Description

AT&T has designed the EMNS Fixed Site VPN Services to provide full management and security across the public Internet. The EMNS Fixed Site VPN Services is designed to provide a turnkey secure solution for remote sites/small offices to communicate back to applications hosted in an Agency Hub Site / IDC.

The components that comprise the EMNS Fixed Site VPN Services include:

- **Enhanced Service Enabling Device (SED) Services** – For each remote site/small office, customers will select the Enhanced SED Services which include the following:
  - **VPN Router/Switch** – As part of the EMNS Fixed Site VPN Services, AT&T will provide the remote site/small offices with the appropriate premise equipment. Depending on the requirement of each remote site/small office and access speed, the managed premise equipment configuration will consist of a VPN router and/or switch. Further, the LAN size is based on the number of Ethernet switch ports required as noted below:
    - X-Small LAN – Up to 8 switch ports

- Small LAN – 9-16 switch ports
- Medium LAN – 17-24 switch ports
- Large LAN – 25-48 switch ports

[redacted]

Conditions for EMNS Fixed Site VPN Services are:

- **Internet Connectivity** –Agency remote site/small offices will separately order AT&T's IPS as the primary network transport via analog dial, Wireless Fidelity (WiFi), Digital Subscriber Line (DSL) or dedicated facilities (fractional T1 up to OC3). As it necessitates, some remote site/small offices can utilize third party IPS broadband access.
- **Geographic Availability** – The EMNS Fixed Site VPN Services will be available to remote sites/small offices located in the continental United States (CONUS) and offshore US territories (OCONUS).

Figure 1.4.13.10-1 illustrates the overall EMNS Fixed Site VPN Services design with all of the components listed above.

Figure 1.4.13.10-1:

1.4.13.11 EMNS Extranet Connectivity Services

EMNS Extranet Connectivity Services provides the technical capabilities for extranet partners to access Government Agency sites/agencies. EMNS Extranet Connectivity Services can be provisioned either by AT&T directly to the extranet partner or by AT&T via the agency. In either case, an extranet partner will subscribe to the Enhanced SED Service and the ESMNS CLINs defined for EMNS Extranet Connectivity Services.

1.4.13.11.1 EMNS Extranet Connectivity Services – Service Description

AT&T's design for EMNS Extranet Connectivity Services is to keep Extranet partner traffic logically and physically separated from all other traffic, no matter if it is trusted or un-trusted. An Agency sees trusted traffic from Agency

locations while un-trusted traffic is viewed as traffic from non-Agency locations. Logically, trusted and un-trusted data will be configured as private and public VLANs. Each VLAN will have associated routing and security policies.

Figure 1.4.13.11-1 [redacted]

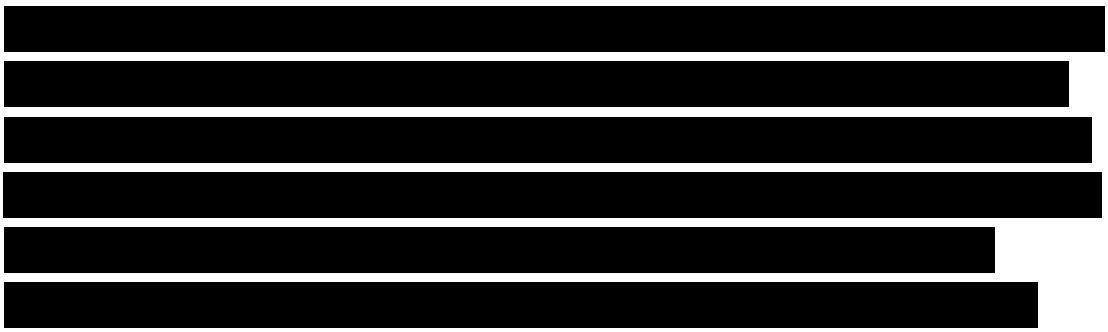


Figure 1.4.13.11-1:

The components that comprise EMNS Extranet Connectivity Services include:

- **Enhanced Service Enabling Device (SED) Services** – For Extranet partners, they will select the Enhanced SED Services for which AT&T will provide the extranet partners with the appropriate premise equipment, depending on the requirement of each extranet partner. The appropriate premise equipment will be provided to the extranet partner with the three components:

Conditions for EMNS Extranet Connectivity Services are:

- **Extranet Transport** – Extranet partners can access an Agency's network via the following transport methods:
  - MPLS based (NBIPVPNS)
  - IPS with added IPSec security
  - FRS
  - PLS

- Extranet Connectivity is not included with EMNS Extranet Connectivity Services.

