2.3.2 Network Management [L.34.2.3.2]

GSA and Agencies are provided with the ability to monitor the management, performance, and maintenance of Networx service offerings. In this module we demonstrate how GSA customers' service requirements are effectively managed across the five areas of the ISO model - fault, configuration, accounting, security, and performance.

L.34.2.3.2 Network Management; The offeror shall describe how it proposes to meet Government requirements specified in Section C.3.3.1, Network Management. The offeror shall describe its management, technical, and operational capabilities for each of the following network management functional areas: (a) Configuration, Management, (b) Accounting Management, (c) Fault Management, (d) Network Services Monitoring and Management. For all services proposed, the offeror shall describe its network management organization, resources, strategies, practices, policies, processes, procedures, tools, systems, reports and any other relevant capabilities to provide the Government with a high degree of confidence that the offeror has sound, effective, and adequate capabilities that meet Government network management requirements. For the network management areas above, the offeror shall describe its network management capabilities to provide the Government a high degree of confidence that the offeror will be a strong partner that understands the challenges that the Government faces in: (a) Managing the range of Networx services, (b) Meeting the needs of a large, heterogeneous, and geographically distributed user community, (c) Ensuring the performance and quality of Networx services, (d) Improving the quality of Networx services to its customers, (e) Minimizing the impact of Networx services changes to Government operations, (f) Planning for future growth, (g) Meeting changes in Government needs, (h) Ensuring real-time access to information regarding the health and performance of, mission-critical services. For Network Services Monitoring and Management, the offeror shall describe the solution's architecture, features, and functions that will be provided to the Government. This includes security features, support to the Government to install, configure, administer, and operate the solution, and the Networx services for which the solution is provided.
If the Offeror's approach to meeting Network Management requirements is different for optional services than for mandatory services, the offeror shall describe the differences in a separate optional services sub-section within the Network Management section of the Offeror's response.

The AT&T Networx solution is compliant in all areas required by GSA - fault, configuration, accounting, security, and performance. The solution includes a number of powerful platforms, described in **Table 2.3.2-1**.

The components of the system architecture, their functions, and benefits to GSA Customers are represented in **Figure 2.3.2-1**. [redacted] **Figure 2.3.2-1** [redacted] for each element of the GSA Customers' service, permitting fast, accurate root cause identification, avoiding downtime and reducing mean time to repair.

NETWORK MANAGEMENT SYSTEM ARCHITECTURE COMPONENTS

[redacted]

[redacted]

Table 2.3.2-1 Network Management System Architecture Components. *These components give GSA Customers high service availability, high service performance, a common tool set, and easy to access web portal.*

FIGURE 2.3.2-1: NETWORK MANAGEMENT SYSTEM ARCHITECTURE. ***AT&T'S NETWORK MANAGEMENT SOLUTION OFFERS GSA CUSTOMERS A COMPLETE SOLUTION.***

These architectural components provide GSA Customers with robust network management capabilities. Network management functions are accessed

through a secure web site that provides [redacted]

AT&T's network management solution is built upon reliability and performance. To achieve this, the physical and logical layers of the network are managed in reactive, proactive, and predictive manners. [redacted] **Figure 2.3.2-2**.

Figure 2.3.2-2: Network Management: Reliability + Performance. *AT&T's network management solution offers GSA customers outstanding reliability and performance by reactive, proactive, and predictive management of the physical and logical layers of the network.*

Global Network Operations Center (GNOC) and Global Technology Centers of Excellence (CoE)

The GNOC (pictured in **Figure 2.3.2-3**) is responsible for the overall network management of the Global AT&T Switched and Data Networks. The AT&T GNOC in Bedminster, New Jersey, in partnership with technology specific Centers of Excellence, form the largest, most sophisticated command-and-control and fault management centers of its kind in the world.

Figure 2.3.2-3: AT&T Global Network Operations Center (GNOC). *The GNOC is responsible for managing AT&T's Global Network.*

AT&T's GNOC, manages one of the largest and most complex networks in the world with the following features and traffic volumes:

- More than 2.75 billion circuit miles of transmission facilities
- 135 local circuit switches with real-time networking
- More than 300 million voice calls per day
- More than 15 million video customers
- Connects virtually every country and territory around the world
- More than 1,000 nodes supporting MPLS-based services
- Carries 4.4 petabytes of IP traffic per business day
- 24X7 centers monitoring over 125,000 routers and 750,000 LAN ports
- Provides managed hosting services from 26 Internet Data Centers (IDCs) worldwide

Assisting the GNOC are the Global Technology Centers of Excellence (CoE). The CoEs provide 24x7 surveillance of network elements supplied to the

Government; providing progress and event notification to the Customer Support Office (CSO) and Contractor's Program Organization (CPO). The CoEs perform asset management, including the availability of spare equipment, and perform logical configuration management. Network upgrades and change management are directly managed by the CoEs (this includes maintenance, capacity management, and activities of the on-site workforce). The GNOC and the CoEs' structure and functions are summarized in **Figure 2.3.2-4**. The people, processes, and network management tools of AT&T's solution enable the Government's Networx services to routinely maintain very high availability and performance. As proof of this for the **entire** year of 2004, the AT&T Global network had a reliability performance rating of between 99.991% and 99.998%. [redacted] **Figure 2.3.2-5**.

