4 NETWORX ARCHITECTURE FOR IP-BASED SERVICES (L.34.1.3)

The offeror shall describe the means by which its infrastructure will support the delivery of high quality, secure, and reliable Transport/IP/Optical, Management and Applications, and Security Services. Table L.34.1-2 lists the mandatory services for the Enterprise Proposal for IP-Based Services.

The Government recognizes that the telecommunications industry has changed significantly since the award of the FTS2001 contracts, as described in the Networx RFP. Such change will continue throughout the lifecycle of the Networx program. Sprint presents our Networx Enterprise technical volume comprising Service types that initially meet and continually evolve with the needs of the Government.

Highlights of the Sprint Networx Architecture

- Mechanisms and controls, best practices leadership and experience comprising our approach to infrastructure security
- Industry-leading networks engineered to avoid congestion, not manage it, to deliver service quality and reliability
- Executing plans for a converged IP architecture capable of interoperability and evolution
- Global, Tier 1 IP network and a history of relationships to provide non-domestic services
- NS/EP and Section 508 strategies for addressing National Policy-Based Requirements
We provide, via the Networx Enterprise procurement, a full-service portfolio similar to that of a Networx Universal offeror. This portfolio includes wireless and wireline telecommunications services, management, applications, and security solutions that are consistent with the goals of the Networx Enterprise procurement. The Networx Architecture extends beyond the service delivery of Networx Service Types. As shown in Figure 4-1, it provides a framework for focusing on integrated Networx solutions allowing Federal Agencies to use Networx as a vehicle to support their missions and fulfill Federal Enterprise Architecture (FEA) objectives. It also provides a framework for focusing on integrated solutions.
The Sprint commitment to the Government, the Sprint history of innovation, best practices, and our defined plan for Network Evolution drives Networx Architecture.

Benefits of the Sprint Converged IP Strategy

- Simplified IT service delivery helping Federal Agencies address FEA objectives
- Enhanced performance supporting network/application convergence and enabling greater performance-based contracting opportunities
- Increased value due to fewer pricing components
- Added opportunity for lower Total Cost of Ownership (TCO)
- Enhanced focus on new and evolving applications, rather than transport, capable of serving Federal Agency users wherever they are via an integrated wireless/wireline architecture
SprintLink and Sprint Peerless IP provide excellent converged IP platforms for the Government. Originally designed in response to Government needs, the Sprint IP networks support Multiprotocol Label Switching (MPLS) Virtual Private Networks (VPNs) and a suite of Security Services critical to Government enterprise networks. Engineered to avoid congestion, not manage it, they are capable of providing the secure, interoperable services sought by the Government while protecting time-sensitive traffic. We plan to use IP networks over the contract term to deliver the service types sought by Networx. Many service types, such as IP-VPNs, VoIPTS, and CPCS data already leverage IP networks. Others, such as traditional voice, evolve over the contract term. In such cases, we continue to leverage technologies such as self-healing 4 Fiber Bidirectional Line Switched Rings (4FBLSRs), the early adoption of which Sprint pioneered. Regardless of the transport, Sprint designs its services for service reliability and employs similar engineering philosophies to provide service quality.

Our multi-service wireless and wireline access platforms provide flexible options for connecting Federal Agency users, regardless of their location. These access arrangements evolve during Networx to focus on converged IP access, rather than disparate access methodologies, enabling Federal Agencies to employ more ubiquitous solutions. We continue to provide the suite of wireline access methods in Networx that the Government relied on during prior FTS contracts. This includes traditional Sprint Provided Access (SPA) up through OC-n bit rates.

Our 16 year partnership with GSA yielded network savings as the predominately use of private lines evolved to frame relay. Sprint is ready to deliver enhanced benefits via our Networx Architecture based on industry-leading converged IP solutions.

The Department of Homeland Security, through the US Visit program, is saving human resources and network costs by using Sprint's wireless access services in kiosks in over a dozen large airports.
and additional access arrangements such as Digital Subscriber Line (DSL), where commercially available from the offeror. Augmenting Networx wireline access options are multiple wireless access arrangements. Using the unique mix of Sprint wireless spectrum holdings and Code Division Multiple Access (CDMA) and Integrated Digital Enhanced Network (iDEN) technologies, we enable Federal Agencies to serve their customers and constituents through advanced mobility applications.

Sprint has the criteria for success in delivering the Networx Architecture. More important than simply having a range of technologies available is having and executing a plan that will unify and leverage technologies for delivering customized solutions to Government Agencies. With many years experience operating industry-leading wireless and wireline networks, Sprint has planned for the next generation architecture. We evolve the network to use unifying signaling and control technologies such as the IP Multimedia Subsystem (IMS). More information on technological evolution and planning is contained throughout this section. Finally, Sprint has transformed the company to focus on solutions—not products—to offer a new generation of solutions based on our combined years of service to the Government.

Customs and Border Protection is able to monitor more border crossings with fewer resources through the use of non-staffed remote video surveillance technology implemented using a Sprint Managed MPLS VPN over Peerless IP. We have a proven track record of delivering solutions and evolving our architecture to meet the needs of the Government: SprintLink, Peerless IP, and first-generation ATM networks built to address government needs Managed Network Services and Managed Security Services offerings allowing Government to increase Return on Investment (ROI) and mission focus Mobility solutions to support secure, wireless data applications Hundreds of customized solutions offered under prior FTS contracts providing options sought by Federal Agencies
We provide governance for the Networx Architecture by collaborating closely with the Government. Included in our proposal is the recommendation to form a Networx Technology Council that will allow the Government and Sprint to drive technology innovation and new and emerging services for the Networx contract. This yields a Networx Technical Environment that is not just capable of providing the service types sought in the RFP, but one that specifically focuses on meeting new and evolving needs of the Government.

Through technology refresh, customizable Networx service offerings such as CSDES, and our team including the systems integration capabilities of Lockheed Martin, we provide a flexible means for delivering the "Integrated Networx Solutions" sought by Federal Agencies. The Sprint Converged IP Architecture enables us to focus on such solutions by simplifying service delivery and improving security and reliability. Yes, the Government can have multiple wireline service types delivered over an optimized, converged, native IP infrastructure. Yes, the Government can facilitate FEA objectives using applications that allow Federal Agencies to stay more connected with the citizens whether in wireline-accessible offices or by using wireless in the field. Yes, the Government can achieve solutions, not simply products, through Sprint—a full-service telecommunications provider teamed with Lockheed Martin, the leading systems integrator, and other technology partners.

Included in the following sections are our responses to Infrastructure Security; Service Quality and Reliability; Networx Architecture, Convergence, Interoperability, and Evolution; Network Convergence; Non-Domestic Services; and National Policy-Based Requirements. Additional details specific
to Service Type roadmaps and their relationship to the Networx Architecture are contained throughout the technical volume.

4.1 APPROACH TO ENSURING INFRASTRUCTURE SECURITY (L.34.1.3.1)

4.1.1 Infrastructure and Security Mechanisms and Controls (L.34.1.3.1 (a))

Describe the mechanisms and controls that the offeror uses in its network(s) to ensure protection of the offeror’s infrastructure and provide security for the services offered to its customers.

Sprint has proven security mechanisms and controls for all operations to protect our infrastructure and ensure the security of services offered via Networx. We have a comprehensive approach to ensuring infrastructure security including:

- A “defense in depth” approach based on industry best practices for deploying security mechanisms and controls
- Measures to provide protection for known attacks, as detailed in our internal security portal that alerts teams to new threats
- Methodical processes for adding enhanced security to the network and additional services for our customers
- A proven track record supporting the government in the C&A process with internal Sprint and small business resources

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

Volume 1 Technical—4, Networx Architecture

Page 7

March 5, 2007
Given the sensitive nature of Sprint services and operations, we protect information assets according to their defined value and risk. We use specific mechanisms and controls defined by the Sprint Protection of Proprietary Information (POPI) to mitigate risks to an acceptable level. The POPI is the Sprint comprehensive security policy and is a collection of standards, policies, and security best practices. It establishes the requirements for the security of information assets and identifies the principles upon which these requirements are based. Information assets, regardless of their source, are valuable assets.

Their integrity, availability, and confidentiality are essential to our business operations and to our relationships with associates, company representatives, and our Federal Agency customers. The POPI policies and best practices derive from industry standards (ISO/IEC 17799:2000 (E)), NRIC, NIST Standards and Guidance, Information Security Forum Standards of good Practice, Data Protection Act of 1988, and Government Regulations – HIPPA, GLBA, and Sarbanes Oxley. In addition, they conform to current Federal and commercial security standards, and we plan to align the POPI with future standards, as they are approved and applicable.

The POPI policy domains shown are enforced across various Sprint assets, including customer data entrusted to Sprint, to protect assets. Sprint Protection of Proprietary Information Policy Domains

- Software
- Personnel
- Physical/Environmental
- Identification/Authentication
- Access Controls
- Business Continuity Planning
- System Integrity
- Encryption
- Audit
- Monitoring and Response
- Data Network Security
- IS Operations
Corporate Security protects assets by defining security mechanisms and controls across multiple policy domains. Sprint Corporate Security leads our approach to infrastructure security. The head of this organization is a Vice President who is also the Chief Security Officer for Sprint. Sprint ensures the objective implementation of security policies and procedures through Corporate Security's independence from other Sprint business units. Sprint Corporate Security has six functional directorates that provide the full spectrum of security support to its internal and external customers. Investigations; Physical Security; Network & IT Security; Data Security Operations & Engineering; Identity Management & Access Control; and Homeland Security. Within Sprint Corporate Security, the Security Operations & Engineering/ Government Systems (SO&E/GS) Team will operate the Sprint Networx Security Program from its offices in Reston, Virginia. More information about SO&E/GS and the Networx Security Program is included in Plan 3, Security Management, of the Management Volume.

4.1.2 Protecting Against Cyber Attacks (L34.1.3.1 (b))

Describe the measures to provide protection to the offeror's infrastructure against cyber attacks (e.g., Denial of Service (DoS), Domain Name Server (DNS), H.323, and SS7 attacks, Spoofing, routing table corruption).

Sprint has extensive measures in place to protect our infrastructure from cyber attacks.
with a comprehensive security program that should be expected from a Networx offeror with our experience. We have appropriate incident and crisis response capabilities within our Security Operations Centers and have formed Critical Incident Response Teams to effectively respond to cyber attacks that we are unable to prevent.

Specific mechanisms and controls used to enforce the POPI vary by the infrastructure being protected, but include the following types of items:

- Example Mechanisms and Controls
  - Operational support infrastructure protections such as operations networks protected with firewalls, IDS/IPS systems, monitoring systems, etc.
  - Layered controls for router/system access (e.g., strong authentication, restrictions based on multiple type of access privileges), physical security (e.g., security guards, entrance monitoring/logging), etc. to mitigate spoofing, tampering, or router table corruption.
  - Policies to block certain types of traffic, for example, packet types that are common causes of Denial of Service/Distributed Denial of Service (DoS/DDoS) attacks.
  - Support for customer filtering policy requests on Sprint edge routers to mitigate attacks known to customers.
  - Session Border Controllers (SBCs) acting as VoIP signaling proxies that dynamically create firewall rules on a per-call basis based on an established trust to mitigate VoIP signaling attacks.
  - Deep packet inspection firewalls to inspect packets, such as H.323 or SIP signaling packets, that may be used as part of an attack.
  - SprintGUARD Plus fraud protection services to mitigate SS7 or other toll fraud.
  - Comprehensive managed security services portfolio as outlined in Section 7—including Managed Firewall, Intrusion Detection and Prevention, E-Authentication, Managed Firewall, etc. to provide Federal Agencies with tools to mitigate a host of cyber attacks.
  - MPLS VPNs and a Peerless IP transport option minimizing potential threats to Federal Agencies.
  - Acceptable Use Policies (AUPs) that augment a response strategy to customer-initiated attacks.

