1.7.1 Cellular/Personal Communications Services (CPCS) [C.2.14.1]

AT&T has teamed together with Cingular Wireless (hereafter, Cingular), to deliver premium wireless mobility services that satisfy Agencies' Cellular/Personal Communications Service (CPCS) requirements. The Cingular CPCS offering includes advanced services, the widest available domestic coverage area, comprehensive worldwide roaming capability, as well as a broad choice of subscriber equipment. AT&T's Customer Service Support provides Agency personnel access to the latest mobility tools required to stay connected and productive while on the move.

1.7.1.1 Technical Approach to Wireless Services Delivery [L.34.1.7.1]

1.7.1.1.a Approach to Service Delivery

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

Cingular offers a nationally implemented 2.5G wireless network, based on Global System for Mobile Communications (GSM) and General Packet Radio Service/Enhanced Data Rates for GSM Evolution standards, that provides a full suite of services including voice, short messaging service (SMS), multimedia messaging service (MMS) as well as mobile data. To meet the diverse needs of the Agencies, Cingular offers a comprehensive service that complies with the CPCS Networx requirements. **Figure 1.7.1.1-1** provides a representation of the CPCS services that are available to Agencies. Cingular's approach to providing high-quality wireless services to Agencies is summarized in **Table 1.7.1.1-1**.

APPROACH	DESCRIPTION
Spectrum acquisition	Cingular has acquired the bandwidth required to offer a premium wireless service to its subscribers

APPROACH	DESCRIPTION
Service coverage	Cingular has built out its network to offer comprehensive coverage of the U.S., and has roaming relationships with other GSM providers throughout the world
Standards based network	The Cingular wireless network is built upon the GSM standard, by far the world's most popular cellular architecture, providing economies of scale that only a 1.4 billion subscriber marketplace can provide
Multilayer security	Strong security algorithms protect subscriber's communications and identities, using a variety of advanced techniques at multiple layers of the network
Quality and performance measurement	Cingular employs advanced tools and techniques that measure, report, and act on statistical data regarding the performance of the network
Advanced data services	Cingular has pioneered the implementation of advanced data services that enable new high-speed applications in all of the wireless service area

Table 1.7.1.1-1: Cingular Cellular Networking Approaches. *Cingular's approaches to building wireless networks provide Agencies with an outstanding CPCS service.*

Cingular's service area is among the largest in the world, offering roaming in 179 countries for voice and 94 countries for data and is the most comprehensive in North America, as shown in **Figure 1.7.1.1-2.**

[redacted] (**Figures 1.7.1.1-3 and 4**). This powerful combination of RF spectrum together with coverage and frequency reuse capability allows the Cingular network to deliver Agencies more services and more bandwidth throughout the entire US.

Figure 1.7.1.1-3 & 4: Adequate Spectrum. *Cingular has the spectrum and coverage necessary to deliver advanced services throughout North America, averaging over twice the available spectrum and cell sites of some competitors in top markets.*

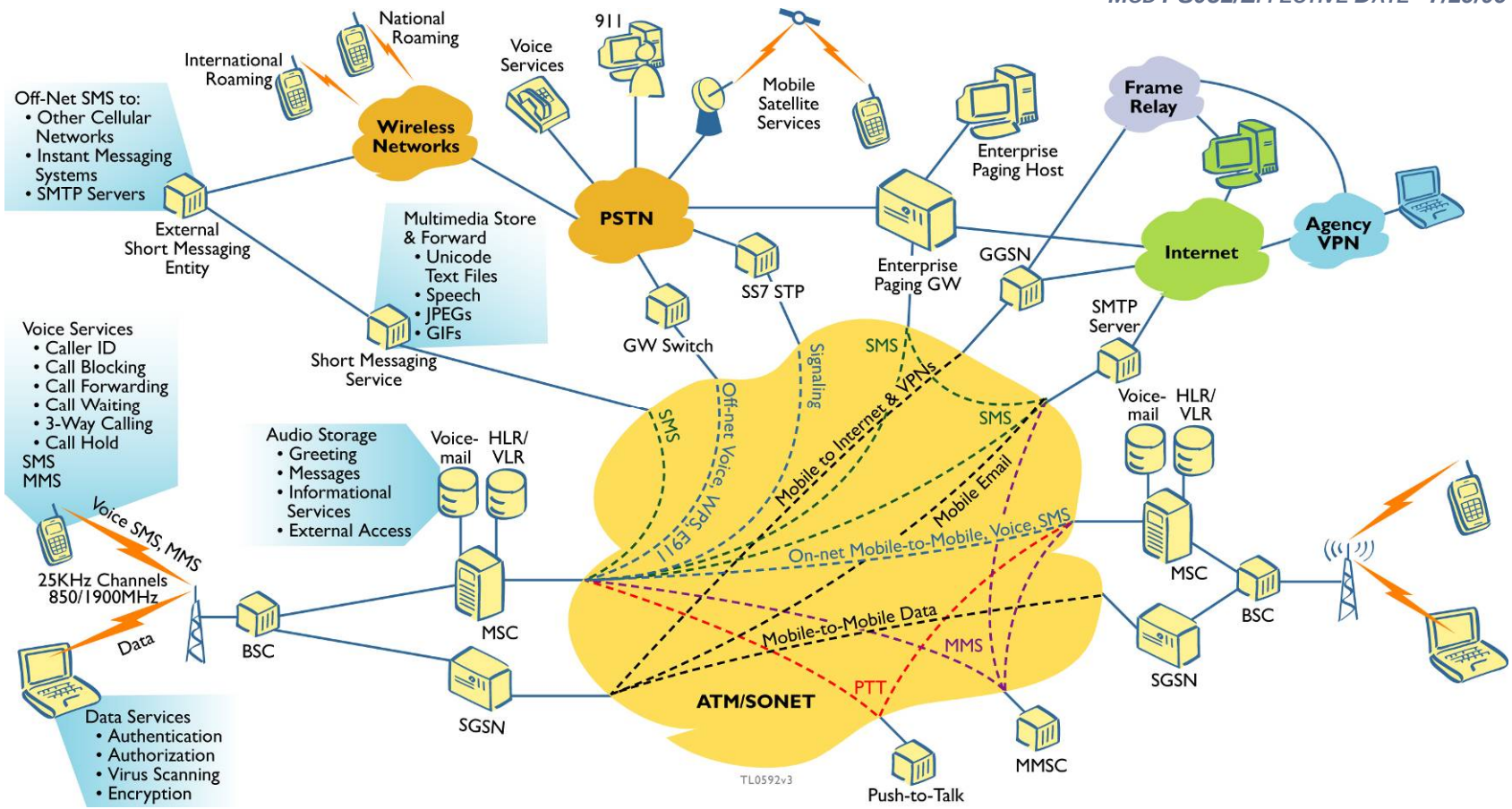

National Roaming
International Roaming
Voice Services
911
Mobile Satellite Services
Frame Relay
Enterprise Paging Host
Off-Net SMS to:
• Other Cellular Networks
• Instant Messaging Systems
• SMTP Servers
Wireless Networks
PSTN
Internet
Agency VPN
External Short Messaging Entity
Multimedia Store & Forward
• Unicode Text Files
• Speech
• JPEGs
• GIFs
SS7 STP
Enterprise Paging GW
GGSN
GW Switch
SMTP Server
Short Messaging Service
Voice Services
• Caller ID
• Call Blocking
• Call Forwarding
• Call Waiting
• 3-Way Calling
• Call Hold
SMS
MMS
Signaling
SMS
Off-net Voice
WPS 911
Mobile to Internet & VPNs
SMS
Mobile Email
Voice-mail
HLR/ VLR
Audio Storage
• Greeting
• Messages
• Informational Services
• External Access
Voice SMS, MMS
On-net Mobile-to-Mobile Voice SMS
25KHz Channels 850/1900MHz
Data
BSC
MSC
Mobile-to-Mobile Data
MMS
PTT
SGSN
ATM/SONET
Data Services
• Authentication
• Authorization
• Virus Scanning
• Encryption
MMSC
Push-to-Talk
TL0592v3

Figure 1.7.1.1-1: Network [redacted]

Figure 1.7.1.1-2: Nationwide Coverage. *The Cingular network offers the most comprehensive coverage of any domestic wireless network.*

Cingular is aggressively upgrading the network with new high speed data capabilities as it move towards a fully implemented third generation (3G) architecture (**Figure 1.7.1.1-5**). Currently, the network offers GPRS/EDGE in all served markets, and Universal Mobile Telecommunications System (UMTS/ High-Speed Downlink Packet Access (HSDPA) upgrades are being implemented now.