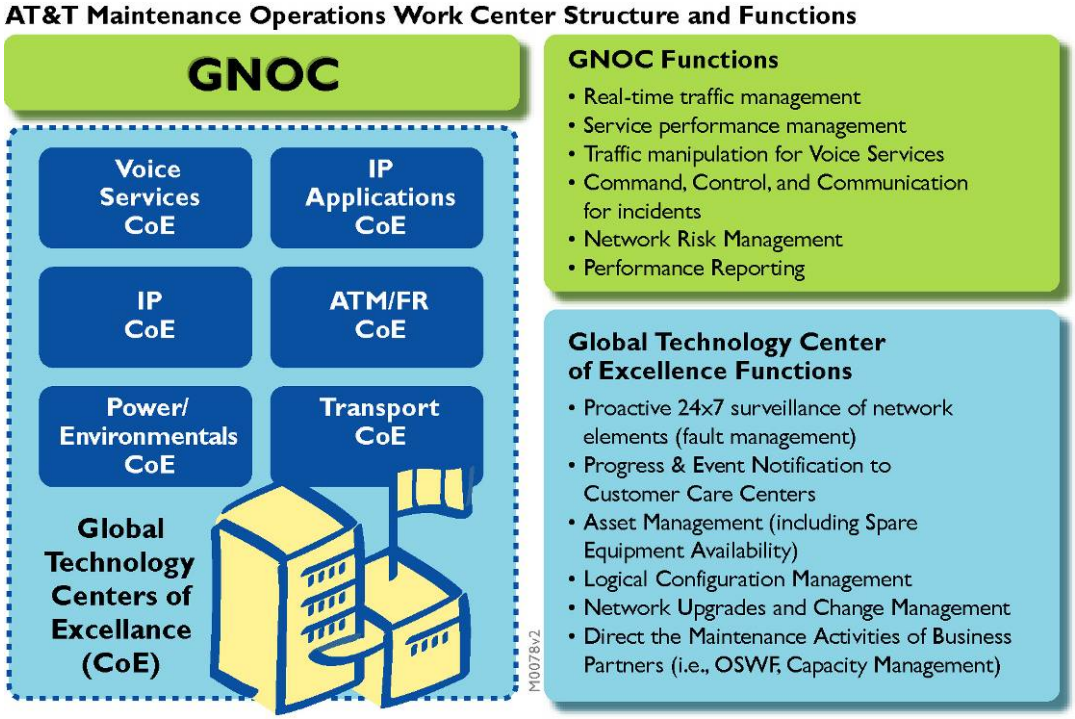


Figure 2.3.2-4 Network Maintenance Workcenter Structure and Functions. *GSA Customers leverage the people, process, and tools of one of the most reliable networks in the world.*

****
G L O B A L N E T W O R K O P E R A T I O N S C E N T E R
M O R N I N G R E P O R T
****
NETWORK PERFORMANCE FOR: TUESDAY, SEPTEMBER 6, 2005
****

AT&T VOICE SERVICES (PLATFORM VIEW)	Attempts	Defects	Daily DPM	YTD DPM	2005 Goal
U.S. Domestic TDM	405,048,028	2,030	5.0	71.0	65-100
- Metro TDM	56,821,576	838	14.7	31.8	N/A
- Inter-City TDM	348,226,452	1,192	3.4	77.8	N/A
International TDM	20,387,816	0	0.0	114.5	215-325
Call Vantage	1,166,440	317	271.8	1,525.4	TBD
BVoIP	609,795	TBD	TBD	TBD	115-175
GVoIP	TBD	TBD	TBD	TBD	TBD

AT&T TRANSPORT SERVICES	Custom Svc DS1 Minutes Available	Custom Svc DS1 Minutes of Outage	Daily DPM	YTD DPM	2005 Goal
Inter-City	1,076,525,160	4,714	4.4	13.5	TBD
Metro	166,252,320	2,815	16.9	49.1	TBD
International	22,262,100	0	0.0	94.4	75-100

AT&T Data Services	PVC Minutes Available	PVC Minutes of Outage	Daily DPM	YTD DPM	2005 Goal
Frame Relay	733,713,120	0	0.0	10.3	25-35
ATM	185,525,280	0	0.0	9.7	10-15
AGN	37,209,600	0	0.0	42.4	70-105
IPFR	123,534,720	0	0.0	35.2	40-50
GFN	17,830,080	0	0.0	51.3	75-110
Metro Layer 2 Packet	10,321,920	0	0.0	9.3	30-45

AT&T INTERNET PROTOCOL SERVICES - CBB	Port Minutes Available	Port Minutes of Outage	Daily DPM	YTD DPM	2005 Goal
CBB Network	76,839,840	0	0.0	72.3	40-90
IP Access (July)				33.7	N/A

AT&T INTERNET PROTOCOL SERVICES - CBB TEST PACKETS	UPS Packets Sent	UPS Packets Lost	Daily DPM	YTD DPM	2005 Goal
CBB Network	3,967,306	39	9.8	46.9	N/A

AT&T WEB HOSTING SERVICES	Customer Minutes Available	Customer Minutes of Outage	Daily DPM	YTD DPM	2005 GOAL
Hosting Monitored	1,869,120	0	0	42	25
Hosting Managed	502,560	0	0	58	75
Totals	2,371,680	0	0	45	

AT&T REPORTABLE INCIDENTS	Daily Total	YTD Total	2005 Goal
FCC Incidents	0	61	N/A
State PUC Incidents	0	16	N/A

M056lvl

Figure 2.3.2-5 GNOC Morning Report. *The AT&T GNOC in Bedminster, New Jersey, in partnership with technology specific Centers of Excellences, form the largest, most sophisticated command-and-control and fault management centers of its kind in the world.*

Managed and Outsourced Services

[redacted] with AT&T **Business**Direct. [redacted]

Table 2.3.2-2 [redacted]

	iGEMS People, Process, and Tools
People	[redacted]
Processes	[redacted]
Tools	[redacted]
GSA Customer Servicing	[redacted]

Table 2.3.2-2 iGEMS People, Process, and Tools. *GSA Customers solution for managed or outsourced services.*

[redacted]

Networx Security Management [L.34.2.3.2, C.3.3.1.2.1 Step 1]

The contractor shall provide network security and fraud prevention, detection, and reporting as specified in Section C.3.3.2, Security Management.