Central to the Sprint approach to deploying countermeasures is a structured knowledge management process that consolidates information and provides it to groups throughout Sprint. Our system fulfills several functions that define policy, facilitate communication, and enable protection, detection,
and rapid response against cyber attacks. Included in the online security system's list of policies and standards is the Sprint POPI. As described in Section 4.1.1, The POPI is our comprehensive security policy for networks, systems and data. One of the goals of the POPI is to maintain and enforce prudent and reasonable controls for the protection of information assets.

One way Federal Agencies may minimize threats is to procure Networx services that use the Sprint Peerless IP platform or MPLS VPNs. As a network logically separate from the public Internet, the Sprint Peerless IP network is not exposed to threats that originate on the Internet and is controlled solely by Sprint. MPLS VPNs isolate Federal Agency traffic in to networks logically separate from their underlying IP transport. Sprint MPLS VPNs may be procured using the Peerless IP platform or via the global SprintLink network.

To explore a particular cyber attack in greater detail, consider the example of DoS/DDoS attacks. The Sprint IP operations group reviews the Sprint POPI and best practices information for applicable policies and standards. Our online security system provides current threat analysis and vulnerability management to help protect against the latest threats. Sprint proactively blocks packet types that are common causes of DoS. We also provide multiple layers of security to block intrusion. For example, we limit traffic to only those ports approved at the router, switch, and server levels. We will support Federal Agencies' requests for filtering policy enforcement at our IP network edge routers. Finally, Sprint provides a comprehensive set of solutions under the Networx contract vehicle that further minimize the threat of DDoS/DoS attacks such as the Security Services Types in Section 7.
4.1.3 Best Practices for Security and Reliability (L.34.1.3.1 c))

Describe how the network architecture is consistent with best practices for security and reliability.

The Sprint network architecture is consistent with best practices for security and reliability. We have always had a strong corporate commitment to protecting our infrastructure from threats that may jeopardize the integrity or availability of the services we provide our Federal customers. This commitment is evident at the highest levels of Sprint.

Sprint Traits of Best Practices
- Encourage and support standards and interoperability
- Address "classes" of problems where possible, noting that some problems are specific
- Involve adherence by one or more companies
- Facilitate industry consensus by avoiding endorsements of commercial products, processes, or services

Sprint was recognized by Aberdeen Group for employing "Best Practice in Security Governance in 2005."
2005, the AberdeenGroup, a research and benchmarking firm serving global business and technology executives, recognized Sprint for its effort with the “Best Practice in Security Governance in 2005” award. The Aberdeen Group based the award on its research, which involved 200 companies from various industries known for operating at best-in-class levels.

Sprint supported the Network Reliability and Interoperability Council (NRIC) since its inception in 1992, and we continue to participate actively in the NRIC and its committees. Originally chartered by the FCC as the Network Reliability Council (NRC), the NRIC is a Federal Advisory Committee that affords Sprint the opportunity to provide recommendations to the FCC and our industry counterparts and collaborate with them on solutions. The role of the NRIC has recently assumed greater importance given the country's focus on homeland security and the current threats to network security. Whereas in the past, the NRIC focused on relatively straightforward telecommunications concerns such as power interruptions, fiber cuts, and equipment failures, the work of Sprint with the NRIC has recently focused on hardening core network elements to improve the overall security and reliability of the national infrastructure.

NRIC deliverables consist of industry best practices developed with collaborative input from major industry players. While implementation of NRIC deliverables is voluntary, we place a high importance on our participation and the value of its deliverables in improving service quality throughout the industry. Sprint uses NRIC deliverables and our participation.

Objectives of the Network Reliability Interoperability Council

- Ensure security and reliability of the U.S. public telecommunications networks
- Provide the means for adequate network capacity during events such as natural or manmade disasters
- Facilitate rapid restoration of services in the event of major disruptions
experience in two ways: First, we proactively review deliverables to incorporate new best practices wherever feasible. Second, we have added a review of NRIC best practices into the Sprint Event Analysis process to improve service quality.

We have a best practices team dedicated to knowledge management and implementation of best practices, including NRIC deliverables, throughout Sprint.
lessons learned from an event with best practices that may further minimize occurrence of the event and improve overall service quality. Sprint is committed to improving service quality for Federal Agencies through support of groups like NRIC.

Figure 4.1.3-1. Best Practices and Event Analysis

Sprint has added a step to our event analysis process to review NRIC Best Practices for applicability, benefiting Federal Agencies through improved service reliability.

As shown in Figure 4.1.3-2, best practices are the focal point of the Sprint approach to network reliability. Not only have we invested heavily in internal
processes to support best practices, but we also play a vital leadership role in the formation of such standards.

Figure 4.1.3-2. Best Practices Focus on Service Delivery

*Best Practices are the focal point of the Sprint Event Analysis Process, enabling Federal Agencies to benefit from industry-standard approaches to service delivery improvement.*
Sprint bases its security best practices on a multi-tiered or "defense-in-depth" approach to information security. As described in Section 4.1.1, the Sprint POPI is our comprehensive security policy that governs the protection of Sprint infrastructure and the services provided to customers. Comprised of three layered focus areas, "defense-in-depth" is a best practice philosophy that defines the objectives of our information security program. As shown in Figure 4.1.3-3, the high-level objectives of the Sprint information security program are not only to protect network infrastructure from threats, but also to detect when attacks are occurring and respond with appropriate actions. Our experience and accepted security best practices demonstrate that addressing one objective, such as "protect," without the others results in an ineffective security program.

Figure 4.1.3-3. Defense in Depth

Consistent with security best practices, Sprint knows that an effective security program must establish objectives using a "defense-in-depth" approach. Simply deploying countermeasures without follow-up action is not enough.
4.1.4  Incorporating Security Enhancements (L.34.1.3.1 (d))

Describe the approach for incorporating into the offeror’s network, infrastructure security enhancements that the offeror believes are likely to become commercially available in the timeframe covered by this acquisition. Include a discussion of potential problems and solutions.

We incorporate infrastructure security enhancements, both in the form of security solutions offered to our customers, and security enhancements related to operation of Sprint infrastructure and service delivery under the Networx contract. As with our approach for incorporating infrastructure enhancements and emerging services, described in Section 4.3.4, we incorporate security enhancements to deliver improved service to our Federal customers while minimizing implementation risks.
Sprint updates its plan for infrastructure security enhancements, the Network Security Technology Evolution Plan (TEP), annually. Security evolution, an integral part of the overall Sprint Network Evolution Plan (NEP), factors security considerations into the overall plan for our infrastructure and the services offered to our customers.

The Sprint POPI security policy detailed in Section 4.1.1, our best practices for security explained in Section 4.1.3, security oversight from Sprint Corporate Security, and technology planning from Sprint Technology Research and Development (TR&D) guide our security evolution.

Specific to the Networx contract, Sprint prepared a Security Plan focusing on the Sprint Networx services program. Sprint addresses throughout this plan the specific technical, management, and operational controls that protect customer assets under Networx. Consistent with offering routine security enhancements, Sprint will update the Security Plan within 30 calendar days of Notice to Proceed, and then annually thereafter. Additionally, Sprint will include the Security Risk Assessment Report and any mitigation efforts planned or in place to reduce risk. The Security Plan is attached to the Management Volume of this proposal.

Sprint addresses potential problems associated with infrastructure security enhancements largely by proper planning and customer involvement. Security enhancements, along with all technology upgrades at Sprint, follow a Potential Infrastructure Security Enhancement Drivers:

- Incorporation of industry best practices
- Compliance with standards, regulations or revised Sprint security policy guidance
- Opportunity to leverage knowledge gained through our 16 years of supporting FTS customers to address security needs faced by Federal Agencies
- Ability to offer enhanced security services to our customers
- Opportunity to improve the overall security posture of our infrastructure
detailed implementation process to mitigate risk. Sprint works closely with vendors and partners to develop and evaluate emerging security technology. These relationships allow us to convey security requirements to the vendors during their product development process. Doing so provides the vendors with an opportunity to release products that meet or exceed Sprint requirements for network security, which ultimately reduces the time required to bring the product to the federal marketplace. Sprint makes thorough evaluations of potential technology enhancements in Sprint test labs. Once selected, Sprint designs and implements the enhancements according to detailed plans. If planning cannot address an unforeseen problem, network upgrades apply back-off plans to reverse changes and allow operations to return to the baseline configuration.

4.1.5 Experience Supporting the Development of Certification and Accreditation Documentation (L.34.1.3.1 (e))


Sprint has extensive experience supporting the Government in developing documentation required in the Certification and Accreditation (C&A) process. Our experience covers support for a variety of civilian Agencies, defense Agencies, and corporations charged with critical missions for protecting the country and its economy from threats. Sprint incorporates infrastructure security enhancements, required to address security policy provisions, into our network as they become commercially available.
Risk Assessment, as requested. As an additional option, Sprint is ready to assist Federal Agencies in their C&A activities by preparing all necessary certification documents.

In addition to security expertise and experience resident within Sprint, we have added a complementary teammate to assist with C&A efforts. SphereCom Enterprises Inc., which is also one of our team’s woman-owned small business partners consistent with our subcontractor diversity goals, is an IT services company that provides information assurance and system security, telecommunications engineering, and business support services to Government and commercial clients. Sprint and SphereCom have worked together for almost ten years preparing security documentation. We added SphereCom to our team specifically because their core competency is preparing security documentation packages in support of system Certification and Accreditation.

Sprint is familiar with NIST FIPS PUB 800-37, Guide for the Security Certification and Accreditation of Federal Information Systems, and has used this guide as well as many other sources of security guidance including those shown below in “Examples of Security Guidance Used by Sprint.” Sprint and SphereCom have developed comprehensive security plans and C&A packages for secure telecommunication systems that were fielded as part of the National Information Infrastructure (NII). These certification packages included complete details of all system components and operations as documented in System Security Plans, System Security Authorization Agreements, Computer/System Emergency Response, and Incident and Audit Reporting Plans and Procedures, Disaster Recovery and Contingency Plans.

Sprint has assisted with C&A efforts for several Federal Agencies including large Agencies charged with supporting the security and finances of the country.
4.2 APPROACH TO ENSURING SERVICE QUALITY AND RELIABILITY (L.34.1.3.2)

4.2.1 Characteristics and Performance of Access Arrangements (L.34.1.3.2 (a))

Describe the characteristics and performance of the access arrangements that will connect to the offeror's backbone network(s) to ensure service quality and reliability. Describe how the performance is consistent with industry best practices.

Sprint, as a current FTS2001 service contractor, is already providing the Government most of the access services required for Networx. We have taken great effort to support FTS2001 contract modifications to add emerging service technologies and access capabilities as these have become available. We will continue to do so for Networx.
services at a wire center from the same Sprint Point of Presence (POP) based on industry best practices such as leveraging the Local Exchange Routing Guide (LERG) if the SDP is also a Public Switched Telephone Network (PSTN) location.