Geographic Availability – The EMNS Fixed Site VPN Services will be available to remote sites/small offices located in the continental United States (CONUS) and offshore US territories (OCONUS).

1.4.13.12 NBIP-VPNS Premier Service

The NBIP-VPNSS Premier Service is a NBIP-VPNS service option that provides basic service capabilities beyond the capabilities of a standard NBIP-VPNS service offering.

Agencies are eligible to order NB-IPVPN Premier Service if they meet the following qualifications:

- A dual carrier diverse network

[redacted]

NB-IPVPN Premier Service consists of NB-IPVPN ports supporting a dual carrier diverse network and includes:

- Management of the equipment and NOC

[redacted]

- Enhanced SLAs
- Negotiated SLOs (provided to the Agency as a contract deliverable)
- Additional Agency-specific plans and deliverables (provided to the Agency as a contract deliverable)

Diversity is defined for NB-IPVPN Premier Service as multiple vendors providing a separate local access and network path for a circuit to a common customer building through a separate facility entrance into the building.

NB-IPVPN Premier Service and associated features are described in the following sections and must be ordered and implemented to build the NB-IPVPN Premier Service and become compliant with the Premier Service management functions and commitments.

A top-level Agency must establish NB-IPVPN Premier Service by ordering the NOC Management Set-up CLIN and outlining for AT&T the additional Agencies eligible for the Premier Service network. Once the top-level Agency identified the additional eligible Agencies, then any smaller sub-agencies may begin placing orders even though they individually do not qualify for Premier Service.

1.4.13.12.1 NBIP-VPNS Premier Service Port

The NBIP-VPNS Premier Service Port is a NBIP-VPNS option that provides key features that go above and beyond the capabilities of a standard NB-I-VPN port [redacted] Using the NBIP-VPNS Premier Service Port, an Agency can acquire a highly reliable and secure network that can outperform the typical NBIP-VPNS constructed network.

[redacted]

1.4.13.12.1.1 NBIP-VPNS Premier Service Port – Basic Capabilities

[redacted]

In addition to the basic capabilities, the NBIP-VPNS Premier Service Port bundles in Collocated Managed Network Service and SLAs.

[redacted]

1.4.13.12.1.2 Node Types Supported by NBIP-VPNS Premier Service Port

The NBIP-VPNS Premier Service ports are available in the following areas using dedicated access only.

- CONUS
- OCONUS
- Non-Domestic

The categories of Node types that are support by NBIP-VPNS Premier Service Port are defined below and dictate the SED types and configurations. The different SED types and configuration are designed to meet the varying traffic needs and the service availability requirements for each of the node types. The node types are as listed in **Table 1.4.13.12-1**:

TYPE	ACCESS CONNECTIVITY OPTIONS	CHARACTERISTICS	APPLICABLE AVAILABILITY*
Type 1: Very High Bandwidth High Availability Sites	[redacted]	Data Center or Computing Facilities that serve many Agency employees	[redacted]
Type 2: High Bandwidth High Availability Sites	[redacted]	Data Center, Computing Facilities or a large District type office; high number of other Agency employees use applications serviced by this site	[redacted]
Type 3: Large Critical Location	[redacted]	A large Critical Office houses a large number of Agency employees	[redacted]
Type 4: Standard Office	[redacted]	A standard Agency Field Office that has no need to deploy applications or house a large number of employees	
Type 5: Very Small Office	[redacted]	Remote Access	
Type 6: Mobile Office	[redacted]	Mobile location with connectivity through port facility when docked and satellite connectivity through CAM station when mobile	

[redacted]

Table 1.4.13.12-1: NBIP-VPNS Premier Service Port site node types vary form very large critical sites to very small and mobile offices. *The highest availability is achieved by the Agency by provisioning two carriers into a critical site. The NBIP-VPNS Premier Service Port ports are configured to support this multiple carrier option when required.*

Each site type described in **Table 1.4.13.11-1** requires Service Enabling Devices (SED). These devices include routers, packet shapers, security systems, and redundant power systems.