AT&T will provide network security and fraud prevention, detection, and reporting as specified in Section C.3.3.2, Security Management. The GSA

and Agencies have the commitment of AT&T to protect all information and resources from unauthorized access, disclosure, corruption, or disruption of service. This security policy is applicable to network elements, systems, applications and workstations as part of our service offerings.

[redacted]

[redacted] **Table 2.3.2-3.** [redacted] AT&T Labs are continually updating these capabilities as demanded to prevent security threats and vulnerabilities.

CAPABILITIES	AT&T PROCESS	NETWORX BENEFITS
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
Innovation [redacted]	AT&T Labs is the only organization of its kind, guided by the day-to-day	[redacted]

[redacted]	needs of AT&T's commercial and government operational business units. No other service provider on the globe maintains the type of research commitment to networking – and more specifically to MPLS – than AT&T.	[redacted]

Table 2.3.2-3: AT&T Carrier Grade Security Capabilities. *This table defines the specific capabilities, AT&T best practices, and the benefits to Networx customers.*

GSA and the Agencies are provided fraud prevention, detection and reporting through a variety of systems across all service types. [redacted]

Figure 2.3.2-6 [redacted]

Figure 2.3.2-6: [redacted]

[redacted] This capability enables investigators to pinpoint exact calls thereby assisting successful prosecution of fraudulent activities.

AT&T Networx Team member Cingular also provides fraud management capabilities for GSA customers. **Table 2.3.2-4** summarizes these capabilities.

FRAUD AREA	CINGULAR CAPABILITIES
[redacted]	[redacted]

Table 2.3.2-4: Cingular Fraud Management. *AT&T's wireless partner has extensive fraud management capabilities to safeguard Networx wireless customers.*

AT&T provides network security and fraud prevention, detection, and reporting as specified in the Networx Security plan and in § 2.3.3 (C.3.3.2) of the proposal, Security Management.

Configuration Management [L.34.2.3.2, C.3.3.1.2.2 Step 2]

Exact details of change control methodology vary, depending upon the customer service or infrastructure requirement (voice, private line, frame relay, ATM, IP, etc.). However, AT&T follows certain general principles irrespective of service. From an equipment perspective, [redacted] as small as a new card for a router, or an upgrade to router operating system software. Each network service such as, transport, private line, ATM, frame relay or IP, uses one or more test labs for pre-deployment and integration testing. Equipment tests answer the questions in **Table 2.3.2-5**:

EQUIPMENT VALIDATION AND VERIFICATION TESTS
[redacted]

[redacted]

Table 2.3.2-5: Equipment Validation and Verification (V&V) Tests. [redacted]

The length of the testing period depends upon the device to be deployed. For [redacted]

Once the equipment has passed these tests satisfactorily, it is certified and may be installed. Should the device fail to become certified, feedback is provided to the vendor detailing the test results. AT&T participates in joint planning meetings with the manufacturers and vendors to resolve the equipment faults that were revealed. These meetings assist the suppliers in enhancing the reliability and manageability of their products. To maintain the highest level of service reliability to the Government, devices that have not passed these rigorous tests are not installed in the network.

Prior to scheduling an installation of certified equipment in the network, a deployment plan is developed. When the deployment of equipment or enhancements to the network could affect the quality or availability of the Government's service during the installation, the affected Agencies are notified as well as the GSA at least 10 business days in advance of the work. For large scale changes 20 business days notice is provided. All upgrades are performed during an appropriate maintenance window as detailed in **Table 2.3.2-6**. As required, the GSA and Agencies are also notified in the same manner of network configuration upgrades that do not present a risk of service interruption. [redacted]

[redacted]

The contractor shall perform configuration changes in a standard maintenance window as stated in the contract to minimize service impact to the Government. **[C.3.3.1.2.2]**

AT&T will perform configuration changes in a standard maintenance window as stated in the contract to minimize service impact to the Government. GSA and the Agencies receive global network [redacted] ensuring high network performance and consequently better, more reliable service to the Government (**Table 2.3.2-6**).

COUNTRY	SCHEDULED MAINTENANCE TIMES
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

Table 2.3.2-6: Scheduled Maintenance. *Scheduled maintenance is planned worldwide.*