Sprint will always provide access unless specifically requested not to do so by the Government. Access arrangements include wireless, cable, and satellite in addition to the traditional wireline arrangements such as fiber and copper from Sprint, Local Exchange Carriers (LECs) and Alternate Access Vendors (AAVs). All these access methods have contributed to more options, lower costs, higher bandwidths and more reliable connections to Agency locations.

Sprint will provision access to conform to UNI specifications at the SDP or specifications at the POP, as defined in the individual service descriptions. Sprint will periodically review and may make recommendations to adjust the quantity of access circuits, dependent on the traffic volume generated by a location to optimize performance, maintain service quality, and ensure reliable service. The performance provided for the above access types will always be within the specifications of RFP Section C and at a minimum what is available for basic commercial services.

Our Approach to Service Quality and Reliability Provides Federal Agencies:

- Access arrangements, based on industry best practices that provide service quality and reliability
- Extensive peering and roaming agreements consistent with Federal Agency expectations of a Tier 1 ISP and communications integrator
- Flexible congestion and flow control strategies based on sound engineering principles that are able to dynamically handle changes in traffic conditions
- An approach for verifying KPIs consistent with GSA performance-based contracting objectives
- Agency-definable quality of service support leveraging standards-based DiffServ technology for protecting time-sensitive traffic
With the exception of inside wiring, Sprint will provide all necessary hardware and software for provisioning of the dedicated access to the SDP as part of the service. The provision of inside wiring is at the user’s choice, and may be provided by the user, a Government’s designated contractor, or by Sprint.

Sprint understands that the Government will authorize the use, without charge, of a reasonable amount of space and power at Government locations for the installation of contractor equipment. In summary, Agencies will be able to select an access arrangement for a particular service type from the access types as specified in RFP Table C.2.16.2, providing the access type is available in the Agency location. Sprint will support the following Networx access arrangements:

- Circuit-Switched Access Arrangements from the serving local CO for SDPs with Presubscribed Interexchange Carriers (PICs) service for VS
- Dedicated Access Arrangements
  - Wireline Access Arrangements (WLNAA)
  - Broadband Access Arrangements (BBAA)
  - Wireless Access Arrangements (WLSAA)
  - Satellite Access Arrangements (SatAA)

4.2.1.2 Dedicated Access Arrangements

4.2.1.2.1 Wireline Access Arrangement (WLNA)

Sprint Provided Access (SPA) is an arrangement that provides a full-service, one-stop solution for access which includes consultation and provisioning of modems, multiplexers, and other hardware where applicable. With SPA, Sprint takes complete responsibility for service availability of any Sprint service that requires dedicated access service.
entrances, providing redundancy at these locations. A SPA customer is automatically placed on existing fiber rings wherever available, providing "built-in" survivability. Connections use the Sprint 100 percent digital, fiber-optic network and over local fiber facilities, where available, and from access providers connected to the Sprint network. Fiber optic based networks increases service reliability and help ensures quality of service by reducing service interruption and by eliminating noise and fade problems.

Sprint has teamed with access providers that meet our high access standards and follow industry best practices. Thus, in some POP serving areas, an AAV may serve as the Sprint primary provider to supply the local access infrastructure in SPA arrangements. This is a departure from using LECs exclusively and has tremendous benefits in creating survivability and redundancy for Agency access requirements. Many AAVs have local fiber ring service, allowing Sprint to maximize its fiber-optic network by extending fiber directly to an Agency location. Using an AAV and a LEC to achieve vendor diversity (where available) creates a true diverse access offering to an Agency location.

Sprint's processes and practices enable continuity of service, network reliability, and survivability.
Connectivity and access to Agency specified locations is based on what is required at the specific locations. Should an Agency require a non-standard access method at a specified Agency location, Sprint will work with the Agency to evaluate and deliver the required access arrangement.

Wireline Access Arrangement Features

Sprint supports the Wireline Access Arrangement standards, connectivity, technical capabilities, features, and interfaces as outlined in RFP.
Access Route or Path Diversity

Sprint engineers a diverse capability for access circuits upon request where commercially available. This option may be appropriate when the critical nature of the Federal Agency's mission requires a guarantee of survivability above that possible from a single route. Sprint supplies two or more physically separated routes for access circuits and works with access diversity suppliers to achieve the diversity as shown in Figure 4.2.1-1. Where feasible, these diverse routes do not share common telecommunication facilities or offices. Diversity between routes is assured within the Sprint network.

Where uncompromised (i.e., adhering to the minimum separation requirements) diversity is not available, Sprint exerts best efforts to propose an acceptable arrangement and provides documentation describing the compromise. Each pair of circuits, which are diverse from each other, Figure 4.2.1-1. Achieving Diversity Sprint works with multiple vendors to provide the highest quality access to Agency locations.
Access Route or Path Avoidance

Between an SDP and its associated connecting POP, Sprint will supply the capability for a customer to define a geographic location or route to avoid. Where avoidance is not possible, Sprint will provide documentation describing the reasons avoidance is not possible, and will work with the Agency to find an acceptable solution. Sprint makes an effort to propose an acceptable arrangement along with documentation describing the reasons for the unavailability.

Figure 4.2.1-2 shows how Sprint works with Agencies to provide alternative access arrangements that address route or path avoidance, thus creating dual access routes and higher reliability for an Agency location.
壮志凌云

Interfaces

Sprint meets the requirements for interfaces in accordance with RFP Section C.2.16.2.1.3.1.

4.2.1.2.2 Broadband Access Arrangement (BBAA)

Access to Agency specified locations is based on services required at the specific locations. Should an Agency require a non-standard access method at a specified Agency location, Sprint will work with the Agency to evaluate and deliver the required access arrangement. Sprint supports the
requirements for BBAA connectivity, standards, technical capabilities, and interfaces where applicable and outlined in the RFP.

4.2.1.2.2.1 DSL Services

- ADSL is provided over a dedicated loop or a line shared loop. Line shared ADSL service rides over the same copper pair as voice service and thus requires the end user to have voice service, i.e., Plain Old Telephone Service (POTS). Either a Network Interface Device (NID) splitter or inline low pass filters are used to ensure the data traffic does not interfere with the voice quality. Dedicated loop ADSL service rides over a copper pair that is dedicated solely to data services (i.e., no ILEC voice is required).

- SDSL and IDSL service are dedicated loop services. The SDSL service rides over its own copper pair dedicated solely to data.

- Dedicated loop DSL services may be used to provide voice over Internet protocol (VOIP) but does not have integrated voice as part of the service.
As mentioned earlier, Sprint complies with the standards for ADSL and SDSL listed above. Sprint will comply with new versions, amendments, and modifications to the above standards when approved and applicable.

4.2.1.2.2 NMLI Services

4.2.1.2.2.3 Cable Access Services

Cable High-speed Services provide a multitude of services with varied upload and download speeds as well as symmetrical speeds in some markets. The industry overall supports speeds from 128Kbps to 384Kbps symmetrical speeds and upload speeds from 256Kbps to 384Kbps and download speeds from 768Kbps to 30Mbps (including 10Mbps) under Data Over Cable Service Interface Specification (DOCSIS) 1.0 and 1.1, and 2.0, where deployed. This is the specification for transmission of data over a cable network approved by the International Telecommunication Union (ITU) as an international standard. CableLabs and a consortium of North American multi-system cable operators developed DOCSIS. This varies by market and Cable Access carrier nationwide.

For customer interfaces to the delivered services, Sprint will offer the interface standards available from the cable industry today. This includes 10baseT, 100base TX and USB 2.0. As actual cable modem hardware
evolves, Sprint will be prepared to offer more capable customer interfaces as part of our service delivery.

4.2.1.2.4 FTTP Services

4.2.1.2.3 Wireless Access Arrangement (WLSAA)

Many wireless access methods are evolving as technology focuses on the ability for wireless to carry data in a secure environment. Connectivity requirements, technical capabilities, and standards will continue to evolve in meeting the requirements of Government Agencies. Sprint will comply with the standards for wireless access described in RFP Section C.2.16.2.3.1.2 to be made available commercially in the future.
Our announcement is further evidence of Sprint’s broadband mobility leadership, and we expect to establish a first-to-market next generation network advantage for Federal Agencies available through Networx. We will have a unique broadband capability for meeting the growing access and mobile Internet needs for computing, portable multimedia, interactive and other electronic devices. These efforts allow Federal Agency customers to experience a nationwide mobile data network designed for faster speeds, lower costs and greater convenience and enhanced multimedia quality.

**CPCS (Cellular Personal Communication Services)**

Sprint offers CPCS services including the largest all digital, all PCS nationwide network built from the ground up reaching more than 230 million people. Leveraging our CDMA and iDEN technology platforms, Agencies voice and data communications traverse a single, integrated voice and data networks.
For several years, Sprint has been involved in comprehensive investigation and internal testing of various wireless technologies. Sprint is also active in multiple standards bodies and groups working to define next-generation wireless broadband protocols for Government and commercial applications.

Access to Agency specified locations is based on services required at the specific locations. Should an Agency require a non-standard access method at a specified location, Sprint will work with the Agency to evaluate and deliver the required access arrangement.

4.2.1.2.4 Satellite Access Arrangement (SatAA)

Sprint has teamed with Hughes Network Systems (HNS) Network Systems to provide Satellite Access Arrangement (SatAA) for connectivity between Government Agency locations and the Sprint network. This will provide Agencies with a robust, reliable and secure broadband network infrastructure that can provide high performance connectivity where Agency locations may not be connected by traditional infrastructure. The use of standard earth terminals and VSAT (Very Small Aperture Terminal) devices allows remote locations to communicate with server hosts at an Agency data center, thus allowing connectivity to applications on the network.

The equipment/elements required for this connectivity consist of four basic elements:

1. Terminals
2. Satellite Space Segment
3. Satellite NOC

HNS provides some of the most advanced satellite technology available today for application to Networx.
4. Terrestrial Backhaul.

The satellite network is designed to exceed 99.5% availability on an annual average basis. Each site will be equipped with antennas and Radio Frequency (RF) equipment sized to meet or exceed that target on a case-by-case basis. Every satellite will have a slightly different footprint based on its Geostationary Orbit.

In some of the outlaying locations in certain harsh climate areas of the United States, we recommend that active de-icing be part of the CPE in these areas in the service to provide availability for Agency access. Sprint, together with HNS, will work closely with an Agency to determine the locations and recommend the right solution.

HNS, as one of the largest providers of VSAT services in the U.S., is recognized as one of the industry leaders in innovation and leading edge technology as well as providing high quality service and reliability. Combining the experience of Sprint and HNS with technology, quality, reliability, and high availability, any agency will have the assurance of two of the best carriers coming together to provide the highest service quality and reliability to any Agency location that requires satellite services.

The Sprint and HNS combined solution for SatAA services adhere to all standards, connectivity, technical capabilities, and applicable interfaces requirements as identified by the GSA.
4.2.2 Arrangements with Other Service Providers (L.34.1.3.2) (b))

Describe the arrangements that the offeror has with other service providers for carrying and exchanging traffic, particularly with Tier-1 peering partners. Describe the impacts on quality and reliability of such arrangements.

Peering relationships with other Tier 1 ISPs are an integral part of the public Internet and are treated with significant importance. Sprint privately peers with leading Tier 1 and Tier 2 ISPs throughout the global Internet market. Additionally, Sprint maintains relationships with service providers who have connectivity to the Sprint network in either a Sprint, as a global provider of multiple services and a Tier 1 ISP, has extensive arrangements with other service providers for carrying and exchanging traffic—each negotiated with quality and reliability considerations.