1.4.13.12.1.3 NBIP-VPNS Premier Service Port Basic Capabilities

The basic capabilities provided by the NBIP-VPNS Premier Service Port go beyond the capabilities of a standard NBIP-VPNS port. [redacted]

Using the NBIP-VPNS Premier Service Port ports, a highly reliable and secure network can be constructed.

1.4.13.12.1.3.1 DMVPN Multiple Node and Redundancy Support

In each NBIP-VPNS Premier Service Port enabled network, AT&T will support configuration and implementation, of a network-wide, robust, scalable

WAN. [redacted]

[redacted] **Figure 1.4.13.12-1.**

[redacted]

Figure 1.4.13.12-1: [redacted]

AT&T will provide Network Based IP-VPN ports that can be configured with multiple MPLS based Virtual Networks terminating in a single NBIP-VPNS Premier Service Port node. This will allow the Agency to operate several sub-networks within their overall NBIP-VPNS based infrastructure.

Each Agency DMVPN provided by AT&T will use an Agency-wide Network-based IP VPN for transporting IP packets between the Agency Nodes. [redacted]

1.4.13.12.1.3.2 NBIP-VPNS Premier Service Port Encryption and Security Mechanisms

[redacted]

The secure access implementation will follow the secure access plan as provided by the Agency. A description of the secure access implementation will be provided by AT&T to the Agency that describes the following:

[redacted]

- The implementation and capabilities of the security design, policies and controls as per the Agency's input.

1.4.13.12.1.3.3 Documentation and On-Going Updates

For Agencies running critical high availability NBIP-VPNS Premier Ports Service networks, documentation and on-going updates of the overall network infrastructure helps reduce potential outages. Documentation and on-going updates on the network architecture including technology and equipment types deployed at POPs. This documentation includes:

- the number and locations of POPs and PE routers including the connectivity between the POPs and PE routers with circuit route descriptions with transmission technology and the intermediate fiber junction points
- the methodology for engineering Agency traffic paths, primary as well as alternate, through the backbone
- the failure recovery mechanism deployed in the backbone at the layer 1 (transmission, e.g., SONET), at layer 2 (e.g., MPLS) and at layer 3 (e.g., IP layer)
- the redundancy scheme

Documentation and ongoing updates are provided to the Agency through the purchase of the NBIP-VPNS Premier Service Port.

1.4.13.12.1.4 NBIP-VPNS Premier Service - Collocated Managed Network Service

AT&T will provide Agencies with NBIP-VPNS Premier Service Collocated Managed Network Service that will optimize the performance of related Networx services. [redacted]

[redacted] NBIP-VPNS Premier Service - Collocated Managed Network Service is comprised of two primary components:

- Management of networking resources
- Monitoring of network performance

1.4.13.12.1.4.1 NBIP-VPNS Premier Service - Collocated Managed Network Service Service Management

AT&T's approach to NBIP-VPNS Premier Service - Collocated Managed Network Service is to engineer a managed network solution that meets the Government's requirements and, if required, provide the necessary data and tool sets. The NBIP-VPNS Premier Service - Collocated Managed Network Service is purchased with every NBIP-VPNS Premier Service Port provided by AT&T.

AT&T will provide a primary Agency NOC responsible for end-to-end installation, implementation, monitoring, management and trouble resolution, maintenance and repair of Agency services at a location chosen by the Agency. AT&T shall provide NBIP-VPNS Premier Service - Collocated Managed Network Service to support these functions at this Agency NOC.