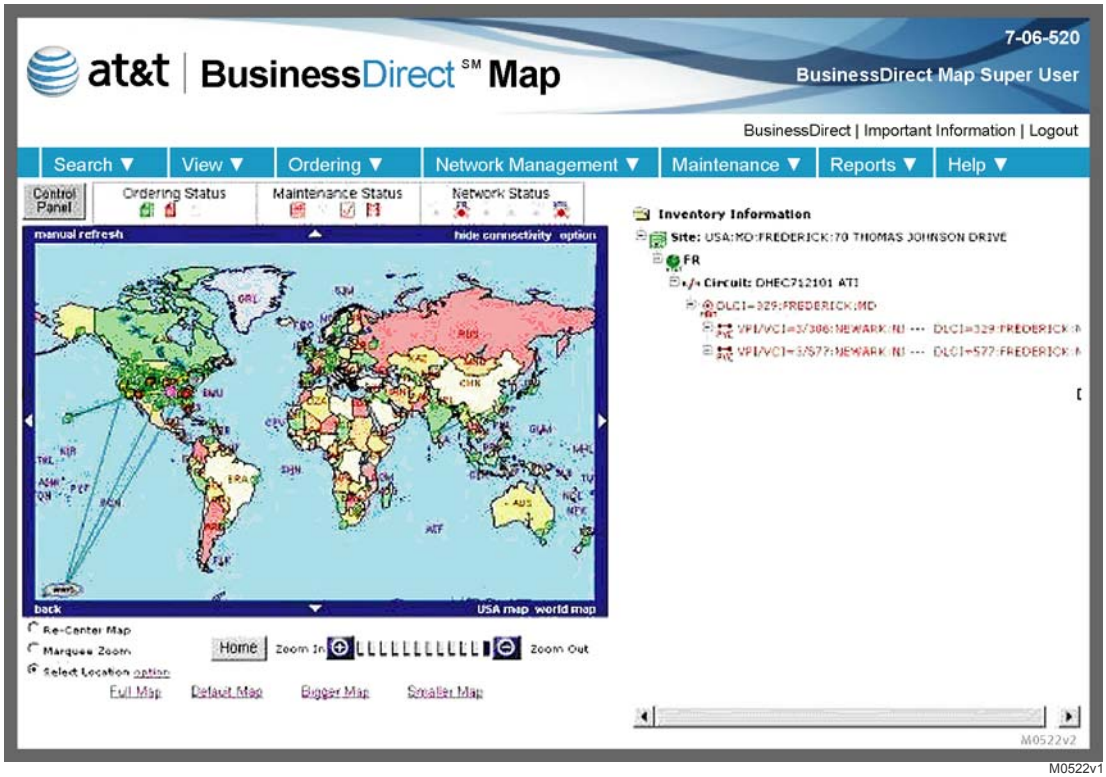
The scheduled maintenance windows are typically used to maintain many backbone sites. The existence of a scheduled maintenance time does not mean maintenance actually occurs during the period. The PMO and affected Agencies are notified at least 10 business days in advance prior to a scheduled network configuration change. In the event an emergency configuration change is required and if due to the nature of the emergency 10 days notice is not practical, AT&T then opens a trouble ticket. In addition the PMO and affected Agencies are immediately notified. In the event of a large scale configuration change the PMO and affected Agencies receive 20 business days notice. All configuration notifications are through e-mail, facsimile, or other agreed to method.

This database shall enable the Government to assess how network changes may impact services to Agencies. [C.3.3.1.2.2]
This database shall enable the Government to perform impact analyses on services during outages. [C.3.3.1.2.2]

AT&T will provide a database that will enable the Government to assess how network changes may impact services to Agencies and to perform impact analyses on services during outages. **Figure 2.3.2-7** is the AT&T **Business**Direct Map application, showing a representation of a customer network. [redacted]

[redacted]

[redacted]



M0522v1

Figure 2.3.2-7: AT&T Business Direct **Map Networx Customer Interface.** *Using the* [redacted] *for Networx customers, the Government can monitor trouble as well as manage network services through AT&T* ***Business****Direct Map.*

Accounting Management [L.34.2.3.2, C.3.3.1.2.3 Step 3]

The contractor's network accounting management system shall provide for the generation and distribution of usage data to support the contractor's detection, resolution, and reporting of network fraud, and abuse as well as optimization activity defined in Section C.3.4, Customer Service.

AT&T's accounting management system will provide for the generation and distribution of usage data to support AT&T's detection, resolution, and reporting of network fraud, and abuse as well as the optimization activity defined in Section C.3.4, Customer Service. AT&T's accounting systems capture data for all network service components employed to provide GSA

Customers' service to the service delivery point, including facilities that may be leased from 3rd party providers. [redacted]

[redacted] AT&T **Business**Direct®:

[redacted]

- [redacted] Sections C.3.3.1.4.1.3 and C.3.3.1.4.1.4.

For the mandatory Networx service types, [redacted] systems are utilized for the collection and distribution of usage data and they support the detection, resolution, and reporting of network fraud and abuse. [redacted] AT&T **Business**Direct, [redacted]

[redacted] AT&T **Business**Direct, [redacted] GSA customers in a pre-determined manner.

GSA customers using Land Mobile Radio (LMR) service [redacted] This is an effective fraud deterrent. Further, [redacted]

The traffic activity levels can be defined by the [redacted] to monitor key LMR parameters used to detect network fraud. Any activity that reaches defined thresholds is reported as the suspect event occurs, or on a periodic basis depending on the users requirement. The activity data can be retained and analyzed for significant changes using performance tools. [redacted] y.

AT&T Unified Messaging Service (UMS) generates call detail records (CDR) on all service components [redacted]

[redacted]

Customer usage reports [redacted] can be requested from the UMS Manager. These are reports are available to users [redacted]

Outbound calling (the initiation of calls from a subscriber's mailbox) [redacted]

A subscriber is authenticated in UMS [redacted] will be investigated by the GNOC.

Mobile Satellite Services (MSS) [redacted] (by the GNOC) if fraudulent use is suspected.

The contractor shall provide the Government with ad hoc traffic and usage reports to support the Government's telecommunications planning and avoidance of fraud, waste, and abuse. [C.3.3.1.2.3]
The contractor shall provide at a minimum Voice Traffic and Data Traffic reports. See Sections C.3.3.1.4.1.3, Voice Traffic Report and C.3.3.1.4.1.4, Data Traffic Report for report requirements. [C.3.3.1.2.3]

AT&T will provide the Government with ad hoc traffic and usage reports to support the Government's telecommunications planning and avoidance of fraud, waste, and abuse. The Networx management system provides GSA and Agencies with real-time traffic alerts, traffic reports, usage reports, and fraud reports for many service types. Traffic alerts take the [redacted]

Reports can be run online, on-demand, and then can be sent to e-mail addresses. Some reports may be scheduled for daily, weekly, or monthly presentation. AT&T will provide the Voice Traffic Reports in full compliance with Table C.3.3.1.4.1.3.3.1 Media/Transport/Format – Voice Traffic Report Sent to GSA. AT&T will provide the Data Traffic Reports in full compliance with Table C.3.3.1.4.1.4.3.1 Media/Transport/Format – Data Traffic Report Sent to GSA.