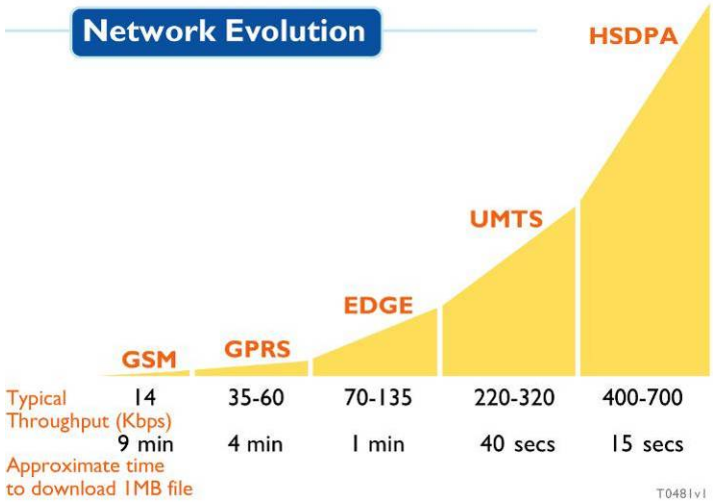


Figure 1.7.1.1-5: Increasing Data Speeds. *The Cingular network meets Agency needs for mobile high speed data services.*

The Cingular wireless network offers a suite of subscriber benefits unmatched by other networks, including comprehensive service coverage, fast data speeds, and the availability of advanced services.

1.7.1.1.b Benefits to Technical Approach

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

AT&T's Networx services support the Government's vision of transformation through the use of the Federal Enterprise Architecture (FEA) as a facilitating mechanism for technologies that contribute to mission performance. In describing services in relation to FEA, AT&T either summarizes their contribution or provides an example of how each service facilitates FEA implementation (**Table 1.7.2.1-2**). AT&T aligns its componentized products and services so they

are easily integrated, commonly manageable, and usable across Government functions, horizontally and vertically, as well as between levels of Government. Services, such as CPCS, are within the technical reference model and support the security management component of the FEA.

APPROACH	BENEFITS	FEA COMPLIANCE
Spectrum acquisition	Agencies may migrate to new 3G architectures as needed, rather than on a carrier's schedule	• Longer equipment life cycles • FEA Link: TRM/ Component Framework//Service Platform and Infrastructure/Wireless-Mobile-Voice
Service coverage	Coverage and international roaming in over 160 Countries provides Government personnel voice and data services while on the move – locally, regionally and internationally	• Increases geographic range in which Government Information Technology (IT) assets can be accessed and used • Increased productivity and reduced downtime of Agency personnel while traveling • FEA Link: TRM/Service Platform and Infrastructure/Hardware & Infrastructure/Wide Area Network (WAN)
Standards-based network	Cingular's network uses GSM, the world's most popular wireless networking standard • Worldwide market for innovative network infrastructure and inexpensive subscriber equipment • Roaming and compatibility with other networks worldwide • Accepted roadmap to advanced services such as UMTS/HSDPA that enable network convergence and service enhancements	• Results in longer product/service lifecycles, inexpensive mobile equipment, and low-risk network migration paths • FEA Link: TRM/ Component Framework/Service Presentation-Interface/Support Platforms/Wireless-Mobile
Multilayer security	Data is encrypted with strong algorithms in multiple layers of the network – over the air, in signaling systems, within the core wired infrastructure, and optionally as part of user applications Additional fraud protection is offered with PINs, logins, passwords, where applicable	• Agencies' data will remain secure as it traverses both the airwaves as well as the wired network infrastructure. • FEA Link: TRM/Component Framework/Security/Digital Signatures
Quality and performance measurements	Agencies have access to statistics that illustrate the performance of the network	• Agencies are assured of high quality wireless services • FEA Link: TRM/ Component Framework/Service Presentation-Interface/Support Platforms/Wireless-Mobile
Advanced data services	Agencies personnel may take high bandwidth data applications into mobile environments	• Subscribers stay connected to familiar applications while traveling • FEA Link: TRM/Service Platform and Infrastructure/hardware & infrastructure/Wide Area Network (WAN)

Table 1.7.1.1-2: Technical Approach. *Cingular's approach to providing subscribers with quality mobile communications is multifaceted and helps Agencies accomplish missions while complying with FEA guidelines.*

From an FEA perspective, AT&T brings a market-based discipline and wireless services that support multiple lines of business (LoB) and subfunctions, as defined by the business reference model (BRM). AT&T

regards wireless services as a horizontal and vertical capability of the service component reference model (SRM) that provides a component of security to the underlying communication infrastructure for individuals who need support or services from the Government. This component consists of telephony or other voice communication infrastructure services that entail the transmission of voice, data, and messages in multiple formats and protocols.

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

- Technical Reference Model capabilities are fully met and linked to the Service Component Reference Model (SRM) and Data Reference Model (DRM).
- These links are structured to support Business Reference Model (BRM) functions and provide line-of-sight linkage to mission performance and ultimate accomplishment per the Performance Reference Model (PRM)
- AT&T operates as an innovative partner through Networx to help achieve the vision of the FEA to enhance mission performance.

In addition to the benefits and FEA facilitations cited earlier, AT&T will assist specific departments and Agencies to meet mission and business objectives through a comprehensive CPCS offering.

1.7.1.1.c Major Issues 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, issues may 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. The AT&T Team's experience

has enabled us to develop proven methods, processes, and procedures applicable the simplest to the most complex projects.

Table 1.7.1.1-3 lists the top service delivery risks for CPCS and our mitigation strategies. As with all large projects, we enter each of these risks and others (after identification and characterization) into our risk-tracking database, and immediately take steps to mitigate them before they become issues. 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. Agencies will receive a CPCS engineered to high standards that address the common pitfalls of wireless networking.

RISKS	DESCRIPTION	MITIGATION
Inadequate service coverage	Services not offered in locations Agency personnel frequent	[redacted]
Requirements changes	Requirements changes (before and after service delivery) contribute to budget overruns, schedule slips, and missed expectations.	• Obtain pre-project understanding of requirements through detailed analysis • Establish strong change management processes • Conduct continuous communications with GSA and Agencies.
Security of subscriber data	User data or information is at risk through loss of wireless terminal or interception of wireless data transmission	Cingular has implemented proactive security procedures to protect subscriber data: [redacted]
Network congestion (voice)	Unanticipated growth leads to call blockage during high traffic demand	Cingular's network engineers follow a formal process to minimize network congestion: • Continuously analyze and trend subscribers' use of the network • Forecast anticipated network demand [redacted]
Network Congestion (data)	Inadequate bandwidth causes slow or unavailable data connections	Cingular's data applications are designed with an end-to-end perspective, taking into account traffic from a variety of perspectives. Cingular continuously monitors: [redacted]

RISKS	DESCRIPTION	MITIGATION
Subscriber equipment issues	Subscriber equipment malfunctions or is non-conformant with Federal standards or internal network requirements, which can cause interference with other subscribers that result in dropped calls or other network problems	• Cingular only allows FCC-approved devices on the network – devices are tested for RF compliance to Federal standards [redacted]
Schedule delays	The delivery of the service suffers from delays stemming from lack of equipment inventories, or other network implementation hurdles	[redacted] • AT&T assigns an experienced Project Manager to oversee the processes necessary to meet agreed schedules [redacted]

Table 1.7.1.1-3: CPCS Risks. *The CPCS service is designed and maintained to avoid common problems encountered in the operation of wireless systems*.

Government users will receive coverage where it is needed, secure connections that protect sensitive data, and reliable wireless connectivity that is available when and where its needed.

1.7.1.1.d Wireless Network Architecture

(d) Describe the overall wireless network architecture and explain the benefits of the network architecture design.

Cingular's network is built upon the world's most popular wireless network platform – GSM, which supports over 1.4 billion wireless subscribers - approximately 79% of all cellular subscriptions. GSM network architecture layers multiple services on a common radio access subsystem that is controlled by Cingular, and elegantly connects subscribers to public networks, as shown in **Figure 1.7.1.1-6**. The functions of security, operations, and management flow throughout the architecture, [redacted]

GSM's architecture is designed in a forum-based environment where many diverse organizations contribute to the design and no single entity controls the technology, as may be the case with other technologies.

Figure 1.7.1.1-6: Overall Network Architecture. [redacted]

Because GSM is accepted as a worldwide standard and follow a common architecture across operators, Agencies gain benefits (**Table 1.7.1.1-4**) that other networks cannot provide, including:

GSM CHARACTERISTIC	UNIQUE BENEFIT TO USERS
Subscriber Identity Modules, or SIM chips	Instant identity portability between approved GSM devices - the user's phone number and preferences stay with the SIM card, not the device
Compatible systems throughout the world	Simplified roaming and associated billing in over [redacted] countries – automatic device registration with Cingular's roaming partners
World's largest marketplace for wireless technology	Subscribers may choose from the widest range of subscriber equipment at prices that reflect worldwide market competition.
Multiband phones widely available	Multiband phones are available from manufacturers that enable subscribers to use their normal and familiar phone while roaming internationally, even if local GSM networks operate on different frequencies than Cingular's.