4.2.2.1 Peering Relationships

Sprint also uses partners in certain cases to expand our global footprint, as explained in Section 4.4, or to enable our customers to “roam” onto different networks.
transit or non-transit relationship. Our strategy emphasizes private peering arrangements with like-sized networks. Although Sprint has de-emphasized public peering, we continue to operate and manage the Pennsauken Network Access Point (NAP) and maintain public peering relationships around the world. As shown in Table 4.2.2-1, our global IP backbone, SprintLink, natively extends to Asia, Europe, and South America using a single Autonomous System (AS) number 1239 for virtually the entire network, and has established peering relationships around the world. This technique delivers better performance to our customers, improves the overall health of the Internet, and provides Federal Agencies with global reach. Additionally, the emphasis on private peering relationships allows Sprint to implement significant engineering advantages and newer technology more quickly than that available at the legacy public peering locations. As another step to ensure the quality and reliability of our peering relationships, Sprint has established requirements for private peering with SprintLink. Included are provisions such as the use of Border Gateway Protocol (BGP) session MD5 password authentication, as well as prefix-limits, to prevent routing misconfigurations from injecting instability into SprintLink via a peering point.

<table>
<thead>
<tr>
<th>Domestic</th>
<th>Non-Domestic</th>
</tr>
</thead>
<tbody>
<tr>
<td>United States</td>
<td>Europe</td>
</tr>
<tr>
<td>Ashburn, VA</td>
<td>Amsterdam, The Netherlands</td>
</tr>
<tr>
<td>Philadelphia, PA</td>
<td>Berlin, Germany</td>
</tr>
<tr>
<td>Anaheim, CA</td>
<td>London, England</td>
</tr>
<tr>
<td>Pittsburgh, PA</td>
<td>Milan, Italy</td>
</tr>
<tr>
<td>Atlanta, GA</td>
<td>Glasgow, Scotland</td>
</tr>
<tr>
<td>Boston, MA</td>
<td>Paris, France</td>
</tr>
<tr>
<td>Cheyenne, WY</td>
<td>Copenhagen, Denmark</td>
</tr>
<tr>
<td>Chicago, IL</td>
<td>Düsseldorf, Germany</td>
</tr>
<tr>
<td>Ft. Worth, TX</td>
<td>Frankfurt, Germany</td>
</tr>
<tr>
<td>Kansas City, MO</td>
<td>Hamburg, Germany</td>
</tr>
<tr>
<td>Sacramento, CA</td>
<td>Hamburg, Germany</td>
</tr>
<tr>
<td>St. Louis, MO</td>
<td>Düsseldorf, Germany</td>
</tr>
</tbody>
</table>

Table 4.2.2-1. SprintLink Global Peering Locations
4.2.2.2 Affiliate Relationships

Sprint originally used several affiliates, using both iDEN and CDMA technologies, to transparently provide improved coverage to our customers.

Sprint Affiliates have constructed all-digital, CDMA wireless networks, the majority of which operate on the licenses owned by Sprint. Nextel Partners also provides iDEN services in mid-sized and smaller markets throughout the United States. Each Sprint Affiliate operates and markets its network as services of Sprint and must adhere to the specifications required to operate a portion of the Sprint network. Sprint is therefore able to maintain quality and reliability while allowing affiliate areas to leverage support, marketing, and distribution organizations. Each Sprint Affiliate benefits from our relationship with key infrastructure and phone manufacturers and national retail distribution partners.
4.2.2.3  Roaming Agreements

4.2.2.3.1 Domestic Roaming Agreements

Sprint has roaming agreements that allow for the making and receiving of calls while off the Sprint Nationwide PCS Network with Sprint PCS roaming-capable phones (digital dual-band, dual-band or dual-band/tri-mode) in nearly every area of the United States where wireless service is available. This service is available as well in parts of Canada, Mexico, and the U.S. areas of Guam, Puerto Rico, and the U.S. Virgin Islands.

4.2.2.3.2 Non-domestic Roaming Agreements

Sprint has roaming agreements in over 150 foreign countries for wireless voice services using CDMA, GSM, W-CDMA, and iDEN networks and devices. Additional details about these locations are contained in Section 4.4.1, Service Arrangements for Non-Domestic Services.
4.2.3 Testing and Verifying Services (L.34.1.3.2 (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.

Sprint is aligned with the objectives of the Federal Enterprise Architecture (FEA) including those that encourage a results-focused Government that maximizes IT investments to better achieve mission outcomes, fulfill legislative mandates, and become more “citizen-focused”. FEA business drivers related to verification of individual services provided under the Networx contract with Sprint include an emphasis on accountability and measurement of performance objectives; and the need for secure, high quality, meaningful data to assess cross-Governmental initiatives and their impact on current state of operations. Indeed, “performance-based contracts” is an objective of the Networx Enterprise procurement. Further evidence of Sprint’s alignment with FEA objectives are results of the Sprint internal transformation. After executing a focused, multi-year corporate restructuring effort, Sprint has redefined our organization to focus on customer-centric solutions consistent with “results-oriented” FEA objectives.

Networx Services Verification Test Plan

[Blacked out text]

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

Volume 1 Technical—4, Networx Architecture

Page 40

March 5, 2007
The Networx Services Verification Test Plan will also describe the change procedures for adding service-specific test plan attachments (J.9 ID 34605). At a minimum, the plan will include:

1. How Sprint proposes to notify the GSA PMO of any changes to its Networx Verification Test Plan, such as the addition of a service-specific test plan.

2. How Sprint plans to request and receive approval from GSA. Service-specific test plans will be provided to the PMO as an attachment to the Networx Services Verification Test Plan no later than 15 calendar days after Sprint issues the Service Order Confirmation for the initial order of the service under this contract. This will allow Sprint to defer delivery of service-specific test plans until the services are actually ordered and to use a phased approach.

Sprint will detail within the Networx Services Verification Test Plan how we propose to perform verification testing on any awarded service at the time of initial service delivery to an Agency. Sprint will notify the Agency of facility access requirements for verification testing, and the Agency will provide Sprint access to conduct verification testing. (J.9 ID 34608)

Sprint understands that GSA reserves the right to reject or request modifications to the Networx Services Verification Test Plan within 15 business days after receiving the initial plan and within 15 business days after receiving a request to change the plan. Sprint will provide updates to the Networx Services Verification Test Plan within five business days of receipt of GSA's comments. Sprint understands that GSA reserves the right to reject or request modifications to the plan within 15 business days after receipt of the updated plan. Sprint will continue to update the plan until a final plan can be mutually agreed upon by Sprint and the GSA PMO.
**Ongoing Performance Verification**

Networx performance objectives are measurable attributes that may be used by the GSA as indicators of Sprint’s contract performance. There is a direct correlation between these performance objectives and the KPI/AQL compliance. Because performance objectives for Networx are defined as either “incident based” or “aggregate based,” Sprint’s testing procedures will vary based on the rate of metric incidence.
As a solutions provider with a long history of partnership with the GSA, Sprint is already very familiar with the types of performance metrics sought by the GSA to measure contractor performance.
4.2.4 Ensuring Quality of Time-Sensitive Traffic (L.34.1.3.2 (d))

Describe the approach to ensure the quality of time-sensitive traffic (e.g., voice quality, video quality, video lip-synch) under different traffic patterns and load conditions on the offeror’s network.

As shown in Figure 4.2.4-1, Sprint does not rely on a single technology or control mechanism, but rather employs a variety of engineering principles, processes, and technologies for a comprehensive strategy for network engineering and protecting time-sensitive traffic.
levels and the resulting survivability and performance required by Federal
Agencies. Sprint designs its networks to achieve minimal latency and routinely
analyzes the design for efficiency. The design of our core IP architecture
focuses on fast, high-efficiency packet switching as consistent with industry
best practices for network design. The entire network is streamlined with
native IP over a diverse, Dense Wave Division Multiplexing (DWDM) optical
architecture resulting in minimal overhead. Our IP networks are based on a
flat network design, with logical meshing over diverse physical paths,
reducing latency from hierarchal network hops. We reduce overhead by

Figure 4.2.4-1. Sprint Congestion and Flow Control

The Sprint approach to congestion and flow control includes specific
technologies, network design requirements, and best practices engineering
processes, and has been recognized in industry for its quality
pushing access/distribution features and policy enforcement to the edge. The architecture is a native IP over DWDM optical design. These attributes provide a high-performance network optimized for delivering all traffic, especially time-sensitive traffic—key concern of the Networx Enterprise RFP—minimal latency and jitter. Our approach also provides the ideal platform for services such as frame relay, Asynchronous Transfer Mode (ATM), packetized private line, VPNs, VoIP, and mobile IP data. This ensures that the government receives the same benefit with other services procured under Networx Enterprise contract as they do with the IP-Based services.

By contrast, some of our competitors did not have the luxury of building greenfield architecture. Sometimes, resulting from merger and acquisition activity, they may try to ensure the quality of time-sensitive traffic by employing complex traffic engineering schemes. These schemes, often overlaid on a Multi Protocol Label Switching (MPLS) core network, itself overlaid on a variety of underlying transports, are designed to support QoS objectives over multiple networks. Instead of building a clean native IP architecture, this approach often requires a more complex control plane with more expensive network management equipment and is less tolerant to the variable traffic patterns and load conditions to which GSA has inquired.

Finally, Sprint routinely analyzes the network for optimization opportunities and grooms SONET-protected connections to LECs and AAVs for efficiency. In our experience, the greatest source of congestion facing our customers is found on the local port. Customers are often unable to size their local access connection with the same congestion avoidance philosophy that we employ in our core architecture, lacking the size and scale of a major service provider. With services such as Sprint IP Class of Service (IP CoS), we empower Federal Agencies with the flexibility to customize the prioritization...
IP CoS leverages standards-based Differentiated Services (DiffServ) technology to map traffic into priority classes-based Agency requirements. This allows an Agency to respond to not only different traffic patterns and load conditions on the offeror's network, but also on their network as well, as they have better visibility into more subjective parameters such as voice quality, video quality, and video lip-synch. IP CoS exceeds Government requirements, and a more detailed description appears in Section 5.2.3.3.2.

Finally, the Sprint architecture is consistent. We rely on years of designing and building wholly-owned networks, and do not require complex traffic management to guarantee Federal Agencies consistent handling of congestion across historically different networks. Our global platform for non-domestic services, SprintLink, is consistent beyond our borders and even uses the same Autonomous System (AS) number for virtually the entire network. Sprint is leading the industry in a consistent, converged IP approach to wireless wireline integration efforts, and will continue without becoming an operating unit of another company.

Our approach, outlined above, not only enables Sprint to plan for different network load conditions on a broader, macro-level, but also provides the Government with the ability to fine-tune their traffic patterns at a micro-level in response to changing Agency requirements. As evidence of our ability to ensure the quality of time-sensitive traffic under different traffic patterns and load conditions, Sprint is able to offer aggressive guarantees on packet loss, latency, and jitter metrics. We also provide independent evidence of our support for time-sensitive traffic: SprintLink was one of the first networks to achieve the Cisco Multiservice VPN designation, attesting to our ability to carry time-sensitive traffic across its security-enabled, converged IP network.
4.3 APPROACH TO NETWORX ARCHITECTURE, CONVERGENCE, INTEROPERABILITY, AND EVOLUTION (L.34.1.3.3)

4.3.1 Providing Integrated Access (L.34.1.3.3 (a))

Describe the approach for providing integrated access to locations that support customer applications with different performance requirements (e.g., voice, data, and video).