[redacted]. **Table 1.4.13.12-2** pre[redacted]

MANAGEMENT DOMAIN	AT&T SHARED NBIP-VPNS PREMIER SERVICE - COLLOCATED MANAGED NETWORK SERVICE AND FIELD SUPPORT FUNCTIONS
Enterprise Level	[redacted]
DMVPN/Agency Nodes Level	
Access Level	
Network	

MANAGEMENT DOMAIN	AT&T SHARED NBIP-VPNS PREMIER SERVICE - COLLOCATED MANAGED NETWORK SERVICE AND FIELD SUPPORT FUNCTIONS
POP to Provider Edge (PE) Router Back-haul Connectivity	
Core (IP MPLS; NB IP VPN) Backbone	

Table 1.4.13.12-2: AT&T's NBIP-VPNS Premier Service - Collocated Managed Network Service Management Domains. *Detail of the management domain functions AT&T provides via NBIP-VPNS Premier Service - Collocated Managed Network Service.*

Table 1.4.13.12-3 details the AT&T Roles and Responsibilities for managing the Agency NOC as part of NBIP-VPN Premier Service - Collocated Managed Network Service.

ENGINEERING AND O&M FUNCTIONS	AT&T ROLE
Design and Engineering	
Transition and Implementation	
Support Enterprise Level Management	
Monitoring	
Trouble Resolution	
Trouble Ticketing	
Change Management	

ENGINEERING AND O&M FUNCTIONS	AT&T ROLE
Performance Management	[redacted]
Reports	[redacted]
Installation, De-installation, Upgrade, and Repair	[redacted]
Security	[redacted]

Table 1.4.13.12-3: AT&T's NBIP-VPNS Premier Service - Collocated Managed Network Service Management Functions. *Indicates the engineering, operations, and management functions AT&T provides via NBIP-VPNS Premier Service - Collocated Managed Network Service at the Agency NOC.*

Supported Node Types

[redacted]

[redacted] **Table 1.4.13.12-4.**

NODE TYPE	CHARACTERISTICS
Type 1: Very High Bandwidth High Availability Sites	[redacted]
Type 2: High Bandwidth High Availability Sites	
Type 3: Large Critical Location	
Type 4: Standard Office	

NODE TYPE	CHARACTERISTICS
Type 5: Very Small Office	[redacted]

Table 1.4.13.12-4: Supported Node Types. *The supported NBIP-VPNS Premier Service - Collocated Managed Network Service Node Types and their descriptions.*

1.4.13.12.1.4.2 NBIP-VPNS Premier Service - Collocated Managed Network Service Monitoring

AT&T will provide visibility into its network backbone (e.g., Access, POP, and IP MPLS network) in order to facilitate management of end-to-end network performance. [redacted]

1.4.13.12.1.5 NBIP-VPNS Premier Service Port SLAs

The NBIP-VPNS Premier Service Port features include custom Service Level Agreements. To verify the SLA, AT&T will collect the necessary network performance data and present the performance data results in a monthly SLA report. Specific the monthly SLA report for the NBIP-VPNS Premier Service Port feature are detailed in **Table 1.4.13.12-5**.

SLA	PERFORMANCE METRIC DETAIL
Repair and Maintenance Missed repair deadline results in Component invoice credit. Sites categorized into High and Normal types (based on the SOW SLA Success Measures). Metric applies to NBIP-VPNS Premier Service Port sites.	[redacted]
Overall Network Performance Five Network Performance measurements grouped as a single metric that indicates the quality of overall network provided by the Contractor. Non-performance (and associated credit) is based on missing any 2 of the 5 measures for consecutive months. Non-performance credit escalates for increasing number of consecutive months missed.	[redacted]
Service Availability Service Availability measures availability of service at individual Nodes, based on being out of	[redacted]

SLA	PERFORMANCE METRIC DETAIL
service (vs. degraded capacity). Availability is defined as ability to send or receive data from the LAN to any other Agency site (as allowed by Policy) over Access links for a calendar month period. The service availability metric is specific to availability of service at the service delivery point and consistent with the Requirements in SOW:	

Table 1.4.13.12-5: Service Levels for NBIP-VPNS Premier Service Port. *The NBIP-VPNS Premier Service Port Service Level Agreement and associated descriptions.*

1.4.13.12.2 NBIP-VPNS Premier Service – Connectivity to External Networks

NBIP-VPNS Premier Service - Connectivity to External Networks is available to Networx Customers that purchase NBIP-VPNS Premier Service Ports.