Table 1.7.1.1-4: GSM Technology Benefits. *Illustrations of the direct user benefits garnered from using GSM as the network platform.*

Cingular's GSM cellular network also serves as the basis for advanced wireless data services (GPRS/EDGE), and is described in **Table 1.7.1.1-5**. EDGE

services have been deployed in all Cingular's served markets and are rapidly being deployed in foreign GSM carriers' networks – many of which can be roamed in by Cingular subscribers on an ad hoc basis.

GPRS/EDGE BENEFIT	DETAILED DISCUSSION
Unprecedented mobile data speeds	EDGE offers average data speeds between 90 to 135 Kbps - typical upload speeds are 50-80 Kbps – a significant improvement over legacy Circuit Switched Data (9.6 kbps) or CDPD (19.2 kbps) systems
Immediacy, convenience, and resiliency of data services	EDGE facilitates instant, always-on connections, so information may be sent or received immediately as the need arises – auto-reconnect features may be enabled to provide continuity of service previously unavailable
Spectral efficiency	GPRS/EDGE radio resources are used only when users are actually sending or receiving data, making more virtual connections and capacity available than circuit switched systems
Internet and/or enterprise aware	EDGE fully enables mobile Internet functionality by allowing interworking between the existing Internet TCP/IP and the GPRS network. Terminals can have IP address and be addressable as such

Table 1.7.1.1-5: EDGE Data Service Highlights. *Mobile data applications have been significantly accelerated and improved by Cingular's network-wide implementation of GPRS/EDGE.*

Offering increased capabilities to users' mobile data applications, GSM's new wireless data standard, UMTS, is a true third generation service (3G). UMTS, together with its upgrade, HSDPA offer data speeds between 400-700 Kbps, and peak data speeds bursts of up to 2 Mbps on capable devices. In July 2004, Cingular began upgrading its mobile data system based on the UMTS standard, and currently offers the service in 20 major metropolitan markets, with most US markets expected to be implemented by the end of 2006. The UMTS/HSDPA service will provide Agency personnel broadband-like performance in mobile applications and enhanced services while on the move, including but not limited to:

- High-speed access to the Internet and Virtual Private Networks (VPNs) with virtual desktop performance
- Wireles-enabled productivity tools capable of accessing home office databases
- Media streaming, high-resolution image captures and transmission
- Simultaneous high-quality voice and data sessions

With the EDGE architecture deployed and the acquisition of radio frequency spectrum, the Cingular network is prepared for the migration to UMTS/HSDPA. In addition, the modular architecture of the Cingular network allows for the migration to an MPLS infrastructure from a SONET/ATM transport network. With these components in place, the Cingular network is prepared for eventual migration to Internet Protocol Multimedia System (IMS).

1.7.1.1.e Security and Reliability of the Wireless Network Architecture

(e) Describe how the wireless network architecture supports and ensures wireless security and reliability, technological evolution, convergence, and interoperability with present and future commercial networks.

As shown in Section 1.7.1.1.d, the network architecture is deployed in a set of specific layers (e.g. air interface, radio control, switching and service, data and transport). Each of these layers contains differing security, reliability, interoperability, and convergence capabilities as defined by the function of the layer (**Table 1.7.1.1-6**).

LAYER	SECURITY	RELIABILITY	EVOLUTION
Air interface and subscriber equipment			
Base station control			
Switching and Service			
Transport			

LAYER	SECURITY	RELIABILITY	EVOLUTION
[redacted]	[redacted]	[redacted]	[redacted]

Table 1.7.1.1-6: [redacted] Highlights. [redacted]

1.7.1.1.e.1 Wireless Authentication (Air Interface and Radio Layers)

In the wireless network, users are protected by network-to-user device stream encryption. [redacted]

Once a terminal has been authenticated, the next step is to produce an encryption key. [redacted]

GSM security algorithms provide both user authentication and RF link encryption, offering security and privacy for Agencies' voice and data transmissions. As part of Cingular's adherence to GSM standards, the network uses a 64-bit encryption scheme on over the air transmissions. [redacted]

Some operators do not implement GSM's encryption capabilities to their fullest extent, but Cingular requires full implementation of GSM's security features in all North American markets served. [redacted]

1.7.1.1.e.2 Wireless Data Device Controls

Wireless data sessions can be further protected with [redacted]

Table 1.7.1.1-7 [redacted]

APN	IP ADDRESS OPTIONS	COMMENTS
General purpose: proxy	[redacted]	[redacted]
General purpose: public	[redacted]	[redacted]
General purpose: internet (mobile terminating data service)	[redacted]	[redacted]
General purpose: blackberry.net	[redacted]	[redacted]
Custom	[redacted]	[redacted]

Table 1.7.1.1-7: APN Types. *Mobile data applications utilize Access Point Names to enable different services types.*

One additional level of authentication that can optionally be invoked between the mobile unit and the GPRS network is [redacted]

1.7.1.1.e.3 Resiliency

Cingular's network is built without single points of failure in order to provide reliability at all of its network layers. The radio network and subscriber equipment work together to form resilient connections through conservative RF planning that takes advantage of abundant bandwidth at multiple

frequencies as well as through dense cell coverage. Important network elements in the radio control, switching, and transport layers are protected against failure through redundant power systems, N:1 sparing on critical modules, diversity of external connections – all provided with robust environmental control systems.

1.7.1.1.e.4 Evolution

[redacted]

Figure 1.7.1.1-7. [redacted]

[redacted]

Figure 1.7.1.1-7: Cell Network [redacted]

1.7.1.2 Satisfaction of Wireless Performance Requirements [L.34.1.7.2]

1.7.1.2.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.

The Cingular network provides cellular services at the thresholds required by Agencies. The Networx RFP outlines the required Availability and Time-To-Restore (TTR) performance levels for CPCS (**Table 1.7.1.2-1**).

KEY PERFORMANCE INDICATOR	SERVICE LEVEL	PERFORMANCE STANDARD (THRESHOLD)	PROPOSED SERVICE QUALITY LEVEL
Availability (Voice Services)	Routine	99.5%	[redacted]
Time to Restore (TTR)	With Dispatch	8 hours	[redacted]
	Without Dispatch	4 hours	[redacted]

Table 1.7.1.2-1: Compliance with Agencies' Key Performance Indicators. [redacted]

Cingular has undertaken precautions that assure network quality and meet the Agency KPIs as well as exceed them. No single point of failure is allowed in the network design. The high availability of cellular service at rates meeting 99.5% is delivered by a network design that acknowledges the performance parameters of all critical network elements, analyzes the impact each has on service delivery, and builds in redundant subsystems with appropriate failover procedures where required. [redacted]

1.7.1.2.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.

Cingular captures a variety of key performance statistics on its critical network elements with [redacted] nodes to provide a comprehensive picture of the network's health [redacted] (**Figure 1.7.1.2-1**).

Figure 1.7.1.2-1: [redacted]

Quality management tools probe the network at strategically important points for resource availability, packet loss rates, and latency statistics. The tools aggregate these indicators into a service quality report that is used for improving the network and responding issues.

AT&T measures the required Time to Restore KPI and Acceptable Quality Level (AQL) for CPCS by [redacted] (**Table 1.7.1.2-2**). [redacted] (**Figure 1.7.1.2-2**) [redacted]

KEY PERFORMANCE INDICATOR	APPROACH TO MONITORING AND MEASURING
Availability	SQM tools by Vallent - server connects to critical network elements and monitors performance: • BSCs (voice call resource availability statistics and retainability rates) • SGSNs (success rates and retainability) • HLR to Switch connections • Switch to Switch connections
Time to Restore (TTR)	AT&T, together with Cingular will perform following functions: • Capture Trouble Ticket data for CPCS services at Customer Service Center • Calculate time Trouble Ticket is open • Provide TTR for each reported event, as applicable, to Government through reports

Table 1.7.1.2-2: Metrics Measurement Approach. *The proposed CPCS solution is measured in accordance with the methods above for compliance with the stated quality metrics.*

Figure 1.7.1.2-2: [redacted] for [redacted]

1.7.1.2.c Approach to Perform Service Delivery Verification

(c) Describe the offeror's approach to perform verification of individual services delivered under the contract, in particular the testing procedures to verify acceptable performance and Key Performance Indicator (KPI)/Acceptable Quality Level (AQL) compliance.

The first time the service is provided through the Networx contract, the service performance must be verified; KPIs will be monitored to certify that the service performance complies with the AQL (**Table 1.7.1.2-3**).