Our approach to Networx Architecture, Convergence, Interoperability, and Evolution accomplishes the following for Federal Agencies:

- Provides integrated access methods that support Agency applications with different performance requirements
- Leverages Sprint’s industry-leading architecture, which builds upon years of experience running wireless and wireline networks
- Ensures interoperability with future services by relying upon proven standards
- Provides service quality through an access agnostic, converged IP core designed for efficiency, reliability, and data delivery
example would be an Agency location that currently has separate access lines to support voice and data services to a location. Sprint provides a channelized T1 to the location that allows the 24 channels on the T1 to be separated for voice and data requirements. This allows for incoming voice and data services to use the same access connection to the network. Figure 4.3.1-1 illustrates this example.

Channelized Access provides dedicated bandwidth for individual applications. As services migrate to IP, greater efficiencies are possible over integrated IP access lines. Sprint IP Class of Service permits the allocation of bandwidth for different priority traffic. This service permits the support of customer traffic with different performance requirements such as voice, video, and data traffic to be supported with a single access line. Sprint IP Class of Service is detailed in Section 5.2.3.3.2. Figure 4.3.1-2 illustrates the use of IP Class of Service to support different applications on a common integrated IP access line. Additionally network and CPE based VPN services can be utilized to permit the economical use of a common integrated IP access line for multiple Agencies at a common location, keeping their traffic logically separate. Use of VPNs combined with Class of Service, provide powerful tools to make...
4.3.2 Benefits of Overall Network Architecture (L.34.1.3.3 (b))

Describe the overall network architecture and explain the benefits of this implementation.

Our architecture is in place today to deliver immediate benefits to the Government.
Architecture details specific to the service delivery of each Networx Service Type are contained in their respective Sections of the Technical Volume.

The wireline timeline provided in Figure 4.3.2-1 reflects Sprint's continued focus on expanding the IP Packet Architecture, facilitating smooth customer migration from legacy services, and offering advanced seamless, converged applications.

Figure 4.3.2-1. Wireline Timeline.

Sprint's IP Packet Architecture is fully deployed and in place today delivering enhanced performance, greater simplicity, better value, and a solid platform for converged wireline/wireless applications.

The wireless timeline provided in Figure 4.3.2-2 highlights Sprint's continued focus on expanding seamless wireless coverage, enabling interoperable communications across technologies, and offering advanced wireless voice and data applications with a combination of 3G and 4G broadband technologies.
4.3.2.1 Sprint Target State Architecture

The overarching Sprint architecture for Sprint infrastructure evolution is referred to as the Target State Architecture.

The Sprint network enables new products and services that appear seamless to the customer while reducing operational complexity and capital expenditures. Our evolution activity is ongoing. This activity affects each technology lane in a manner that is consistent with the drivers and architectural principles of the Sprint network evolution mentioned throughout this document.
Architecture. This target state is an optimized, all encompassing view across all layers, acknowledging the end-to-end delivery requirements of all services and applications. Functional layers describe the Target State Architecture. These layers are Access, Transport, Network, Signaling and Control, Operational Support Systems, Devices and Customer Premise Equipment (CPE), and Services & Applications.

Figure 4.3.2-3. Sprint Target State Architecture

Based on principles aligned with the Networx RFP and FEA objectives, the Sprint vision for a converged, next-generation Target State Architecture approach will yield many benefits to Federal Agencies.
4.3.2.2 Layered Architecture

The following sections describe the network in a logical manner based on the layered model illustrated in Figure 4.3.2-4.

Figure 4.3.2-4. The Sprint Layered Architecture Approach

Sprint has a methodical, layered approach to designing its network architecture. Our approach benefits Federal Agencies by providing a scalable, flexible, standards-based platform for delivering Networx service types.
4.3.2.2.1 Services and Applications

The vision for Sprint Services and Applications is an open, extensible, standards-based architecture that enables us to rapidly and efficiently deploy new services, expand service functionality, support product differentiation, and provide an improved end user experience. The vision provides for migration toward open, industry-standard technologies and architectures under development by: Open Mobile Alliance (OMA), 3rd Generation Partnership Project 2 (3GPP2), Internet Engineering Task Force (IETF), International Telecommunications Union (ITU), and Parlay Group Open Services Architecture (OSA). The pace of services and applications evolution is tempered by the fundamental evolution of computing components and software paradigms.

Services and Applications goals include achieving cost efficiency, facilitating interoperability, providing integrated services, and enabling/enhancing third party development. As shown in Table 4.3.2-1, our vision covers across a multitude of services and applications.

<table>
<thead>
<tr>
<th>Services and Applications</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Voicemail</td>
</tr>
<tr>
<td>Push to Talk over Cellular</td>
</tr>
<tr>
<td>Wireless Application Gateway</td>
</tr>
<tr>
<td>IP Centrex</td>
</tr>
<tr>
<td>Personal Information Management (PIM)</td>
</tr>
<tr>
<td>Multi-modality</td>
</tr>
<tr>
<td>Cable Telephony Integration</td>
</tr>
<tr>
<td>Device Management</td>
</tr>
<tr>
<td>Location based Services</td>
</tr>
<tr>
<td>Data Messaging</td>
</tr>
<tr>
<td>VoIP Security</td>
</tr>
<tr>
<td>Collaborative Services</td>
</tr>
<tr>
<td>Email Security and Policy Enforcement</td>
</tr>
<tr>
<td>Multimedia Messaging</td>
</tr>
<tr>
<td>Home Subscriber Service (HSS)</td>
</tr>
<tr>
<td>SIP-based Collaboration Client</td>
</tr>
<tr>
<td>Parlay/OSA</td>
</tr>
<tr>
<td>Public Key Infrastructure and Certificate Services</td>
</tr>
<tr>
<td>SIP-based Application Server</td>
</tr>
<tr>
<td>VoIP Security</td>
</tr>
<tr>
<td>IP Contact Centers</td>
</tr>
</tbody>
</table>
4.3.2.2.2 Signaling and Control

As Sprint evolves our network architecture toward integrated all-IP networks, we address multiple signaling and control functions the network infrastructure requires to facilitate IP-enablement of services and to meet objectives as described next.

IMS, a standard of 3GPP2, is the basis of the target Signaling and Control Architecture. IMS enables interoperation of wireless and wireline networks in a standardized manner and allows Public Land Mobile Network operators to offer subscribers IP multimedia services in an access-agnostic environment. IMS facilitates the convergence of, and access to, voice, video, messaging, data, and Internet services across wireline and wireless networks.

Sprint has a comprehensive approach to addressing signaling and control functions, focusing on the architecture holistically rather than a "by product" approach. The Sprint signaling and control architecture objectives are to:

- Standardize signaling and control functions in the network to better support IP multimedia services
- Replace legacy signaling protocols with IP network equivalents to facilitate the transition from circuit-switched voice to VoIP
- Implement a unified mobility management architecture to enable seamless intra and inter technology handoffs
- Deploy a next-generation Signaling and Control architecture to enable wireless/wireline convergence
- Implement a new optical control plane to improve network adaptability.

The long-term Sprint VoIP architecture is a single, converged core VoIP platform. VoIP rationale centers on superior economic benefits, manageability, and inter-carrier connection cost reduction. Targeted VoIP signaling architecture is Session Initiation Protocol (SIP)-based with evolution...
requirements to support existing signaling and control protocols. Packet switching uses new signaling and control protocols. These new signaling and control protocols enable the implementation of existing and emerging applications. Inter-provider connection with Sprint is targeted via Network-to-Network Interconnection (NNI) architecture. Some NNI functions may exist in a distributed model. Distributed functions include Security and Denial of Service (DoS) protection, Network Address Translation (NAT), Topology Hiding, and Policy enforcement. Firewalls are logical locations to include these distributed functions. Centralized functions include Call Admission Control (CAC), voice-switching functionality, signaling interoperability, and proxy functions. Centralized functions should be optimally located within the network, most likely at an existing switching center.

The target state signaling and control network includes data transport peering to the Cable industry. The architecture supports integrations such as the Cable-Wi-Fi (Cable's Packet Cable Multi-Media convergence with 802.11/Cellular Roaming) functionality. The Sprint Target State Architecture supports seamless hand-offs for mobility.

Moving Signaling & Control discussion into the Transport Layer, the target state IP Optical Control Plane provides faster and easier provisioning via automatic connection establishment and teardown. Key control plane features include support for permanent and switched connections; support for call detail records and billing information, and, support for protection and restoration. Facilitating convergence is a natural outcome of the integrated target state network.

4.3.2.2.3 Switching and Routing

In the target state network, voice traffic routes over an IP network rather than switching through wireline, wireless, or long distance networks.
Sprint public IP network continues to evolve for greater efficiency, reliability, and security. Sprint evolves frame relay and ATM services onto the IP platforms. Sprint uses Layer Two Tunneling Protocol Version 3 (L2TPv3) for the encapsulation of frame relay and ATM.

We planned our deployment of a fully IP-enabled VoIP voice network carefully to ensure that we offer VoIP services in a scalable, secure, and seamless manner to the subscriber. Real-time traffic, such as voice, is very sensitive to delays, which can reduce voice quality and affect customer perception. The network infrastructure must be able to support the stringent delivery requirements of IP telephony in an efficient and cost-effective manner. To achieve cost savings from network convergence, voice networks need to evolve to an IP-enabled core network, which is capable of supporting the quality of service requirements and service level agreements (SLAs) including delay, budget, jitter, and packet loss.

The core network continues to use standard IP protocols, BGP and IS-IS for topology updates. Layer 2 transport uses L2TPv3 for the encapsulation of FR and ATM.

4.3.2.2.4 Transport

The target network architecture for transport is an optical network with a logical mesh structure offering enhanced network survivability. Key features include the ability to offer additional restoration options. The Target State Architecture is capable of provisioning traffic directly between nodes, grooming traffic at the edge at VT1.5 levels, and supporting efficient transport of data protocols such as Ethernet and Storage Area Networks.

Optical Cross Connect systems, either photonic or electrical matrix-based, are deployed at large transport hubs and provide SONET interfaces at ring-to-ring transfer points. DWDM or Coarse Wavelength Division Multiplexing
Sprint’s target access network strategy applies equally to both business and government customers. In the government and public sector segments, Fiber-to-the-Node (FTTN), Fiber-to-the-Premises (FTTP), Passive Optical Networks (PON), and cable facilities will serve large and medium government agency locations (i.e., headquarters, regional offices) while small government agency locations (i.e., field offices) will be served by DSL, PON, TDM, or Wireless technologies. Additionally, wireline networks will integrate with wireless networks to serve mobile, temporary, or rapid deployment locations.

The combination of these technologies to serve the full range of small/mobile locations up to large/fixed locations enables flexible solutions optimizing performance and economics.

4.3.2.2.5 Access

Sprint expects that initial deployment of wavelength-based optical access networks will happen within five years, and the standards-based optical control plane will extend into those new access networks. Sprint’s standards-based optical control plane will provide enhanced network survivability, better traffic provisioning, and improved protocol support resulting in a reliable, fault-tolerant, and efficient/high performance core network supporting our converged product portfolios.

These same survivability, provisioning, and protocol support benefits may be extended from the core transport network architecture to the access architecture as technology continues to evolve, mature, and extend into the access networks. Sprint expects and is planning for this extension of core features into the access network over the next five years.
(Evolution Data-Optimized), improving coverage, and moving to an all IP packet-based infrastructure. An end-to-end, all IP, packet network requires packet-based network processing elements in the network. Additionally, Sprint is researching the optimal use of its Broadband Radio Service (BRS) spectrum.