AT&T **Business**Direct users are provided with a large array of traffic reporting capabilities across their services such as the following:

- Daily summaries of inbound and outbound domestic long distance usage. Some service tools do not provide real-time status [redacted]
- Management monitoring reports for toll, PBX, and calling card fraud
- Monthly, weekly, daily and daily exception and recommendation reports

- Traffic statistics on peg counts, busy hour, overflow, trunks busy, blocking, average call length, [redacted]

The GSA and subscribing Agencies have access to management tools for Networx services to query and download accounting information through the secure Networx [redacted] with AT&T **Business**Direct. Ad hoc traffic and usage reports to support Government telecommunications planning and avoidance of fraud, waste, and abuse are accessible through **Business**Direct.

Fault Management [L.34.2.3.2, C.3.3.1.2.4 Step 4]

The contractor shall implement a process for Government-driven escalations as well as contractor-driven escalations to succeeding levels of management when a fault is not resolved within the required performance target or when the Government has indicated dissatisfaction with the way the contractor has handled the issue. [C.3.3.1.2.4]

AT&T will implement a process for Government-driven escalations as well as AT&T-driven escalations to succeeding levels of management when a fault is not resolved with the required performance target or when the Government has indicated dissatisfaction with the way AT&T has handled the issue. AT&T runs one of the world's largest and fastest growing IP networks with a Common Backbone network of nearly 500 high-speed routers. To keep the IP network up and running with the reliability, speed, and performance that is demanded by GSA Customers, we face three major challenges, namely:

[redacted]

To achieve these goals we need superior systems and tools that monitor the status of the IP Network at all times, alert when problems arise with traffic flows, delays or latency, diagnose the root causes of the problems, and model the effects of proposed solutions. In addition we need the capability for auto-provisioning new network elements and services, auto-configuring the network to meet ever changing traffic patterns, fault management techniques that rapidly restore the network on failures, a level of control of all network elements that enables us to offer Service Level Agreements (SLAs) to GSA Customers, and a unified database architecture that supports the network management and operation goals outlined above. The desired end state is the economic improvement of network performance and reliability. [redacted] **Figure 2.3.2-1**. [redacted] **Figure 2.3.2-8**. [redacted]

FIGURE 2.3.2-8 GFP ARCHITECTURE. [redacted]

[redacted] **Figure 2.3.2-9**.

[redacted]

[redacted] and shall be posted on the restricted area of the Networx services website. Only authorized personnel may view these notifications. Agencies may only view notifications about their impacted service. Any fault that affects more than one GSA Customer's service [redacted] a [redacted] that notifies the PMO (as well as the affected Agencies and the GSA). The PMO has [redacted] The PMO and customer Agencies have access [redacted]

FIGURE 2.3.2-9 NETWORK LAYER 1, 2, AND 3 CROSS DOMAIN FAULT CORRELATION ARCHITECTURE.

GSA CUSTOMERS OBTAIN POWERFUL FAULT CORRELATION CAPABILITIES THAT DRAMATICALLY REDUCE REPAIR TIME AND IMPROVE SERVICE AVAILABILITY.

Service affecting faults and the fault information communicated are defined in **Table 2.3.2-7**. Service outage resolution time and percentages for dispatched or non-dispatched personnel are defined in **Table 2.3.2-8**.

SERVICE AFFECTING FAULTS	FAULT INFORMATION
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

SERVICE AFFECTING FAULTS	FAULT INFORMATION
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
	[redacted]
	[redacted]

Table 2.3.2-7 Service Affecting Faults and Fault Information. *GSA Customers receive extensive notification of service affecting events.*

SERVICE OUTAGE RESOLUTION TIMES AND PERCENTAGES			
Outage Classification	***Personnel***	***Time Hours***	***%***
Outages measured at the Agency level	[redacted]	[redacted]	[redacted]
Outages measured at the Agency level	[redacted]	[redacted]	[redacted]
Any Networx service	[redacted]	[redacted]	[redacted]
Any Domestic Networx service	[redacted]	[redacted]	[redacted]

Table 2.3.2-8 Service Outage Restoration Times and Percentages.

The Networx Help Desk in the Customer Support Office (CSO), available 24X7, [redacted] **Figure 2.3.2-10** describes the operational flow of this function. The Time To Repair (TTR) is defined as the service restoration time as measured from the outage recorded [redacted] This TTR is reduced accordingly by any scheduled configuration or maintenance outage, any agreed to outage by the Government, or any Government caused delay.

Figure 2.3.2-10: Networx Help Desk Trouble Ticket Management. *GSA customers leverage commercial best practices in managing Networx customer trouble tickets.*

GSA customers can generate and track all trouble tickets electronically in [redacted] through AT&T **Business**Direct. Updates are provided as a function of the severity of the problem. **Table 2.3.2-9** defines the response notifications.