KEY PERFORMANCE INDICATOR	VERIFICATION APPROACH	[redacted]
Availability	[redacted]	[redacted]
Time to Restore (TTR)	[redacted]	

Table 1.7.1.2-3: Service Delivery Verification. *The Key Performance Indicators are closely monitored through a comprehensive verification approach and testing procedure that certifies the service performance achieves or exceeds the Acceptable Quality Levels.*

Cingular uses real-time monitoring and measurement tools to verify the CPCS is delivered per Agency metrics. [redacted]

[redacted] (**Figure 1.7.1.2-3**).

Figure 1.7.1.2-3: Wireless Network Status Report. [redacted]

The real-time monitoring system allows quality statistics to be collected on an Agency-by-Agency basis and aggregated into a report that allows delivered service performance to be compared to service commitments.

1.7.1.2.d Performance Level Improvements

(d) If the offeror proposes to exceed the Acceptable Quality Levels (AQLs) in the Key Performance Indicators (KPIs) required by the RFP, describe the performance improvements.

Agencies will benefit from enhanced service performance when the KPI performance thresholds are exceeded. **Table 1.7.1.2-4** summarizes the proposed improvement to the KPI performance thresholds, and the benefit

that Agencies will experience through the higher service performance. [redacted]

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

Table 1.7.1.2-4: Performance Level Improvements. *Agencies will experience substantial performance and quality improvements with the proposed Acceptable Quality Levels.*

[redacted]

1.7.1.2.e Approach and Benefits for Additional Performance Metrics

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

The proposed CPCS (**Table 1.7.1.2-5**) is capable of exceeding the Agency's requirement through the addition of performance metrics. [redacted]

NEW PROPOSED KPI	NEW PROPOSED THRESHOLD	AGENCY BENEFIT
[redacted]	[redacted]	[redacted]

Table 1.7.1.2-5: [redacted] Level [redacted]

[redacted]

[redacted]

1.7.1.3 Satisfaction of Wireless Specifications [L.34.1.7.3]

1.7.1.3.a Service Requirements Description

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

Agencies' requirements for voice, data, and messaging services are fulfilled by Cingular's wireless network. To do so, the network has evolved with dual cores (**Figure 1.7.1.3-1**) – one core delivering primarily voice services via the PSTN and other dialable destinations, and the other offering access to public and private data networks.

Agencies' requirements for wireless communications are fully satisfied by the Cingular network's advanced capabilities, providing immediate and measurable benefits to Government personnel (**Table 1.7.1.3-1**).

Figure 1.7.1.3-1: Dual Core Network. [redacted]

SERVICE REQUIREMENT	DESCRIPTION	BENEFIT TO AGENCIES
GSM 2.5G/3G Network	GSM-compliant mobile services provided by North America's largest and fastest wireless network	Fulfills Agencies' needs for mobile connectivity and advanced services with systems that comply with truly global standards that keep
Connectivity to other networks	• Dialing to any PSTN destination via E.164 (World Dialing Plan) • Connectivity to Mobile Satellite Services (MSS) • Connectivity to Fixed Satellite Services (FSS), as applicable • Connectivity to the Internet via EDGE/UMTS/HSDPA at a variety of data speeds • Connectivity to premise-based and network-based VPNs	Agencies may access public or private networks through accepted and familiar connection schema
Roaming	• Largest roaming service area in the world • Roaming relationships in over [redacted] countries • Many roaming partners support advanced services (see appendix)	Agency employees can travel throughout the world and remain in touch, regardless of whether they are registered on Cingular's domestic network
Packet Data	• EDGE provides links up to 130Kbps and is fully deployed throughout Cingular's system • Systems support full mobility including links while traveling up to 65MPH • UMTS/HSDPA offers up to 700Kbps - 3G deployments are now beginning implementation in large markets	Agency personnel can access their normal applications at data rates that allow enhanced productivity while on the move
SMS	• Store and forward delivery of 179 character messages • Delivery with Priorities, Confirmations, Escalations and Expirations • Supports messages originated from: • Other mobile terminals • SMTP • Paging services • Off-net cellular systems (e.g. CDMA cellular networks) • Instant Messaging (IM) systems	Provides subscribers with notifications and brief notes from a variety of on-net and off-net origination points
MMS	• Store and forward delivery of large files in a variety of formats • Supports text, audio, images and video	Agency personnel can receive files too large for SMS directly on their mobile phones, without the need for data equipment
E911	Compliance with Enhanced 911 services specified by the FCC, Phase I and Phase II	Agency subscribers can be accurately located in an emergency
WPS	Provides the requesting authorized subscriber with the next available radio channel when invoked	Offers essential Agency personnel the capability to bypass network congestion in emergencies
Provided GSM Wireless Equipment	79% of the world's mobile phones run on GSM networks, serving a billion customers in over 200 countries and creating one of the world's largest consumer electronics marketplaces	Agencies may choose from a variety of manufacturers, models, capabilities, and price points for their subscriber equipment

Table 1.7.1.3-1: Service Delivery Approach. *Cingular's CPCS provides subscribers with a variety of advanced services that deliver Agency personnel many benefits.*

Agencies are provided CPCS over a network with unique and advanced features. For example, data services provided by the Cingular network are based on GSM's GPRS/EDGE technology – providing network-wide data

rates of 130kbps. [redacted]

[redacted]The Cingular network is based on GSM standards, providing subscribers the capability to roam onto compatible GSM networks in over 160 countries. In emergencies, subscribers can utilize E911 (full phase II implementation complete) to be located with excellent geographical precision. [redacted]

1.7.1.3.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 CPCS with additional features and capabilities for an additional fee. **Table 1.7.1.3-2** highlights additional service features and capabilities available with CPCS. AT&T proposes the attributes in **Table 1.7.1.3-2** as service enhancements.

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

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

Table 1.7.1.3-2: Service Enhancements. [redacted]

1.7.1.3.b.1 Push-to-Talk

[redacted]

Figure 1.7.1.3-2: Push-to-Talk Group [redacted]

[redacted] Figure 1.7.1.3-2. [redacted]

[redacted] **Figure 1.7.1.3-3**

[redacted]

Figure 1.7.1.3-3: Push-to-Talk [redacted]

[redacted] (see **Table 1.7.1.3-3**).

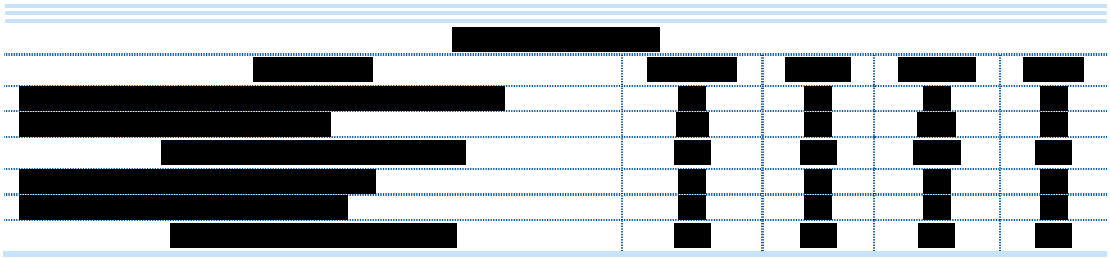


Table 1.7.1.3-3: Push to Talk [redacted]

The Push-to-Talk service is available throughout all of Cingular's domestic network beginning in the fourth quarter of 2005, and will be available in select international locations in the first quarter of 2006.

1.7.1.3.b.2 Enterprise Paging

[redacted]

[redacted]

(**Figure 1.7.1.3-4**). [redacted]

Figure 1.7.1.3-4: Enterprise Paging. [redacted]

1.7.1.3.b.3 BlackBerry Enterprise Service

AT&T proposes Blackberry Enterprise Service as an option to its Networx Cellular/Personal Communications Service (CPCS), offering Agency personnel the capability to synch their mobile devices automatically to the home network for improved productivity when on the move. BlackBerry Enterprise Service was introduced in 1999 by Research in Motion (RIM) to bring users a mobile computing experience that simulates and integrates with their desktops, with capabilities that include push email, remote file/folder management, calendar/appointment updates, advanced mobile data,

encryption and security functionalities. As of late 2007, AT&T provides service to more BlackBerry subscribers than any other wireless carrier.

The BlackBerry Enterprise Service is based on an Agency-managed server deployment with mobile networking support from AT&T and RIM. Subscribing Agencies collocate a BlackBerry Enterprise Server with the appropriate number of user licenses together with their productivity platform's enterprise server which then exchange user traffic for delivery to mobile devices. User data is forwarded to the RIM Network Operations Center (NOC) via the Internet, and ultimately to AT&T's mobile data system for delivery to the appropriate user client device. This architecture also works in reverse, offering subscribers access to their enterprise platform's desktop applications.