From each Agency Data Center location, AT&T provides network connectivity to selected external networks (other federal agencies, and state and local governments, commercial entities). Connectivity to external networks is provided using the following methods:

1.4.13.12.3 NBIP-VPNS Premier Service - Occasional Use Ports

NBIP-VPNS Premier Service - Occasional Use Ports are available to Networx Customers that purchase NBIP-VPNS Premier Service Ports.

NBIP-VPNS Premier Service - Occasional Use Ports provide connectivity to an Agency's temporary processing facilities such as a backup Network Operations Center (NOC) or other data processing facility. NBIP-VPNS Premier Service - Occasional Use Ports will have the same attributes as permanent use NBIP-VPNS Premier Service counterparts. [redacted] The Occasional Use Ports will allow an Agency to operate with emergency/backup processing locations without having to bear the full price of bandwidth to those sites when they are not in use.

NBIP-VPNS Premier Service - Occasional Use Ports will be permanently ready for an Agency's use. [redacted]

AT&T provides NBIP-VPNS Premier Service - Occasional Use Ports to customers that purchase NBIP-VPNS Premier Ports Service Collocated Managed Network Service and operate backup NOC or processing facilities. Access to the Agency's occasional use sites is not included in the price of the NBIP-VPNS Premier Service - Occasional Use Ports.

1.4.13.12.4 NBIP-VPNS Premier Service - Secure Internet Gateway

NBIP-VPNS Premier Service - Secure Internet Gateway is available to Networx Customers that purchase NBIP-VPNS Premier Service Ports.

[redacted]

1.4.13.12.4.1 NB-IP-VPN Premier Service - Secure Internet Gateway Basic Features

Agencies requiring an Internet gateway function will receive a highly available Internet Gateway designed to operate at the customer's Data Center location. The basic attributes of the Internet Gateway are as follows:

- The systems will provide a point for terminating Internet access at the Agency chosen/provided Data Center and will be highly available
- The NBIP-VPNS Premier Service - Secure Internet Gateway will provide protection from attack using various security mechanisms

[redacted]

AT&T provides NBIP-VPNS Premier Service – Secure Internet Gateway service at each Agency selected Internet gateway location using a specially selected set of Internet security tools and appliances. The Secure Internet

[redacted]

[redacted]

Figure 1.4.13.12-2.

Figure 1.4.13.12-2

Internet access is available via the Networx Internet Protocol Service (IPS) and enterprise networking is available via the Networx Network Based IP Virtual Private Network Service (NBIP-VPNS).

[redacted]

1.4.13.12.4.2 Service Availability and Equipment

The NBIP-VPNS Premier Service - Secure Internet Gateway is available to Agencies that have a data center location that acts as a common Internet access point for Agency sites. [redacted]

Utilizing AT&T's expertise in designing and deploying secure Internet gateway systems, the Agency can have access to the Internet without the large amounts of risk that are normally associated with internet access and usage.

1.4.13.12.4.3 NBIP-VPNS Premier Service - Secure Internet Gateway Functional Description

[redacted]

[redacted]

1.4.13.12.4.3.1 NBIP-VPNS Premier Service - Secure Internet Gateway Service Functions

Design and Engineering: Working with the Agency, AT&T will provide the design and engineering services required to deploy the Secure Internet Gateway infrastructure as an on-premise infrastructure in one or more Agency data center locations. Design and engineering services include review of current network traffic, performance, transport, hardware and software components; and an overall evaluation of the network topology, configuration, addressing, bandwidth, availability, scalability, reliability and disaster recovery requirements.