Sprint began deploying 1xEVDO Revision 0 in top markets. Sprint now upgrades its network with 1xEVDO Revision A, which supports a peak data rate over 3 Mbps in the downlink and 1.8 Mbps in the uplink. 1x EVDO Revision A is backward compatible to 1x EVDO Revision 0 making the migration step more feasible and economical. 1x EVDO Revision A supports VoIP, broadcast/multicast service, Quality of Service, and high performance Push-to-Talk (PTT).

In addition to CDMA technology, Sprint is engaged in analyzing solutions for its BRS spectrum. BRS development centers on emerging IEEE 802.16 and 802.20 standards. IEEE 802.16e is an amendment to the IEEE 802.16-2004 standard, for both fixed and mobile operation in licensed bands below 6 GHz. Sprint is evaluating the potential use of this standard for access in its BRS spectrum and leveraging the involvement of key industry players such as Intel. Sprint is influencing the development of a true global standard through involvement with the Broadband Wireless Forum (BWF) and WiMAX.

BRS could potentially use the IEEE 802.20 standard, also referred to as Mobile Broadband Wireless Access (MBWA). This technology supports mobile broadband wireless access systems operating in licensed bands below 3.5 GHz and is optimized for IP-data transport at vehicular speeds up to 250 km/hr. IEEE 802.20 is a new standard, unlike IEEE 802.16e, which is an amendment to IEEE 802.16. To date, the standards development group has shown slow progress relative to IEEE 802.16e (a work in progress).
4.3.2.6 Devices and Customer Premise Equipment (CPE)

Four main drivers are influencing the evolution of devices and CPE: 1) device component evolution, 2) network evolution, 3) application environments, and 4) customer satisfaction. These devices adhere to Moore’s Law, i.e., the numbers of transistors per square inch on integrated circuits have doubled every year since the invention of the integrated circuit.

4.3.2.7 Sprint Operational Support Systems (OSS)

Increasing OSS technology standardization is essential to creating an environment that enables greater speed to market and ease of integration with collaborators and integrators.
4.3.3 Supporting Technological Evolution 
(L.34.1.3.3 (c))

Describe how the network architecture supports technological evolution, and convergence; and ensures interoperability with present and future commercial networks.

Sprint supports architecture evolution and inclusion of emerging technologies by following a rigorous, controlled, seven step Technology Development Process.

1. Ideation – Initial assessment stage to formulate, screen, prioritize, validate, and size potential emerging technologies for adoption in accordance with the Sprint Network Evolution Plans and Technical Evolution Plans.

2. Concept – Documentation and initial estimation stage to further define the business concept/project with associated Initial Design Concept Documentation and Cost Estimations.

3. Plan/Analyze – Working stage to develop functional requirements, operational requirements, systems requirements, and overall technical solution with risks, gaps, and overlaps between business requirements and technical capabilities.

4. Design – Working stage to design technical solutions based on business, technical, and functional requirements including creation of...
5. Lab Build/Test – Build and test stage to develop installation specifications, complete test plans, deploy hardware/software in lab environment, complete comprehensive lab testing, resolve lab testing defects/issues, and publish complete lab test results and reports.

6. Field Integration Test (FIT) Build/Test – Build and test stage to deploy hardware/software in field environment, complete comprehensive field testing, resolve field testing defects/issues, and publish complete field test results, reports, and readiness checklists.

7. Rollout – Build and deploy stage to rollout hardware/software in full-scale production network environment, complete deployment acceptance testing, resolve deployment defects/issues, and publish Network/Product Ready notice indicating closure of project.

This process combined with Sprint's focus on leveraging open, standards-based technologies and a layered architectural model result in controlled, efficient, and seamless introduction of new, emerging technologies and evolutionary enhancements to the network architecture. Sprint's layered architectural model is further described in Section 4.3.2 and provides the foundation for introducing technology enhancements in a controlled, organized manner as each layer can be treated independently. Sprint's focus on compliance to industry standards and participation in standards body activities ensures a forward looking approach to requirement definition, technology evolution, and delivery of innovative high quality products and services. Sprint's Technology Development Process is further defined in Section 4.3.4 discussing the tactical testing, deployment, and integration of
network enhancements and our program for inclusion of new services to the Networx contract.

Sprint is further ahead of its competitors in wireless/wireline integration and in defining its vision for an IP core. Sprint is actively engaged in the development of industry standards and lends a strong voice to the community in setting direction and policy. Sprint participates in a number of standards bodies including the ITU, IETF, 3GPP2 and IEEE, and pursues open standards to facilitate lower expenditures and greater interoperability.

Just as the FEA Business Reference model includes the supply chain as a critical sub-function supporting Federal lines of business, Sprint too considers the role of suppliers in its plans. Sprint has focused on a select group of strategic suppliers who bring complementary strengths to the long-term relationship. As shown in Figure 4.3.3-1, we have strategic vendor partnerships that allow Sprint to drive technology development, plan for network evolution, facilitate convergence, and ensure future interoperability.
These partnerships led to many innovations brought to the Federal market.
4.3.4 Incorporating Infrastructure Enhancements and Emerging Services (L.34.1.3.3 (d))

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

Sprint has a methodical approach to incorporating infrastructure enhancements and emerging services. The FTS2000 and FTS2001 programs demonstrate our proven capabilities in introducing and managing new and enhanced services driven by Federal Agency needs as they become available. The Government drives Networx enhancements through:

- GSA/Federal Agency/Sprint involvement in the Networx Technology Council
- FTS2001 Program Management Office or Sprint lifecycle team members
- Federal Agency needs and recommendations
The Sprint Technology Research and Development (TR&D) team is responsible for researching, developing, and delivering new and emerging technologies for the nationwide network in the form of products, features, and functionality. TR&D also defines the Sprint Network Evolution Plan (NEP) that defines the overall Sprint architecture, and specific Technology Evolution Plans (TEPs) that plan the evolution of specific technologies and components of the overall network architecture. Sprint thoroughly tests technologies before implementation to verify effectiveness and mitigate risk.

We have several laboratories available to support new and emerging services. In addition, our partners also have several lab facilities available to test technologies before deployment, and to develop and verify solutions with the involvement of our Government customers.

The Technology Development Process (TDP) is an integrated development and implementation process used by the TR&D organization to introduce new technology evolution, products, or services. As shown in Figure 4.3.4-1, the TDP is a comprehensive process that guides ideas from ideation through execution. Once infrastructure enhancements and emerging services are ready for use, we work with our customers to offer the new services.

**Laboratories Supporting the Sprint Solution**

- **Sprint Technical Integration Centers (STICs):** STIC labs are one of several ways that Sprint tests new technologies.
- **Sprint Solutions Laboratory:** Provides a test and verification environment for Government and other customers.
- **Lockheed Martin Center for Innovation:** Provides an environment for developing operational concepts and solutions.
Figure 4.3.4-1. The Sprint Technology Development Process

Our detailed technology development process ensures that infrastructure enhancements and emerging services are developed, thoroughly tested, and made available to our customers. The TDP is an existing process used by Sprint to support technology evolution and emerging services. The resultant capabilities developed by the process lend themselves to services that Sprint then offers to our customers as applicable. Potential problems associated with infrastructure enhancements are largely addressed by proper planning and customer involvement. As shown above, we have several facilities available to develop and verify solutions. The Sprint Solutions Lab and the Lockheed Martin Center for Innovation specifically address delivery of the right solutions that meet Government requirements. All technology upgrades in Sprint follow a process where Sprint has been a force in creating advanced wireline and wireless capabilities and value-added mobility and managed-service solutions. We also built our SprintLink, Peerless IP and original ATM network in response to government needs.
4.3.5 Supporting and Ensuring Interoperability (L.34.1.3.3 (e))

Describe the approach to support and ensure interoperability between Internet Protocol (IP) networks and the Public Switched Telephone Network (PSTN), including the approach to map between IP and PSTN addresses.

Interoperability between IP and the PSTN is critical for any large VoIP deployment to be successful. Sprint knows that this is especially true for Federal Agencies. Therefore, IP-PSTN interoperability is critical today and will be well into the future.

The PSTN consists of two primary parts: signaling and transport.
if the call can be established. If the two end parties agree to the call, an IP packet flow is set up between the two end points using IP addresses agreed to by the end parties.

Session Initiation Protocol (SIP), an IETF standard for VoIP signaling, uses logical addresses (e.g., Governmentpartner@sprint.com) or IP addresses (e.g., 10.20.1.3), while the PSTN uses telephone numbers (e.g., 202-555-1234). The VoIP logical end address traditionally determines the called party IP address by using a DNS server. Today, PSTN to VoIP interworking between PSTN and IP end points relies on a Media Gateway Controller (MGC) for signaling and a Media Gateway (MG) for transport. As a call passes through the MG, voice connections in the form of VoIP flows and DS-0 TDM connections are converted at the Media Gateway. This occurs in conjunction with the conversion of VoIP SIP signaling to and from PSTN SS7 signaling in the MGC. IP addresses to and from PSTN numbers are typically provisioned at a given MGC.

Sprint supports interoperability with the PSTN or with Agency User-to-Network Interfaces (UNIs) using the current capabilities of our VoIP service offerings. We provide network-based media gateway solutions for VoIP access to the PSTN, Agency WANs, or Agency TDM networks. By leveraging a network-based capability, the Government will have interoperability between PSTN and IP endpoints while reducing expenditures resulting from Agency-funded technology upgrades. These gateway solutions support a variety of configurations and signaling protocols. More details on our solution appear in Section 5.2.2, Voice over IP Transport.

Sprint also provides a plan for scalable interoperability that will become a standard throughout the telecommunications industry. We plan to deploy a new DNS service called Electronic Numbering (ENUM) over the next couple of years. The primary function of ENUM is to resolve SIP end point addresses
4.3.6 Approach for IPv4-to-IPv6 Migration (L.34.1.3.3) (f))

Describe the approach for IPv4-to-IPv6 migration.

IPv6 migration is a critical issue facing Federal Agencies. OMB has recently directed that the Federal Government transition to IPv6 by June 2008, and has released additional guidance to Federal
Agency CIOs in memorandum M-05-22 released 2 August 2005. Even while the Networx procurement progresses, OMB asks Agencies to respond to OMB M-05-22 so that they may begin their IPv6 planning. For example, many of the activities listed below must be complete before the award of Networx.

**Summary of OMB M-05-22 IPv6 Guidance for Federal Agencies**
- Assign Agency planning leadership, complete inventories, and begin impact analysis by 15 September 2005
- Provide an update progress report and complete a transition plan as part of an enterprise architecture submission to OMB by February 2006
- Complete inventory and impact analysis efforts by 30 June 2006
- Complete migration of Agency backbones to native or dual-stack IPv6 by 30 June 2008

We augment our IPv6 network migration plans with 16 years of experience supporting FTS and our appreciation of the IPv6 requirements facing Federal Agencies.
The current topology is comprised of dedicated IPv6 routers using Generic Routing Encapsulation (GRE) protocol tunnels over our existing public IPv4 network, SprintLink, to connect to other IPv6 routers located within the United States and Europe.

Figure 4.3.6-1 graphically shows our current IPv6 footprint. Sprint also peers with numerous other IPv6 providers and has one of the most well-connected IPv6 networks available. We peer via BGP4+ through a combination of IPv6-over-IPv4 tunneling, and through various native IPv6 exchanges. Currently, Sprint is one of the first members present at the NY6IX in New York City.