Figure 1.7.1.3-5: Blackberry Enterprise Service Architecture. [redacted]

The AT&T's Wireless Network, the RIM NOC, and the BlackBerry Enterprise Server work together to provide true mobile-to-network synchronization, meaning the system actively monitors the availability of the mobile client device and initiates the exchange of data whenever the client is in range of

AT&T's data services. The BlackBerry service is tightly integrated with Microsoft Exchange Server™ and Lotus Domino™, (other platform support is optional) and Agencies may dynamically define what services and rights within their platforms' applications are available to any individual user. Further, Agencies may allow users to poll non-enterprise email accounts outside of the BlackBerry system, including email systems based on POP, IMAP, and web-based accounts, if desired. BlackBerry Enterprise Service is inherently secure, being FIPS-140 compliant, but also includes advanced encryption options for critical applications. Should a mobile BlackBerry device containing sensitive data be lost or stolen, Agencies have the capability to remotely erase and disable that device at no additional cost.

BlackBerry-compatible devices utilize AT&T's GPRS/EDGE network to provide high speed mobile data connectivity, while offering the largest available domestic service coverage to mobile users. BlackBerry Enterprise Service includes unlimited access to AT&T's GPRS/EDGE data on this system, eliminating the need to purchase a separate data plan for wireless data (except the BlackBerry Enterprise 4MB plan, which includes 4 megabytes of data monthly and is metered thereafter). As an option to BlackBerry Enterprise Service, Agencies may opt for international service coverage, available in far more locations than any other comparable service. A further option, "Tethering", allows Agency personnel to utilize an appropriately equipped BlackBerry device as a wireless modem for PCs and laptops.

Figure 1.7.1.3-6: AT&T's GPRS Service Area. *BlackBerry Enterprise Service uses the AT&T's Wireless Network's GPRS system to provide connectivity in the largest available service area.*

AT&T's Networx Blackberry Enterprise Service is an effective means to maximize productivity in Agencies with mobile personnel. The service offers Agencies superior control and flexibility when managing mobile workforces in one cost-effective bundle.

A BlackBerry® Networx solution is comprised of the following components:

(A) **BlackBerry handset/PDA device (as listed in Technical section 1.8).**

(B) **BlackBerry Enterprise Server (BES)** – BlackBerry Enterprise Server is robust software that acts as the centralized link between wireless devices, enterprise applications and wireless networks. Designed to meet the needs of enterprise and government organizations, it provides a proven, secure, open architecture for globally extending wireless communications and corporate data to mobile users. BES is required for BlackBerry service to function under the Networx contract. However, it may not be necessary to order if the Agency already has BES software through another or pre-existing arrangement.

(C) **BlackBerry Client Access License (CAL) or BlackBerry S/MIME CAL** – Each BlackBerry user under the Networx contract will require a CAL or a Secure Multi-Purpose Internet Mail Extension (S/MIME) CAL. Non-S/MIME CALs are provided in the following user increments (1, 5, 10, 50, 100, 500, and 1,000). BlackBerry S/MIME CALs provide the same function as their non-S/MIME counterparts with the exception that they provide an additional layer of security by encrypting the email. S/MIME CALs are provided in the following user increments (1, 5, 10, 50, 100, and 200). While CALs or S/MIME CALs are required for BlackBerry service to operate under the Networx contract, they may not need to be ordered if the Agency already has acquired them through another or pre-existing arrangement.

(D) **BlackBerry Service Rate Plans** – The final component required for BlackBerry service under Networx is the appropriate rate plan to cover the actual use of the BlackBerry device/PDA.

1.7.1.3.b.4 iPhone Visual Voicemail

The iPhone service plans include Visual Voicemail, which allows users to access their incoming voicemails with greater flexibility than standard “dial-in” architectures. Visual Voicemail utilizes data channels (GPRS/EDGE, UMTS/HSDPA) to retrieve incoming voice messages for local storage in the iPhone’s memory. This local storage architecture allows users to choose the order in which they listen to voicemails, as well as allowing message playback at any time after retrieval, regardless of the current connection status. Visual Voicemail is not available in all areas (e.g. areas where data is not supported), however, conventional dial-in voicemail is accessible via normal procedure when Visual Voicemail is not supported.

Visual Voicemail requires Users to establish a new voice mail box. When transitioning existing service to the iPhone solution, all current voice mail messages are erased. For this reason, users are advised to listen to existing voicemails before completing the activation process.

Receipt of Visual Voicemail messages when roaming internationally are charged as indicated in Networx table B.2.14.1.2-5 CPCS Feature Prices (Data-Roaming). If the Data roaming toggle on the iPhone is set to OFF, data roaming will be blocked as well as the receipt of Visual Voicemail messages outside AT&T’s Home service area as defined in Table B.2.14.1.1-4. An iPhone user can optionally password protect the Visual Voicemail to secure his/her voicemail messages, contacts and related content.

1.7.1.3.c Wireless Services Experience

(c) Describe the offeror's experience with delivering the mandatory Wireless Services described in Section C.2 Technical Requirements.

The 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 services. Examples of the AT&T Team's ability to deliver managed services are listed in **Table 1.7.1.3-4**.

Table 1.7.1.3-4: Experience Delivering Wireless Services. *Cingular has successfully provided mobile voice and data solutions to Government Agencies as well as large commercial organizations.*

Agencies will work with an experienced wireless service provider that operates the largest cellular operator in North America with the following coverage: [redacted] Government organizations at the Federal, state, and local levels are served by Cingular.

Agencies will have access to service in more locations through enhanced coverage inside Federal buildings including: the U.S. Capitol, offices of the Environmental Protection Agency and the Federal Communications Commission as well as others in the Ronald Reagan Building – [redacted] Fortune® 100 companies, [redacted] of the Fortune® 500 companies rely on Cingular to provide wireless voice and data solutions.

[redacted] subscribers obtain wireless service from Cingular. [redacted]

[redacted]

[redacted]

1.7.1.4 Robust Delivery of Wireless Services [L.34.1.7.4]

1.7.1.4.a Wireless Design Measures and Engineering Practices

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

In order to keep the wireless network operating at high availability for both voice and data services, Cingular's engineers employ strict design methodologies when making additions or enhancements to the wireless network (**Table 1.7.1.4-1**).

TECHNIQUE	DISCUSSION	BENEFIT
Voice channel forecast (vcf)	Voice Channel Forecast (VCF) was developed by Cingular to assist network engineers in determining how and when new RF channels and other resources are needed to achieve the required level of service and provides input into: • RF channel growth planning • Cell infrastructure planning (power, backhaul, etc.) • Cabinet and frame planning • Spectrum management.	Modifications and enhancements to the wireless network are implemented smoothly and in a timely manner .
Cell splitting (frequency reuse)	Cingular's criteria to implement a cell split or to sectorize an omnidirectional site in a GSM dual band system is as follows: • GSM markets have a 12 Broadcast Control Channel plan with 1/1 hopping • Minimum of 3 radios per sector for GSM 1900 • Utilize 1900MHz only after 850MHz spectrum is exhausted.	Cingular has predefined conditions under which additional capacity will be added through frequency reuse, providing a more robust service.
Propagation prediction tools	Cingular uses RF prediction tools to design the network the following thresholds: • Urban design for 1900MHz footprint: -74dBm • Suburban design for 1900MHz footprint: -82dBm • Rural design for 850MHz footprint: -92dBm.	Cingular utilizes design techniques and frequencies tailored to the RF environment where service is to be provided, contributing to enhanced coverage.

TECHNIQUE	DISCUSSION	BENEFIT
Management of time slots	The GPRS/EDGE network is designed with two time slots dedicated to data and another five time slots that are voice preferred.	The wireless network will keep resources available for both voice and data services and will not preempt data calls in preference to voice calls, keeping network availability high.
Cell overlap	Cells frequently offer overlapping coverage especially in urban areas, and the loss of a single sector or even the entire cell site will not ordinarily interrupt transmissions.	If a cell site becomes unavailable a neighboring site will often pick up the traffic, resulting in a more robust service.
Redundant power at network sites	To protect against power failure, Cingular has Uninterruptible Power Supplies (UPS) with backup batteries located at MSCs, Data Centers, and cell sites that are capable of providing at least six hours of service at peak operation. Back-up generators are also located at all data centers, MSCs, and critical cell sites, to provide back-up power and/or recharge existing batteries. A mobile fleet of more than 600 trailer-mounted generators are deployed as needed. All data centers, MSCs, and cell sites are alarmed with power-fail alarms and are monitored 24 hours per day by our Data Center Operations group and Wireless Network Control Center (WNCC).	Cellular services remain available during power outages
Redundant backhaul and inter-element links	Transport network based on ATM and redundant dual-ring SONET configurations with full alarm capability and sub-50ms detect and failover capability.	Should a critical link between network elements become unavailable, there is an alternate path for maintaining connectivity.