Secure Internet Gateway Capacity Planning: [redacted]

Establishing Secure Internet Gateway Sites: Upon completion of the NBIP-VPNS Premier Service - Secure Internet Gateway design and engineering solution, AT&T will establish the Secure Internet Gateway Sites in accordance with designed and engineered solution. [redacted]

[redacted]

Managing and Maintaining Secure Internet Gateway Sites: Upon deployment of the NBIP-VPNS Premier Service - Secure Internet Gateway, AT&T will provide ongoing management and maintenance of the Secure Internet Gateway. [redacted]

Response to Security Events: [redacted]

1.4.13.12.4.3.2 NBIP-VPNS Premier Service - Secure Internet Gateway Service Components

The NBIP-VPNS Premier Service - Secure Internet Gateway functions are supplied using SEDs that provide the following functions:

[redacted]

[redacted]

[redacted]

1.4.13.12.5 Rapid Router Deployment

For customers with a NBIPVPN Network provided by AT&T, AT&T offers a Rapid Router Deployment Service. This service is composed of components and activities to support pre-deployment management, deployment, and tear-down of [redacted] routers. These services are based on

terrestrial connectivity that is delivered through Telecommunications Service Priority (TSP) code ordering.

An Agency with this service is able to get pre-configured, tested, “ready-state” router delivery and installation within [redacted] after the service is ordered. This service is provided to Agency locations in CONUS, Alaska, Hawaii, and in four U.S. territories ([redacted] . Requests for comparable service in [redacted] or in non-domestic locations will be handled on an ICB basis in a separate contract modification. With this service, AT&T [redacted] and has responsibility for pre-deployment management, maintenance, deployment/tear-down, installing, and testing of the routers. These routers are an integral part of the Rapid Deployment Service and are included as part of this offer; therefore, no Service Enabling Devices (SEDs), as described in the Networx Universal contract, are required to support this offer.

On a per event basis, Agencies order router deployment and tear-down. The router deployment, together with the connectivity provided through the TSP ordering will allow an Agency with this service to communicate in an expedited timeframe.

With this service, ready-state routers are available and pre-configured to support the terrestrial bandwidths of 2xT1, 4xT1, and 6xT1. [redacted]) routers are used to support the TSP circuit installations. AT&T has configured the [redacted] router per the **Table 1.1.**

Table 1.4.13.12-6: [redacted]

The ready-state routers are maintained and deployed from dual deployment locations in order to facilitate deployment to a disaster location within [redacted] Deployment personnel are collocated near the equipment which enables efficient testing, technology updates, and maintenance of the equipment, as well as rapid response during a live deployment. Once deployed, the accommodations of deployed personnel are provided in the deployment plan for events that require long-term attendance. The field teams are truly self sufficient.

Due to the nature of disaster zones and the possibility of circumstances beyond the control of AT&T, the [redacted] and [redacted] SLAs as specified in the Networx contract cannot be offered for this Rapid Deployment Service. AT&T will use commercially reasonable best efforts to deliver routers within the timeframes specified in this Rapid Deployment Service.

In providing this service, AT&T will include use of certain equipment owned by AT&T that will be located at the location specified by the Authorized User*/DAR ("AT&T Equipment"). [redacted]

[redacted]

[redacted]

* As defined in the Networx Universal RFP Glossary, Section J

Table 1.2 lists the AT&T process for router deployment, initiated by a request from an Agency.