Sprint is ready to support Federal Agencies wishing to trial IPv6 now with our IPv6 network and history of supporting the development of the protocol. Sprint is ready to support Agencies wishing to use IPv6 on a trial basis now, and continues to plan the Sprint IPv6 migration based on customer demand and the ongoing development of the protocol. The main goal of the Sprint IPv6 network today is to allow Sprint and its customers to test both vendor implementations and routing policy on the 6bone test bed. Our
support for customers connected to 6bone has grown from roughly 15 customers in 1998 to over 300 customers in mid-2004.

Sprint bases its migration strategy for IPv6 on an "edge in" philosophy, as shown in Figure 4.3.6-2. We expect that demand and emerging technologies will drive migration from IPv4 to IPv6. These may include widespread deployment of devices that increase the need address space provided by IPv6.

Sprint's phased migration strategy supports IPv6 on the edge and progress towards the core as the protocol matures. Sprint can support IPv6 trials today, and Agencies will benefit from Sprint's experience supporting the 6bone overlay network. Sprint is also reviewing the IP mobility aspects of IPv6 in the context of expected benefits to our network architecture and the deployment devices.
such as VoIP-enabled phones. Sprint is planning to first migrate to IPv6 at the edge of our network. Devices at the edge will initially function in a dual stack mode allowing IPv4 and IPv6 elements to coexist during the transition. The core of the IP network will remain IPv4 for a longer timeframe until such time that all network elements are IPv6 capable. During migration, Sprint will carry IPv6 packets across the IPv4 core using one of several available tunneling options. This may include the use of GRE tunnels as Sprint is doing today with our 6bone overlay network, manually configured tunnels, semiautomatic or fully automatic tunnel mechanisms such as 6to4.

As a Tier 1 Internet Service Provider with a history of stable IP networks, Sprint cautiously and methodically approaches network upgrades such as the IPv6 migration. To move to IPv6 prematurely would be a detriment to our customer base. Migration from the current IPv6 overlay test network to full-scale, native IPv6 implementation requires resolution of several outstanding technical issues. We continually review factors such as IPv6 protocol maturity, vendor support, and anticipated customer demand such as that driven by OMB's recent guidance. Demand for IPv6 is a key component of evaluating the business case for network migration.

To foster the ongoing development of IPv6, Sprint plays an active role in the applicable IPv6 standards bodies and working groups. Sprint is a trusted partner, familiar with the business of numerous Federal Agencies, and will work with the Agencies as they prepare for their transition. As Federal Agencies plan as per OMB guidance, we will factor anticipated IPv6 demand into our ongoing plans and migration strategies.
4.4 NON-DOMESTIC SERVICES (L.34.1.3.4)

4.4.1 Service Arrangements (L.34.1.3.4 (a))

Describe the arrangements the offeror has with foreign (non-domestic) communications carriers and service providers, including at a minimum, the performance standards associated with such arrangements.

Sprint is committed to be the single point of contact for the Government for the installation, maintenance, performance, and billing of all non-domestic service ordered by the user Agencies under the Networx contract. We will use our many years of experience and lessons learned in the international marketplace in supporting the non-domestic requirements of the Networx contract. Sprint is committed to growing non-domestic reach by expanding our global IP backbone and establishing relationships with new non-domestic providers.
Our North American expansion includes partnerships with TelMex and Rogers Telecom (formerly known as Sprint Canada) to provide cross-border solutions that offer service uniformity and integration.

Our other network partners are globally recognized, award-winning providers in both quality of service and customer satisfaction. We use our long relationship with Equant and Infonet to provide additional global reach. Sprint has bilateral agreements with more than 240 PTTs and other international service providers. Sprint establishes an agreement with a PTT or provider to offer a portfolio of services. We provide the Government a single point-of-contact that helps ease the burden of working with multiple carriers. Local Sprint staff act as the international agent for the Government in working with access providers on a daily basis and have developed strong professional relationships over the years. The local knowledge, as well as the fact that Sprint is a significant customer for local access services, simplifies the provisioning process.

**International Roaming Highlights**

- Service in over 150 countries
- Support for CDMA, iDEN, GSM and WCDMA technologies
- Multiple roaming options:
  - International roaming with an existing Sprint PCS phone provides domestic coverage and roaming throughout parts of Asia Pacific, Canada, Mexico, the Caribbean, and Central and South America with dual-band or tri-mode Sprint PCS phones
  - International roaming with iDEN: Customers with NEXTEL National Network service are able to make and receive calls in Canada, Mexico, Brazil, Bermuda, Peru, Argentina, Israel, Jordan, Singapore and the Philippines with their standard iDEN handsets
  - International Roaming with a Sprint PCS International Phone provides domestic overage and roaming in over 130 countries with a single CDMA/GSM phone
  - International Roaming with a GSM or WCDMA phone provides roaming throughout Europe and parts of Asia, South America, Africa, Australia and the Middle East via a GSM phone, or Japan with a WCDMA phone

We provide extensive roaming coverage via our international agreements, and offer such capabilities via CPCS.
Sprint applies stringent qualifications and specifications to its partners so that Federal Agencies consistently obtain superior performance with their international voice and data networks.
philosophy applies to the Los Osos and Point Arena, California cable heads supporting the Japan-U.S. cable system. All global voice calls made from the mainland United States have the inherent advantage of originating on the Sprint 100 percent digital, fiber-optic U.S. network. Sprint has converted all global trunk connections to digital facilities, as well. Analog cables, which some U.S. Global Record Carriers still use extensively, are more prone to quality problems.

As a result, Sprint experiences only 2.06 global trouble reports per 10,000 call attempts from subscribers to global switched voice services. This drops to only 1.92 trouble reports per 10,000 direct-dialed calls served over our direct facilities. The trouble-reports ratio is lower for calls routed completely over our global network transmission facilities to the foreign global gateways. Calls routed over Sprint facilities through direct connection agreements constitute more than 90 percent of the millions of global calls we handle each month. Sprint continues to pursue quality improvement measures to reduce trouble reports on calls handled through transit countries or on a resale basis. Sprint proactively and aggressively manages the quality of global traffic carried by direct, transit, and resale carriers. Answer Seizure Ratio (ASR) benchmarks exist for all destinations, with specific guidelines for the direct, transit, resale, and mobile expectations. A team of analysts actively monitors performance through daily reports and traffic data and contacts carriers to request improvements when the performance does not meet Sprint standards. Weekly performance summaries are sent to resellers to communicate the quality of their service in comparison to other Sprint traffic, thereby encouraging each carrier to improve the call quality to the highest standards.

In general, the Sprint objective for non-domestic performance standards is to provide a performance experience comparable to any domestically
4.4.2 Infrastructure Security (L.34.1.3.4) (b))

Describe the infrastructure security measures the offeror has with foreign (nondomestic) communications carriers and service providers.

Sprint understands the importance that the Government places on non-domestic security risks, and have several mechanisms and controls to enhance security. We have multiple security measures in place for non-domestic services, both with other communications carriers and within Sprint itself.

One of our infrastructure security measures for non-domestic services is the use of Sprint facilities wherever possible. We have a long history of providing global services and are routinely expanding our global IP backbone, SprintLink, to provide services both provisioned over IP as well as native IP. Our current facilities-based network has over 75 nodes in over 26 countries and continues to grow. Additional details about our IP services appear in Section 5.2.3.

As we build our global IP network, we add security measures to protect non-domestic services such as Global MPLS, VPNs, and L2TPv3 support. Providing global reach and security based on RFC4364 MPLS VPNs, GMPLS provides Federal Agencies with global reach using the same MPLS VPN technology used by Sprint for domestic services. A key component of the Sprint Global MPLS network is the Value Added Services (VAS) gateway.
The VAS gateway provides support for secure Internet access, IPSec tunnels, as well as gateways to other services and access methods. Sprint will make use of the Global MPLS VAS gateway to support many of the access features required in the Networx RFP.

Sprint has collaborated with Cisco to develop L2TPv3 technologies capable of supporting layer 2 data services such as Frame Relay, ATM, Ethernet, and private lines over our IP core networks. By providing different data services as overlays over a common IP core network, we can achieve large efficiencies in hardware, management, design, and transport. Sprint can deliver a range of data products over a common, global infrastructure using these new L2TPv3 protocols and an extremely stable, high performance IP core network.

We also have security measures in place with overseas service providers and participate in international standards bodies to improve security best practices used by carriers throughout the world. Sprint negotiates terms and conditions with each non-domestic service provider. Additionally, because of the size of the Sprint Tier I global IP backbone, many non-domestic service providers are actually Sprint customers that must adhere to Sprint acceptable use policies. As described in Section 4.4.3, we participate in global standards bodies and recently discussed security in the context of global services at a Sprint-hosted ITU meeting.

Regardless of how Sprint provides services, we have proven security mechanisms and controls for all operations to protect our infrastructure and ensure the security of services offered via Networx.
We recognize that a good security program consists not just of objectives or countermeasures, but requires an ongoing process to maintain the required security posture. A summary of Sprint security policy is included in Section 4.1.1.

4.4.3 Arrangements for Interoperability (L.34.1.3.4 (c))

Describe the arrangements for interoperability of services between domestic and non-domestic locations.

Our arrangements for the interoperability of services range from processes, to our standards-based implementation, to the fact that our wholly owned IP backbone reaches North America, Europe, South America, and Asia. Of greater benefit to Federal Agencies however is not just that Sprint has arrangements in place to provide interoperability of domestic and non domestics services, but that Sprint is a leader in developing best practices for facilitating interoperability on a global scale.

In Section 4.1.3, we explained how our active involvement with the Network Reliability and Interoperability Council (NRIC) helps to ensure that our services are consistent with Best Practices. Sprint participates in additional standards bodies that focus specifically on interoperability, security, and reliability on a global scale. As a leader in developing global standards, Sprint has several arrangements in place to support the interoperability of services between domestic and non-domestic locations.
Sprint has an established relationship with the International Telecommunications Union (ITU). Within the ITU Telecommunication Standardization Sector (ITU-T), which coordinates telecommunications standards on behalf of the ITU, Sprint is an active member of the Service and Network Operations (SNO) working group. SNO supports ITU Study Group 2, a group currently chartered through 2008 to study the operational aspects of service provisioning, networks, and performance, as well as any other operations-focused initiatives sponsored by ITU-T. Due to its longevity and its status within the United Nations, the Recommendations published by the ITU achieve a high level of international recognition and are a particularly effective means to further the cause of interoperability of domestic and non-domestic services.

Sprint is taking the leadership role in the industry to get carriers together to advance Best Practice initiatives for the nation's infrastructure. In July 2005, Sprint hosted the North American Regional SNO Conference at our World Headquarters in Overland Park, KS. The conference had representation from thirteen major telecommunications carriers and addressed several topics to further the interoperability, security, and reliability of global networks.

Figure 4.4.3-1 shows the agenda from the meeting. The biggest outcome of our meeting is that Sprint is going to use subsequent meetings to drive mutual aid initiatives that will benefit the reliability of networks around the world.
4.4.4 Extending and Developing Foreign Arrangements (L.34.1.3.4 (d))

Describe the offeror’s plans for extending these existing foreign (non-domestic) arrangements and developing new arrangements to support the delivery of services internationally.

As a full-service provider, Sprint plans to extend existing non-domestic arrangements and develop new arrangements to support international service delivery. We continue to expand service availability into countries based on customer demand for the service and local regulatory conditions.
Alliances are often required in order to service customers as a global carrier. As a cornerstone of our global strategy, Sprint will continue to build our global presence on long-standing and strong relationships with traditional carriers, as well as our new partners who share complementary strategies.