Table 1.7.1.4-1: Design Practices. *Cingular engineers the wireless network using industry-leading practices developed to keep the network performing at optimal levels.*

Adherence to formalized engineering practices when growing or altering the network allows Cingular's to offer high quality and uniform service across vast regions.

1.7.1.4.b Radio Frequency Network Optimization

(b) Describe the methodologies employed for continuous Radio Frequency (RF) Network Optimization including drive tests and network audits to ensure cell site performance meets design criteria.

To optimize the network, Cingular monitors and audits its RF facilities for capacity and performance. RF reconfiguration projects and cell adjustments are triggered based on a set of predefined rules or methodologies as described in **Table 1.7.1.4-2**.

METHODOLOGY	MEASUREMENT OR CRITERIA
[redacted]	[redacted]
[redacted]	[redacted]

METHODOLOGY	MEASUREMENT OR CRITERIA
[redacted]	[redacted]

Table 1.7.1.4-2: RF Optimization. [redacted]

[redacted] **Figure 1.7.1.4-1**.

Figure 1.7.1.4-1 RF: Optimization Process. [redacted]

[redacted] **Figure 1.7.1.4-2**.

Proactive measurements are undertaken by regional authorities within Cingular and are scheduled at intervals appropriate to the local network design. Examples include regular network audits and scheduled maintenance that measure the network's RF performance in the field. Examples of reactive responses to network deficiencies include responding to the extensive alarm and management systems that most frequently notify Cingular operations personnel of radio-related issues before subscribers are adversely affected.

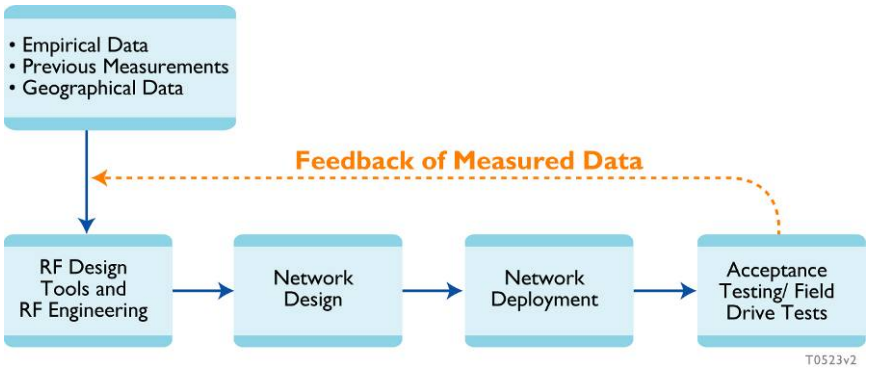


Figure 1.7.1.4-2 RF: Optimization Process. *Continued maintenance of the RF portion of the network is managed on a proactive, as well as reactive, schema.*

1.7.1.4.c Approach to Disaster Recovery

(c) Describe the approach for disaster recovery from occurrences such as commercial power grid failures and natural disasters.

Cingular has taken a number of steps that verify the reliability of its critical processes and supporting infrastructure in order to provide high-quality services to customers under adverse conditions. This planning includes up-front prevention and mitigation efforts, as well as comprehensive emergency response and recovery plans in the event of a disaster/crisis (**Table 1.7.1.4-3**).

APPROACH	DESCRIPTION	PROCEDURES
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 1.7.1.4-3: Disaster Recovery Planning. *Cingular includes disaster planning as part of their ongoing operational plan.*

In the event of a disaster, Cingular Wireless has developed Disaster Response and Recovery Plans to avert failures and recover operations of critical components in the network (**Table 1.7.1.4-4**).

METHOD	PREVENTION UNDERTAKEN	BENEFIT
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

METHOD	PREVENTION UNDERTAKEN	BENEFIT
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]
[redacted]	[redacted]	[redacted]

Table 1.7.1.4-4: Disaster Recovery Techniques. *The proposed CPCS solution guards against service interruptions due to power outages and natural disasters in a variety of ways.*

Each Disaster Recovery Plan is formulated regionally and contains key information specific to the recovery within a market area. Local disaster recovery assets, such as COWs (**Figure 1.7.1.4-3**), are deployed locally in each region, but are also available to other regions when events call for a larger response.

Figure 1.7.1.4-3: Cell-on-Wheels. *Cingular operates many Cell-on-Wheels that are capable of quickly restoring communications to an area stricken by disaster.*

Cingular has established Disaster Field Offices (DFOs) in major locations that serve as focal points for front-line restoration activities in a particular area.

Further, Emergency Operations Centers (EOCs) support the DFOs from regional locations throughout the country. Cingular's National Operations Center coordinates response and recovery efforts for EOCs. All of these organizations participate in regular business resumption training, which is practiced and drilled frequently in order that critical employees work effectively during a crisis.

1.7.1.4.d Wireless Fraud Prevention

(d) Describe the mechanisms to detect and prevent wireless fraud, and protect end-user privacy for voice communication and data transfer.

Cingular Wireless has launched an aggressive and multi-faceted campaign to combat wireless fraud, which is summarized in **Table 1.7.1.4-5**.

FRAUD PREVENTION MEASURE	DISCUSSION/BENEFIT
GSM authentication	[redacted]
Fraud Management System (mobile terminal)	[redacted]
SIM Card Personal ID Number (PIN)	[redacted]
Roaming authorization per mobile MSC (RAM)	[redacted]
Cingular wireless employee training	[redacted]

Table 1.7.1.4-5: Fraud Prevention for Voice Services. *The proposed CPCS solution combats wireless fraud with a variety of tools and techniques.*

To gain access to the GSM/GPRS network the subscriber must have a SIM Card for the mobile device. Cingular supplies SIM cards for each user device that it provides, which contains user identity information. SIM cards implement the GSM authentication algorithm (described in Section 1.7.1.1.e) which is based on challenge/response mechanisms. For voice services, the Mobile Switching Center handles the challenge/response activity while the Serving GPRS Support Node (SGSN) for GPRS data services handles it for

data service. **Table 1.7.1.4-6** summarizes the GSM/GPRS authentication process. At no point during the authentication process is the subscriber authentication key transmitted over any portion of the network.

AUTHENTICATION STEP	DISCUSSION
Mobile request	
IMSI verification	
Challenge/response derivation and forwarding	
Response generation and forwarding	
Comparison and authentication	

Table 1.7.1.4-6: GSM/GPRS Authentication Process. *GSM networks provide a built in layer of mobile terminal validation upon each registration.*

SIM cards can be further protected by requiring the user to enter a personal identification number (PIN) to use the wireless device. If the user enters an incorrect PIN more than three times, further attempts are blocked until the user enters an administrative code that can only be obtained from Cingular Customer Care.

Cingular actively monitors its network for fraudulent activity with advanced detection tools such as Minotaur™. These tools apply extensive data mining and statistical analysis to identify potentially fraudulent use of the network. **Table 1.7.1.4-7**, describes the mechanisms that detect and prevent fraud.

FRAUD DETECTION TECHNIQUE	BENEFIT
Rules-based indicators	
Behavioural models	
Scorecards	
High usage detector	
Data proximity detector	

Table 1.7.1.4-7: GSM/GPRS Authentication Process. *GSM networks provide a built in layer of mobile terminal validation upon each registration.*

[redacted] **Figure 1.7.1.4-4**.

Beyond these measures, customers can further protect against misuse of lost or stolen mobile equipment by implementing application passwords, hardware tokens, or biometric systems. Cingular provides a number of wireless solutions which include remote device wipe and remote kill. In addition Cingular is in the process of developing a general purpose hosted device management solution with a range of administrative, diagnostic, and security features, including remote device wipe and kill.

Figure 1.7.1.4-4: Fraud Detection Report. [redacted]

1.7.1.4.e Approach to Multicasting Commercial Advertising (Spam)

(e) Describe the approach on multicasting of commercial advertising (i.e., spam). Discuss the policy and user options supported (e.g., opt-in, opt-out, filtering).

Spam is most typically delivered to users via email services for services that stop SMTP-based spam *(see* Section 1.6.8*,* Secure Managed Email Service*)*. As it relates to the CPCS service, it is possible to receive spam via messaging services such as SMS or MMS. Cingular takes steps to prevent forwarding illicit messages to subscribers. The CPCS system provides two filter levels, network and subscriber, as summarized in **Table 1.7.1.4-8**.

SPAM BLOCKING KEY	BENEFITS
Network Filter Rules	
[redacted]	[redacted]
Subscriber Filter Rules	
Allow list (Opt In)	Allows subscribers to designate that only specific SMS messages are accepted
Block list (Opt out)	Allows subscribers to designate that specific SMS messages are blocked

Table 1.7.1.4-8: Message Blocking. *The Cingular network prevents malicious or illicit messages based upon network filter rules and subscriber filter rules.*

The two-tier system provides general filtering of messages that enter the network and selective filtering of messages as defined by the subscriber.