SEVERITY	DESCRIPTION	RESPONSE (TROUBLE TICKET UPDATE)
1	A critical problem stops a Networx provided service or circuit from functioning. The network or application is unusable.	[redacted]

SEVERITY	DESCRIPTION	RESPONSE (TROUBLE TICKET UPDATE)
2	Major problem has a severe impact on a customer's business, but does not stop it from functioning. The network or application is degraded and the customer is partially unable to work productively.	[redacted]
3	Minor problem with limited impact on a customer's business.	[redacted]
4	No problem – a customer's business is not impacted; there is no significant impact to the user. Incident may be a request for service information or a suggestion.	[redacted]

Table 2.3.2-9: AT&T response notifications. *As service faults are entered into the trouble ticketing system, notifications are handled as described in section C.3.4.2 Trouble and Complaint Handling.*

The escalation process for notification consists of a set of Tiers (levels). [redacted] CSO [redacted] Problems must be resolved in the minimum timeframes shown in **Table 2.3.2-10**. If not then the problem is escalated as in **Table 2.3.2-10**. Table 2.3.2-10 is also followed for Government driven escalations. Status to appropriate personnel within the Government will be provided in the same timeframes as the escalation progresses.

ESCALATION LEVEL	REPORTING CRITERIA	REPORTING FREQUENCY	AUTHORITY
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]

Table 2.3.2-10: Contractor Driven and Government Driven Trouble Ticket escalation procedures. *Networx customers are assured of appropriate attention due to rapid escalation notifications through the AT&T organization.*

The contractor shall resolve each service outage for any Networx service, with the exception of Fixed Satellite Service (FSS), within 8 hours for restoration requiring dispatching of personnel except for non-domestic SDPs. The contractor shall resolve each service outage for FSS within 72 hours for restoration requiring dispatching of personnel. [C.3.3.1.2.4]

AT&T will resolve each service outage for any Networx service, [redacted] requiring the dispatching of personnel [redacted]. AT&T

[redacted]

Performance Management [L.34.2.3.2, C.3.3.1.2.5 Step 5]

The [redacted] provides the PMO and GSA Customers with an identical set of service performance reports as commercial customers receive. These are available through AT&T **Business**Direct. Agency performance reports are available to those individuals with access permission from the specific Agency. They include SLA, usage, availability, Quality of Service, and real-time performance exception reports. Metrics are collected across all key

performance indicators (KPI) including [redacted] Any credits associated with service performance not meeting Networx requirements are established by [redacted] information.

The [redacted] platform is integrated into the network service, element management system (EMS), and operational support system (OSS) layers. At the network service layer there is integration with the access network, the core network, and the Internet. [redacted] **Figure 2.3.2-11** [redacted]

Figure 2.3.2-11 [redacted] **Architecture.** *GSA Customers receive electronic performance reports across their KPIs.*

Network Services Monitoring and Management

[L.34.2.3.2, C.3.3.1.2.6 Step 6]

The contractor shall provide a Network Services Monitoring and Management capability to provide real-time information regarding the health of the contractor's network as it applies specifically to the services the Agency has selected for this option. [C.3.3.1.2.6]
The contractor shall provide a Network Services Monitoring and Management capability to provide real time informational updates of the status of problem resolution efforts within the contractor's Trouble Management System as it applies specifically to the services for which the Agency has selected this option. [C.3.3.1.2.6]
The contractor shall provide additional hardware, software, and other means of access as determined by the contractor to provide this capability. [C.3.3.1.2.6]

AT&T will provide a Network Services Monitoring and Management capability to provide real-time information and informational updates regarding the health of the AT&T network and the status of any associated problem resolution efforts within AT&T's Trouble Management System as they apply specifically to the services the Agency has selected for this option. Service-specific real-time fault notification, traffic-reporting, and SLA reporting capabilities are defined in **Table 2.3.2-11**. Service independent traffic and

SLA reporting mean that the traffic and SLA information is collected independent of the service, but applies to the service (many services operate on common facilities). [redacted] AT&T **Business**Direct presents the Agencies with the network services monitoring and management functionality

for the services in **Table 2.3.2-11**. [redacted] **Table 2.3.2-11**. The capabilities defined in **Table 2.3.2-11** are available through two separate applications accessible via **Business**Direct. Real time notifications are provided via the **Business**Direct Map (BD Map) application. [redacted]

SERVICES TYPES	SERVICE	VIA BD MAP REAL TIME NOTIFICATIONS (C.3.3.1.2.6)	VIA E-MTCE REAL TIME TRAFFIC AND SLA REPORTING (J.13.1)
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]

SERVICES TYPES	SERVICE	VIA BD MAP REAL TIME NOTIFICATIONS (C.3.3.1.2.6)	VIA E-MTCE REAL TIME TRAFFIC AND SLA REPORTING (J.13.1)
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	[redacted]
	[redacted]	[redacted]	
	[redacted]	[redacted]	
		[redacted]	
		[redacted]	
		[redacted]	
		[redacted]	

Table 2.3.2-11: Service-Specific Reports Available. [redacted]

Real time informational service updates (fault notification, traffic, and SLA reporting) and the status of problem resolution efforts are communicated to GSA Customers through [redacted]. This includes KPIs for each service the Agency has selected (**Figure 2.3.2-11**). GSA Customers are able to perform their own KPI measurement if desired [redacted] Access to Agency real-time informational service updates is only available to those individuals with appropriate access permission from the specific Agency.

GSA Customers will have access to the eMaintenance application within the **Business**Direct® web portal. This application includes real time informational updates of the status of problem resolution efforts within our Trouble Management System as it applies specifically to the services the Agency has selected for this option.

BusinessDirect is a worldwide-web accessible portal provided to authorized Government users and is Internet accessible requiring no additional hardware or software.