	AT&T PROCESS/TASKS FOR RAPID DEPLOYMENT SERVICE
[redacted]	AT&T shall prepare the routers for transportation. Upon receipt of written Agency notice for deployment, AT&T shall determine which deployment location is best positioned for router deployment to the impacted area. Routers at the specific deployment location will be packaged in "ruggedized" (e.g., Pelican) cases for transport. Routers will be equipped to support a 6xT1 interface, in case the Agency requests an upgrade from 2xT1 or 4xT1 while on-site. Note: Routers will be configured on-site; which eliminates the task of protecting data at the depots.
	AT&T will work with the Agency POC to identify Agency personnel for any site-specific configuration details during install.
	AT&T shall arrange for transportation of the router(s) and deployment team. Transportation options will be selected based upon most reliable means of transport, whether air or ground.
	AT&T shall make initial contact with the Agency, to identify exact address for delivery and installation. AT&T will determine any site or situation specific requirements that may complicate the delivery or installation, and plan accordingly. AT&T will transmit the deployment team's credentials to the Agency POC for access to site.
	AT&T dispatches router(s) and deployment team to the site.
	Travel to site, periodically providing arrival status to the service provider (AT&T), site POC and other Agency personnel as required.
	Upon arrival, AT&T will notify the NSEP service provider and Agency personnel and work with the Agency POC to identify the proper installation location for the router(s). AT&T will install and activate power on the router(s) after receiving any site-specific wiring layout and configuration requirements from on-site Agency POC. AT&T will commission router and coordinate operations with the Agency POC. AT&T will test and verify operations, troubleshooting configuration or connectivity issues, as necessary.
[redacted]	After router operation is stable and error-free, AT&T turns over router operations to Agency POC. AT&T shall receive signed acceptance document from Agency POC and will provide the Agency POC with an inventory checklist of the router(s) and other supplies.
Post Event	The AT&T deployment team leaves the site.
	AT&T shall record deltas to deployment, operational procedures or instructions, and produce deployment report.
	After AT&T receives written notification from the Agency POC that the emergency has ceased, normal network service is restored, and the equipment is no longer required, AT&T will commence the process to remove the router(s) and return them to the pre-deployment location. The Agency site POC provides any situation or site-specific information that constrains or affects recovery and removal.
	Transportation for the equipment and deployment team (removing the equipment) is arranged by AT&T. The AT&T deployment (removal) team travels to site.
	AT&T will stage the router for shipment back to the deployment site.
	AT&T shall inspect the router conditions against checklist.
	AT&T will logically disconnect the router from the network. AT&T will coordinate the disconnection of router with the Agency.
	The Agency POC agrees to transfer of equipment back to AT&T.

	AT&T PROCESS/TASKS FOR RAPID DEPLOYMENT SERVICE
	AT&T receives signed removal document (i.e., transfer of equipment) from the Agency POC.
	AT&T will physically uninstall the equipment.
	AT&T stages the equipment and packages it for shipment back to the origin deployment location.
	The equipment is transported back to deployment location.
	The AT&T deployment team travels to origin location.
	AT&T readies the router for potential redeployment within [redacted]
	The AT&T deployment team produces a recovery report within [redacted] from the return of the equipment, detailing what occurred and any additional information helpful for updating and revising plans, assessments and procedures. This report is provided to the POC/DAR and other personnel as identified by the Agency POC/DAR.

Table 14.13.12-7: Rapid Router Deployment Service Process.

1.4.13.12.5.1 Training and Maintenance Procedures

The AT&T team performs tests every six (6) months in order to keep all Rapid Deployment equipment operationally ready as well as keeping the deployment teams trained in deployment strategies. These tests are performed in a mock emergency situation so that processes and procedures can be examined and all of the equipment that may be deployed in a disaster situation can be tested.

Any parts of the equipment that do not perform properly in a test are replaced through the manufacturer's maintenance program. Any parts of the process to deploy that do not produce a valid test are re-examined for validity or personnel are re-trained on the process. After every test, both the process and equipment functions are analyzed against the expected results in the mock scenario in order to increase the effectiveness of a deployment in an actual disaster. A brief written report on the status of the pre-deployed equipment and testing results will be provided to the Agency POC within [redacted] following the conclusion of the testing exercise.

1.4.13.13 NBIP-VPN RAS – [redacted]

[redacted]

[redacted]

Figure 1.4.13.13-1.

Figure 1.4.13.13-1: NBIP-VPN RAS – SOHO.

1.4.13.13.2 Access Interfaces

1.4.13.13.3 Implementation

[redacted]

1.4.13.13.4 Agency Responsibilities

[redacted]

[redacted]