When desired by a subscriber (**Figure 1.7.1.4-5)**, the network will allow legitimate bulk content such as downloadable files (e.g. tones, graphics, vCards, etc.), free opt-in content (subscriptions to text-based information for mobile users), email forwarding (ISPs and Portals may forward copies of emails to mobile terminals), and Enterprise “message blasting” and alerts (as a pager replacement) to be delivered to the subscriber equipment.

Figure 1.7.1.4-5: Message Filtering. [redacted]

1.7.1.4.f Architecture Security and Reliability Best Practices

(f) Describe how the wireless network architecture is consistent with best practices for security and reliability.

Cingular maintains a broad range of security policies including physical, systems, and customer-access controls designed to protect the network and customers from malicious activity and keep it operating reliably (**Table 1.7.1.4-9**).

PRACTICE	IMPLEMENTATION
	Physical Security
Access	[redacted]
Enforcement	[redacted]

PRACTICE	IMPLEMENTATION
	Systems Security
Service Control	
Firewalls	
Encryption	
IP Controls	
Network Separation	
Operational Controls	

Table 1.7.1.4-9: Cingular Systems and Physical Security Practices. *Cingular maintains security policies that prevent malicious activity in facilities or in the network. In addition, customers access the network over protected and authenticated means to prevent fraud.*

Additionally, Cingular and AT&T have implemented reliability best practice measures that protect subscribers' communications and provide quality service while traversing the network (**Table 1.7.1.4-10**).

PRACTICE	IMPLEMENTATION
Redundant network systems	
Independent power	
Monitoring	
SONET	
Automation	
Frequency management	
Cell overlap	

PRACTICE	IMPLEMENTATION
Emergency response	[redacted]

Table 1.7.1.4-10: Security Measures. *Cingular maintains security policies that prevent malicious activity in facilities relating to the network.*

AT&T and Cingular will help secure sensitive Government data against disruption and interception. Agencies' data is always carried in environments with comprehensive security and service protection policies and over network elements implementing state-of-the-art operational features.

1.7.1.4.g Approach to Number Portability

(g) Describe the approach for implementing number portability. Discuss the benefits and limitations of the approach.

Cingular has fully imlemented Local Number Portability (LNP) functionality mandated by the 1996 Telecom Act. This feature allows eligible incoming customers to retain their existing phone numbers when switching to the Cingular network, thus eliminating the need to notify associates of contact detail changes, minimizing the time subscribers are out of touch. Most LNP requests are processed and implemented in less than 6 hours, with the primary timeframe dependency being the cooperation of the outgoing carrier. There are eligibility requirements and limitations within LNP, summarized in **Table 1.7.1.4-11**.

LNP LIMITATION	DISCUSSION
Number eligibility - Requested numbers must be confirmed as eligible in order to be ported through the Portability Eligibility Tool (POET)	Eligibility affects the capability to port numbers – POET checks that incoming subscribers are not changing services areas, and have provide proof of ownership of the requested accounts, among other variables
LNP process requires cooperation from the outgoing carrier, some of which have limited experience or capability in the LNP process	Outgoing carriers are required by law to cooperate in the LNP process, but some smaller carriers have difficulty complying – this has historically created delays in porting numbers
Subscriber must have Cingular-compatible equipment in hand before process can complete	Subscribers either must acquire Cingular equipment or an approved, compatible cellular phone – users can determine if their equipment is compatible by calling customer service
Port cannot complete activation until customer receives the wireless equipment and calls the 800 number to activate	Subscribers must simultaneously activate a wireless account at the completion of the LNP process – in order to do so, the wireless equipment must be in hand with all appropriate identification numbers

LNP LIMITATION	DISCUSSION
Wireline-to-wireless porting is still not as efficient as porting between wireless carriers, and can take considerably longer, sometimes up to one month	The porting process of working with a wireline carrier is different than working with a wireless carrier: • Different systems are utilized by wireline carriers than wireless carriers • Wireline carriers are not covered under the same guidelines that wireless carriers agreed to before number porting launched • These alternate processes are not specific to Cingular and all other wireless carriers that port with wireline carriers are impacted

Table 1.7.1.4-11: Limitations and Dependencies of Local Number Portability. *Successful LNP implementations are limited to eligible numbers and require cooperation from outgoing carriers as well as action by the requesting subscriber.*

The required steps within an LNP implementation are:

- Subscriber collects pertinent information:
  - Wireless number to be ported
  - Account owner name or administrator name that is identified on the account of the outgoing carrier's records
  - Exact billing address and subscriber information as provided to outgoing carrier
  - Outgoing carrier's account number, Tax-ID, and/or SSN as applicable
  - Any passwords or PIN identifications of the old account
  - Another unrelated phone number for contacting the subscriber if needed during the LNP process
  - Desired subscriber equipment for new order or the existing equipment in hand (only compatible equipment supported) with serial number access.

Agency subscribers specify an LNP request at the time of a Networx CPCS order. If the subscriber already has a compatible handset, the port will typically be completed within six hours.

Cingular notifies the outgoing carrier of the LNP request. Port availability time is dependent on them - it may take longer than six hours to complete the port (Some small carriers asked for regulatory relief from the May 24th 2004 deadline, so LNP may not be available from some smaller carriers)

1.7.1.4.h Approach to Incorporate Security Enhancements

(h) Describe the approach for incorporating into the offeror's wireless network, infrastructure security enhancements that the offeror believes are likely to become commercially available in the timeframe covered by this acquisition, including discussion of potential problems and solutions.

Due to the criticality of maintaining GSM standardization while simultaneously driving technological innovation, Cingular is a member of key standards development organizations and Industry forums. Cingular places high importance on participation and collaboration with GSM technology forums, and takes leadership roles in shaping the overall future of wireless communications. Throughout these organizations, Cingular has delegates that follow the relevant activity in each group.

1.7.1.4.h.1 3G Security: Security Threats and Requirements, 3GPP TS 21.133

Cingular Wireless takes proactive mitigation measures to protect its wireless network against security threats [redacted]

The backend wireless provisioning systems, storage systems (such as HLRs) and self-service systems are hardened according to corporate security baseline standards to protect against misuse or misappropriation of subscriber information. The controlled access of subscriber information is only granted after successful authentication [redacted]

GSM/UMTS mutual authentication (using USIM or GSM SIM) and radio interface encryption are enabled so that the resources and services provided by servicing network and home environments are adequately protected against misuse or misappropriation by malicious wireless intruders.

[redacted] The controlled access of Cingular Wireless network from business partners is only granted after successful authentication and is protected by [redacted]

1.7.1.4.h.2 3G Security: Cryptographic Algorithm Requirements, 3GPP TS 33.105

[redacted] the mutual authentication of both the subscriber and the cellular network is enabled and GSM/UMTS radio interface encryption is enabled.

1.7.1.4.h.3 3G Security: Security Principles and Objectives, 3GPP TS 33.120

The Cingular Wireless GPRS/EDGE/UMTS network enforces mature and proven security practices accepted within our industry segment. Cingular Wireless GPRS/EDGE/UMTS network retains and enhances the proven security features in the second generation GSM network and minimizes the security weaknesses of the GSM network. It continues to evolve toward improved security aligning with industry practices.

1.7.1.4.h.4 NIST FIPS Publication 140-2

Cingular recommends and interoperates with commercial off-the-shelf products from our business partners that are FIPS 140-2 compliant. Cryptographic modules introduced into our network have been adequately assessed and evaluated and appropriate level of assurance is provided.

1.7.1.4.i Approach to Network Convergence

(i) Describe the approach for network convergence (i.e., IP Multimedia Subsystem (IMS terminal)). In particular, describe how the approach ensures service quality over the converged network for data, voice, video, and multimedia.

[redacted]

Figure 1.7.1.4-6 [redacted]

[redacted]

Figure 1.7.1.4-6: The IMS [redacted]

1.7.1.4.j Approach to 2.5G-to-3G Migration

(j) Describe the approach for 2.5G-to-3G migration.

Cingular was the first North American wireless carrier to deploy EDGE, the high-speed data solution offering rates up to 130kbps that is available in all markets. The full deployment of EDGE brings the Cingular network to a fully implemented 2.5 status, an important interim step toward offering UMTS-based 3G services and, ultimately, HSDPA. Further detail on the Cingular's approach toward 3G service is provided in **Table 1.7.1.4-12**.

APPROACH	BENEFIT
[redacted]	[redacted]

Table 1.7.1.4-12: Keys to 3G migration. *Cingular has completed several key steps towards offering 3G services to its subscribers without wide scale disruptions to service.*

[redacted] (**Figure 1.7.1.4.l-1**).