Network Management Capabilities and Methodologies [L.34.2.3.2]

For all services proposed, the offeror shall describe its network management organization, resources, strategies, practices, policies, processes, procedures, tools, systems, reports and any other relevant capabilities to provide the Government with a high degree of confidence that the offeror has sound, effective, and adequate capabilities that meet Government network management requirements.
For the network management areas above, the offeror shall describe its network management capabilities to provide the Government a high degree of confidence that the offeror will be a strong partner that understands the challenges that the Government faces in:
(a) Managing the wide range of Networx services, (b) Meeting the needs of a large, heterogeneous, and geographically distributed user community, (c) Ensuring the performance and quality of Networx services, (d) Improving the quality of Networx services to its customers, (e) Minimizing the impact of Networx services changes to Government operations, (f) Planning for future growth, (g) Meeting changes in Government needs, (h) Ensuring real-time access to information regarding the health and performance of mission-critical services
For Network Services Monitoring and Management, the offeror shall describe the solution's architecture, features, and functions that will be provided to the Government. This includes security features, support to the Government to install, configure, administer, and operate the solution, and the Networx services for which the solution is provided.

As a benefit to the Government new management tools and technology providers are constantly evaluated to enhance network management capability and functionality when demanded. [redacted] development and systems engineering organizations maintain OSS (GFP[redacted] Laboratory facilities with the

latest network and computing equipment, as well as other resources such as technical libraries, membership in professional organizations, and attending conferences are available to the OSS research and development team. This team applies industry best practices to evaluate, prototype, and test proposed technology enhancements as shown in **Table 2.3.2-12**.

Life-Cycle maintenance and support for the network management platform is provided by OSS Research & Development. These organizations provide the following technical support functions:

[redacted]

[redacted]

Table 2.3.2-12 presents network management capabilities and methodologies. **Table 2.3.2-13** describes why AT&T provides a high degree of confidence maintaining we are a strong partner for GSA.

AREA	DESCRIPTION
Network Management Organization	AT&T Labs, OSS lifecycle management organizations, Government Solutions Enterprise Management [redacted]
Resources	[redacted] AT&T has a wide range of commercial offerings and integration experience. AT&T operates one of the largest networks in the world.
Strategy	[redacted]
Practices	[redacted]
Policies, Processes, and Procedures	[redacted]
Tools	[redacted]
Systems	[redacted] AT&T **Business**Direct™
Reports	[redacted]
Other Relevant Capabilities	Customers may function in a shared or dedicated environment. In 2004 AT&T received the Yankee Group's #1 Ranking of Telecommunications Service Providers, and ranked number one by earning top scores in Corporate Reputation, Sales and Marketing, Technical Competence, and Service and Support.

Table 2.3.2-12: Overarching Network Management Capabilities and Methodologies. *Today, AT&T manages the wide range of Networx services across a large and diverse marketplace and has the capabilities to meet Government network management requirements.*

NETWORK MANAGEMENT CAPABILITIES	HOW DO AT&T'S CAPABILITIES PROVIDE THE GOVERNMENT A HIGH DEGREE OF CONFIDENCE THAT THE OFFEROR WILL BE A STRONG PARTNER THAT UNDERSTANDS THE CHALLENGES THAT THE GOVERNMENT FACES IN?
Managing the wide range of Networx services	[redacted]
Meeting the needs of a large, heterogeneous, and geographically distributed user community	[redacted]
Ensuring the performance and quality of Networx services	[redacted]
Improving the quality of Networx services to its customers	[redacted]
Minimizing the impact of Networx services changes to Government operations	[redacted]
Planning for future growth	AT&T makes annual investments [redacted] in the network management areas. AT&T Labs have been awarded 128 patents over the last 2 years. More than 80% of the Labs work is in the development of new services and the solution of important business requirements.
Meeting changes in Government needs	[redacted] GSA Customers receive the benefit of proven change management practices.
Ensuring real-time access to information regarding the health and performance of mission-critical services	[redacted]

Table 2.3.2-13: Strong Partner for GSA. *Here we describe the capabilities of AT&T's solution and how we will meet the challenges the Government faces.*

Security features were discussed in the Networx Security Management (C.3.3.1.2.1) above. AT&T will provide support to GSA Agencies directly through the CPO and CSO to install, configure, operate, maintain, and administer the network management solution for Networx services.

If the Offeror's approach to meeting Network Management requirements is different for optional services than for mandatory services, the offeror shall describe the differences in a separate optional services sub-section within the Network Management section of the Offeror's response.

AT&T's approach to meeting GSA's network management requirements for optional services is identical to its approach for GSA's network management requirements for mandatory services.

Summary

GSA customers have access to future services and business practices because of substantial annual R&D investments in the telecommunications technology environment. Our dedicated integration, development, life-cycle support, and operations support teams have the primary goal of enabling GSA Customers to focus their resources on accomplishing their missions more effectively and efficiently. **Table 2.3.2-14** summarizes the features of our solution and the benefits to GSA.

FEATURES	BENEFITS
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]
[redacted]	[redacted]

FEATURES	BENEFITS
	[redacted]
[redacted]	[redacted] AT&T Labs [redacted] GSA customers have access to future services, practices, and solutions they need as their requirements change.
Technological Refresh	[redacted] This gives GSA customers regular predictable upgrades to maintain technological currency and minimizes impact to Government operations.
Scheduled Worldwide Maintenance and Service Change Notifications	[redacted] This improves operational efficiency, and minimizes impact to Agency missions.

Table 2.3.2-14: Features & Benefits. *The AT&T network solution provides GSA customers with conspicuous lifecycle and service management value.*

Gartner

AT&T is the only Network Service Provider (NSP) to be listed in the "Leader Quadrant" in all four of the Network Service Provider Magic Quadrants covering Europe, Asia Pacific, and the U.S.

Gartner Group 2004

2.3.2.1 Enhanced Managed Network Service

The Enhanced Managed Network Service (EMNS) is a bundled service offering comprised of several different Network service components:

- Enhanced NB-IPVPN
- Managed Network Service
- Enhanced Internet Access Security Services (EIASS)
- Modem Management (a sub-component of EIASS)
- Managed Firewall Service (Optional)
- Intrusion Detection Protection Services (Optional)
- Anti-Virus Management Service (Optional)
- Dedicated – Directory Hosting Service (DHS) (Optional)

All of these services, described in Technical Volume I, must be ordered and implemented to build the EMNS service and become compliant with the EMNS management functions and commitments.

2.3.2.2 EMNS Managed Reports & Data

Management reports for Agencies with an EMNS network consisting of a two-category site configuration in over 500 locations will contain the following characteristics and deliverables:

1. Real-time, web-based visibility into network management statistics and network configuration information on the network through a secured portal. The visibility will include a view of network performance statistics, capacity utilization, fault management, health monitoring and similar information. Reports will be provided both on a regular and ad hoc basis.
2. Real-time, read-only views into configuration settings for all provider equipement (routers, switches, firewalls, IDS, etc.)
3. Week-to-Date, Month-to-Date, and Year-to-Date statistics available through the secured portal and will include the following:
   - Access Circuit and router statistics (for each site)
   - Peak bandwidth utilization
   - Hourly average bandwidth utilization
   - Edge/access router CPU utilization
   - Average ping response time between the site access router and the nearest core backbone router
   - Average ping response time between two pre-defined access routers (within each Agency or sub-Agency)
   - Traffic breakdown up to the port level; e.g. HTTP, FTP, etc., (along with the bandwidth consumed and the source and destination IP addresses)
   - Ability to build and run ad hoc custom reports on managed service provider systems in real time
4. Backbone circuit and router statistics

- Peak bandwidth utilization of all Government traffic between core backbone routers
- Hourly average bandwidth utilization

5. AT&T will meet with the Government Agency bimonthly during the first year of an EMNS implementation and quarterly thereafter to provide and discuss utilization and trending reports and capacity planning services to maintain and improve site service levels. Automated alerts will be provided when average utilization exceeds 60% of total capacity at any site. Reports will include the site and recommend actions for improving capacity and performance. Notifications will be provided for any access circuit utilization exceeding 30% for four (4) or more hours per day at any site for five (5) or more days in a month.

2.3.2.3 EMNS Security Services Logs and Reports

Security logs and reports for Agencies with an EMNS network will contain the following characteristics and deliverables:

- Firewalls and intrusion detection systems (IDS) provide audit log tracking of all client transactions (including all NIST 800 series recommended data elements).
- Provide audit log access to the appropriate Government personnel.
- Provide log files to the Government via a secure data feed.
- Archived audit logs will be maintained for a minimum of five (5) years and are subject to request for retrieval by authorized Government personnel.
- Archived audit logs will not be destroyed without the prior written approval of the authorized Government personnel.
- All archived audit logs will be encrypted according to FIPS 140-2 encryption standard for unclassified but sensitive information.

- Firewall and IDS will be capable of displaying event information and sending management and event statistics to a centralized management tool/server.
- Central management tool/server will be able to generate customized reports of event information in both raw (e.g. comma delineated, etc.) and web-based formats and will be compatible with security management system applications.
- Feed ID sensor output, firewall audit logs and alarms, real-time Net flow compatible data feeds (from edge devices) to the Government's security Operations Center.

2.3.2.4 EMNS Alarm Notification

Alarm notifications for Agencies with an EMNS network will contain the following characteristics and deliverables:

- Alarm notifications will be sent via voice and email to the Agency for network performance degradation and security breaches. The thresholds for email notification will be coordinated with the Government.
- Advisory email messages will be sent to the impacted government agencies when network service affecting issues are detected.
- Agencies will have the capability to update the alarm notification database.

2.3.2.5 EMNS Archive System Events

For Agencies with an EMNS network, AT&T will store all system event log files for firewalls, IDS, smart switches, and routers for one (1) year using on-line media, and for at least 2 (two) additional years on off-line electronic/optical/magnetic storage media and as per government guidelines. Firewall audit logs will be stored for Government review for a period of five (5) years. Archived audit logs will not be destroyed without prior written approval

of the authorized Government personnel. All archived audit logs will be encrypted according to the appropriate FIPS standards.

2.3.2.6 EMNS Network Management

For Agencies with an EMNS network, AT&T will notify the DAR by email or call of any problems occurring within the AT&T network that could potentially impact the quality or availability of the EMNS service.

For Agencies with an EMNS network, the following maintenance parameters apply:

- A quarterly maintenance review schedule for routine maintenance activities will be submitted 15 calendar days before the start of each quarter.
- 30 minute or less notification of emergency maintenance activities will be provided prior to working unscheduled maintenance.
- Network maintenance will be delayed during agency emergencies based on immediate notice and busy seasonal periods based on the quarterly maintenance review schedule.
- Service impacting EMNS maintenance activities will be performed upon approval by the agency based on the agreed Quality Control Plan schedule and timeline.
- Scheduled EMNS maintenance activities will be suspended at the request of the agency given a minimum four (4) hour notice.

2.3.2.7 EMNS Network Configuration Changes

For Agencies with an EMNS network, the following Network Configuration Response Times apply:

TYPE OF CHANGE	EMERGENCY TYPE	INTERVAL
Soft/logical changes	Emergency	12 hours
Soft/logical changes	Non-Emergency	14 Calendar Days
Hardware changes	Emergency	24 hours
Hardware changes	Non-Emergency	14 Calendar Days

Table 2.3.2.7-1: Network Configuration Response Times. *This table identifies emergency and non-emergency changes and the corresponding response times.*

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]

[redacted]