Figure 1.7.1.4.I-1: [redacted] of RF Network. [redacted]

1.7.1.5 Stipulated Deviations

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

1.7.1.6 Narrative Text Requirements

1.7.1.6.1 Data Optimized Capabilities

The following Cellular/Personal Communications Service capabilities are mandatory unless indicated otherwise: Offerings may include data optimized capabilities including EvDO, HSDPA, or equivalent standards. (optonal)

Cingular today offers Agencies optimized data capabilities over an expanding coverage area with its new HSDPA service. Cingular is implementing an aggressive program to build out HSDPA within its markets, and projects that approximately 80 major markets in the US will be

operational by year end 2006, and approximately 100 major markets served in the second quarter of 2007. For additional information on the capabilities and implementation of HSDPA, please refer to **Figure 1.7.1.1-5:** Increasing Data Speeds and Section **1.7.1.4.j** Approach to 2.5G-to-3G Migration, respectively.

1.7.1.7 Technical Clarifications

Unlimited Voice Services

Unlimited voice services are provided solely for live dialogue between individuals. Unlimited voice services are not engineered for monitoring services, data transmissions, transmission of broadcasts, or transmission of recorded material.

Roaming

The use of Networx CPCS services when roaming is dependent upon the roaming partners' support of applicable network technology and functionality. A compatible international-capable device is required to use data services while roaming internationally.

When outside the coverage area, access will be limited to information and applications previously downloaded to or resident on the device.

Service Availability and Access

Services (including without limitation and/or service areas) are subject to change. Coverage areas vary between services. Actual data download speeds depend upon device characteristics, network, network availability and coverage levels, tasks, file characteristics, applications and other factors. Performance may be impacted by transmission limitations, terrain, in-building or in-vehicle use and capacity constraints.

Information and Content

Regarding Information and content provided by third parties, the service is engineered such that:

- Information or content available to the Networx user through Networx CPCS Information Services and web browsing is provided by independently owned and operated content providers or service providers who are subject to change at any time without notice.
- AT&T is not a publisher of third-party information or content and is not responsible for any opinions, advice, statements, or other information, services or goods provided by third parties.
- Third-party content or service providers may impose additional charges.
- Policies regarding intellectual property, privacy and other policies may differ among AT&T's content or service providers and therefore the Networx CPCS user is bound by such policies when visiting their respective sites or using their services.
- It is the responsibility of the Networx CPCS user to read the rules or service agreements of each content provider or service provider when accessing their services.
- Any information that is involuntarily or voluntarily provided to third parties by the Networx user is governed by their policies.
- The accuracy, appropriateness, content, completeness, timeliness, usefulness, security, safety, merchantability, fitness for a particular purpose, transmission or correct sequencing of any information or downloaded data is not guaranteed or warranted by AT&T or any content providers or other third party. AT&T remains responsible for the transmission of data in accordance with the terms and conditions of the Networx contract.
- Delays or omissions may occur.

- Neither AT&T nor its content providers, service providers or other third parties shall be liable to the Networx CPCS user for any loss or injury arising out of or caused, in whole or in part, by any information acquired through the Service.
- AT&T nor its content and service providers or suppliers, in providing the Networx CPCS user access to information, underwrites, can underwrite, or assumes the user's risk in any manner whatsoever when accessing information.

CPCS Data Plans

Data plans enable: (i) Internet browsing; (ii) email; and (iii) intranet access (including access to intranets, email, and individual productivity applications). Data plans are not engineered to support uses that cause extreme network capacity issues or which may result in interference with the network.

Data plans are not engineered to support the following uses: (i) server devices or host computer applications, including, but not limited to, Web camera posts or broadcasts, automatic data feeds, automated machine-to-machine connections or peer-to-peer (P2P) file sharing; (ii) as a substitute or backup for private lines, landlines or full-time or dedicated data connections; (iii) "auto-responders," "cancel-bots," or similar automated or manual routines which generate excessive amounts of net traffic, or which disrupt net user groups or email use by others; (iv) software or other devices that maintain continuous active Internet connections when a computer's connection would otherwise be idle or any "keep alive" functions.

The Networx CPCS data plans (unless specifically designated for tethering usage) are not engineered for use of any applications that tether the device (through use of, including without limitation, connection kits, other phone/PDA-to computer accessories, Bluetooth® or any other wireless

technology) to Personal Computers (including without limitation, laptops), or other equipment for any purpose. AT&T acknowledges that for purposes of this section, “tethering” does not include routine device synching.

SMS and MMS

SMS and MMS messages, including downloaded content, not delivered within 7 days, will be deleted. Some elements of MMS messages may not be accessible, viewable, or heard due to limitations on certain wireless phones, PCs, or e-mail. The delivery of SMS/MMS messages sent by an AT&T customer to another user (not necessarily on the AT&T network) is reliant on the receiving user’s equipment and or vendor status (i.e. turned off, broken, out of service, etc.). For these reasons, AT&T does not guarantee the delivery of messages.

Text message notifications may be sent to non-MMS subscribers if they subscribe to SMS.

CPCS Security

AT&T does not guarantee security for Networx CPCS. Data encryption is available with some, but not all, Wireless Services sold by AT&T.

If the device is used to access company email or information, it is the responsibility of the user to ensure that the service usage complies with the Agency’s and / or Government’s internal IT and security procedures.

Access Requirements

Additional hardware, software, subscription, internet access from the Agency’s and/or user’s compatible PC and/or special network connection may be required and the Agency and/or its users are solely responsible for arranging for or obtaining all such requirements. Some solutions may require third party products and/or services, which are subject to any applicable third

party terms and conditions and may require separate purchase from and/or agreement with the third party provider.

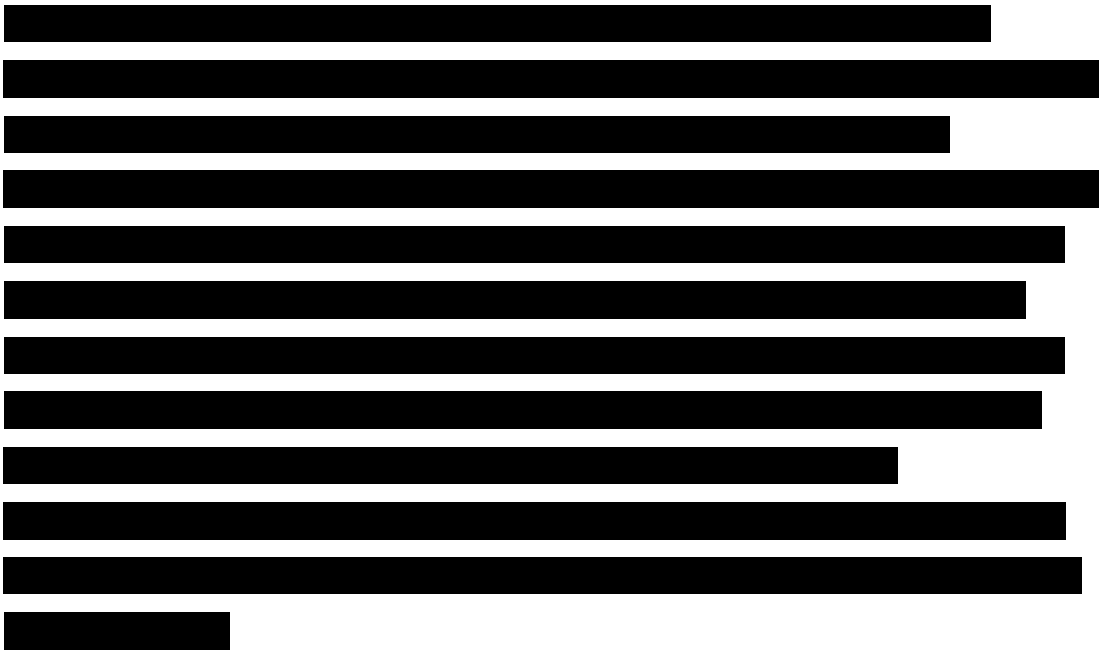
The Agency and/or its users are solely responsible for access to, and use of the preceding hardware, software or other such items/requirements.

Subscribing agencies ordering AT&T's Networx CPCS will be notified of these technical clarifications prior to their acceptance of the service.

Unlimited Data and SMS Bundled Plans

AT&T is offering two bundled unlimited domestic Data and domestic SMS plans on Networx. One is specifically for service with the BlackBerry feature, and the other is the basic data and SMS bundle. These two bundled plans offered by AT&T will be available beginning August 1, 2009.

Apple iPhone Service Clarifications



Apple iPhone handsets will be shipped by AT&T to the ordering Agency for activation and distribution to each individual, Agency-designated, employee, End User.

[redacted]