Sprint has strategically built assets within a country, on a country-by-country basis for key services available today, while building a network infrastructure, which allows for smooth migration paths into future technologies.

4.5 NATIONAL POLICY-BASED REQUIREMENTS (L.34.1.3.5)

4.5.1 Satisfying NS/EP Functional Requirements (L.34.1.3.5 (a))

Describe the offeror’s approach to satisfy each NS/EP basic functional requirement listed in Section C.5.2.2.1.1.

Today, Sprint satisfies the critical user community’s National Security/Emergency Preparedness (NS/EP) needs as a provider of the Government Emergency Telephone Service (GETS) and Wireless Priority Service (WPS). Sprint addressed both of these NS/EP services through special development efforts paid for by the NCS. Between these two services, Sprint can accommodate the 14 basic functional requirements listed in Section C.5.2.2.1.1 for voice band use.

Sprint acknowledges that standards have been approved that support some of these functional requirements for some of the indicated services and that some vendors may produce compliant hardware; however, application of non-mandatory standards and development of unique features on commercial services usually occur only after market analyses indicate a good business case to do so. It is also noteworthy that some NS/EP standards are not available for universal application. For example, the standard addressing
Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

Volume 1 Technical—4, Networx Architecture

Page 86

March 5, 2007

4.5.1.1 Enhanced Priority Treatment

Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic.
special tailored capabilities necessary to satisfy GETS functional requirements from call initiation to completion.

The Sprint voice VPN service combines the features, capabilities, and service assurance of a private dedicated network with the economies of scale, survivability, and ubiquity of a shared public network. Sprint accomplishes this by partitioning the switch software so that GETS NS/EP traffic, specifically routing and service capabilities, is completely separate from the public switched network (PSN) traffic.

To differentiate all GETS NS/EP calls throughout the network, Sprint created a VPN software partition for GETS traffic in the Sprint Northern Telecom DMS 250 network switches. This partition maintains separate definition of translation and routing requirements for the Sprint public network.

The virtual private network for GETS enables Sprint to provide special routing for GETS traffic and ensures preferential treatment across the Sprint network. The GETS VPN partition provides the following advantages in the handling of GETS NS/EP traffic:

- Separate traffic management
- Special routing and increased grade of service (trunk queuing)
- Exemption from network restrictive controls

Upon validation of a GETS authorized user, the SCP assigns the user's call to the unique partition built for the GETS service. Call routing is based on the route list associated with this partition. Signaling between switches consists of the destination number and information digits that identify the VPN partition and a facility code associated with the call.
with that call. The facility code identifies special call conditions, such as queuing requirements. The GETS VPN partition route list, available at each switch, identifies the route choices available to a call.

GETS traffic is physically routed over shared inter-machine trunks to a distant switch, maintaining its GETS identity across the network. The GETS users automatically benefit from an improved grade of service over the PSN. This is accomplished using expansive control tools such as trunk queuing and Sprint network management control capabilities and procedures where, in the event of severe network traffic congestion, protective (restrictive or blocking) controls are applied to the public switch traffic to protect the GETS NS/EP traffic transiting the Sprint network. In addition, in accordance with ANSI standard T1.631, 1993, the Sprint implementation of GETS includes High Probability of Completion (HPC) features.

**NS/EP Code Point**

For all GETS calls in which the user Personal Identification Number (PIN) has been validated, the associated ISDN User Part (ISUP) Initial Address Message (IAM) protocol supports an NS/EP Calling Party's Category (CPC). The CPC parameter is coded as an NS/EP (11100010 or #E2).

GETS on DINA provides a mechanism that allows the SCP to pass an HPC condition instruction through the Response Transaction Capabilities Application Part (TCAP) messages to the DMS-250. The HPC condition is set by messages between the SCP and SCN following PIN validation. The DMS-250 populates the CPC parameter of the IAM message terminating to ISUP or ISUP Inter-machine trunks with the NS/EP code.
IAM Priority

Sprint automatically sets the IAM priority to the NS/EP level "1" in the DMS-250 for every validated GETS call processed through the SCP. The GETS IAM priority of level "1" is used within the Sprint network and provided to the destination LEC for its appropriate use regardless of what IAM priority information or its absence is provided by the originating LEC.

Networx critical users can obtain access authorization for GETS from the National Communications System (NCS). Application requirements and procedures appear on the NCS web site: http://gets.ncs.gov.
• Priority 4: Public Services/Utilities and Public Welfare

• Priority 5: Disaster Recovery

Networx users dial *272 (Star code is reserved) plus the called number.

The priority call is moved to the top of the call queue at cell ingress for channel availability and processing priority on inter-machine trunks (IMTs) between Mobile Switching Centers (MSCs) and the Inter-Exchange Carrier (IXC) network (if required). End to end priority calling is available by dialing *272-NCS-GETS and following the GETS procedures for authorization and call processing.

Toward the end of December 2004, in response to an RFP from CSC, the Integration Contractor for the NCS, Sprint submitted a proposal for WPS on the Sprint CDMA based network. Subsequently, Sprint wireless hardware vendors started development efforts for a service offering expected during CY2006 or CY2007 dependent upon vendor progress. While WPS on iDEN is available in 48 of 50 states, the addition of WPS on our CDMA network will significantly expand service coverage to many additional locations reached by Sprint PCS.

As indicated in the introduction to this section, priority on current Networx Commercial-Off-The-Shelf (COTS) offerings described in RFP Section C.2 is limited to intrinsic capabilities available to all Networx users. Voice VPN services, for example, are only available to Networx users and provide a degree of additional priority over POTS users, limiting the user community to authorized Networx callers.

Some level of priority on IP data services is achieved through Sprint CoS offerings. In addition, Sprint Peerless IP services include a true private network that shares no physical interfaces with other provider’s networks or with the World Wide Web. Consequently, Sprint maintains total visibility and control over the network and can react quickly...
4.5.1.2 Secure Networks

Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.

Consistent with best commercial practices, Sprint has taken every possible measure to protect physical assets and system resources from any threat that might affect the reliability/availability of Sprint network services to our customers. These measures extend to our customer services and address threats from both within and external to Sprint.

Sprint also developed a uniquely secure data service called Peerless IP (PIP). PIP is an Internet protocol service developed for our Government
4.5.1.3 Non-Traceability

Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).

4.5.1.4 Restorability

Should a service disruption occur, Sprint can restore or repair voice and data services to required service levels on a priority basis.

The FCC established the TSP System in November 1988 when it issued a Report and Order (FCC 88-341) as an amendment to Part 64 of the

The TSP System identifies all telecommunications services that the Federal Government finds necessary for National Security or Emergency Preparedness (NS/EP) services. The TSP System applies to all domestic NS/EP telecommunications services and to the domestic part of international NS/EP telecommunications services. The OPT assigns a TSP provisioning and/or restoration priority code to each NS/EP service that service vendors must provision or restore on a priority basis. Eligible TSP System users include Federal Agencies; and Federally sponsored state, local, and foreign Government Agencies and certain private industries that support the functions of national security and emergency preparedness.
Agency then places the service order with Sprint. A Sprint account manager responsible to the applying Agency processes the order through internal systems that facilitate implementation management and provisioning. Note that for provisioning TSPs, Sprint provides direct alert paths from the OPT to the Sprint TSP Manager. This path ensures expedited coordination and special treatment preparing for implementation in parallel with the Agency's order submission.

TSP information flows from the Order Administration system into a service information system that sets up necessary databases to support initial implementation/provisioning and subsequent maintenance and billing functions as shown in Figure 4.5.1-1. This process includes generation of all necessary automatic service requests (ASRs) to Local Exchange Carriers (LECs) providing the local access facilities. Customer data and service physical facility/connection information including the complete TSP code with Figure 4.5.1-1. Sprint Service Order Process.

Service restoration is via the Sprint Service Order Process.
priorities is fed to the Sprint Facilities Management System (FMS). FMS is the principal reservoir for all service detail information from start of implementation through service disconnect. Once a service is implemented, identifying data, e.g., Sprint identification for a dedicated circuit, LEC information and the associated TSP two digit priority is passed to the Sprint Trouble Reporting System (TRS). If service disruption occurs, Sprint maintenance technicians immediately check TRS, identify that the service has restoration priority, and places resources to bring the service up before other services having no priority or lower priority. While TSPs do not have associated time related SLAs, the focused application of resources has the effect of restoring services more expeditiously than any commercial expedite process or SLA. They use TRS to deliver the required hourly status information on restoration of TSP services.

4.5.1.5 International Connectivity

Voice and data services must provide access to and egress from international carriers.
to remain a competitive leader and to focus on being a complete solutions provider to our customers. Sprint uses global network providers to meet our objectives by collaborating with companies that have robust global networks and services that complement our offerings. We apply stringent qualifications and specifications to our partners to ensure that our customers consistently obtain superior performance with their international voice and data networks. As a Sprint customer, GSA can be confident that Sprint and its global partners fully back our industry-leading SLAs.

Many of our managed network partners have been long-standing and rewarding relationships with Sprint. We work very closely with these partners to develop jointly seamless extensions of our products, processes, and networks and to deliver quality services to our multi-national customers. Sprint provides significant international data service coverage using its own network resources. Sprint global network partners are recognized, award-winning providers in both quality of service and customer satisfaction. Together, Sprint and its partners have a vast global reach, offering Global Frame Relay, Dedicated IP, Global VPN, and other global voice and data services, connecting essential business centers in 220 countries and territories with local support in 191 countries.

4.5.1.6 Interoperability

Voice and data services must interconnect and interoperate with other Government or private facilities, systems, and networks.

Sprint is committed to addressing all Networx requirements for interoperability. Networx
4.5.1.7 Mobility

The ability of voice and data infrastructure to support transportable, redeployable, or fully mobile voice and data communications (i.e., Personal Communications Service (PCS), cellular, satellite, high frequency (HF) radio).

4.5.1.8 Nationwide Coverage

Voice and data services must be readily available to support the national security leadership and inter- and intra-Agency emergency operations, wherever they are located.

4.5.1.9 Survivability/Endurability

Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.
as they occur. The Sprint voice and data network architecture is composed of three elements:

• The switched network
• The transmission network
• Control and management systems

Although these basic network elements are common to all networks, in the Sprint network they were designed and built from the ground up with a single plan and objective, rather than piecemeal by replacing pieces to accommodate changing demands. Therefore, each element of the Sprint network represents the latest in design philosophy and technology resulting in an application of technology that is unique in the industry. This uniqueness is because the same technology, and therefore capability, exists everywhere in the network today, and provides the flexibility to support changing requirements and technologies in the future. These characteristics are important to Networx. Since the Networx network is a subset of the Sprint network, it means that every switch in the network is a "Networx" switch, and every transmission link is capable of providing Networx service.

One of the most significant advantages of the Sprint proposed Networx voice and data solution is that Networx is a subset of the Sprint network, rather than a network composed of selected network elements that produce a dedicated or hybrid network. Dedicated or hybrid designs result in a stranded network whose technology remains fixed. Because the Networx Technical Environment is an integral part of the Sprint network, Networx shares in the technological evolution of the Sprint network. In the last ten years, Sprint has made major network enhancements benefiting our customers. Advancements have included a transition from old linear DS-3 (45 Mbps) intermachine trunks
with limited ring architecture for survivability, to a fully SONET-based IMT network offering almost immediate service restoration following disruption. In our voice network, implementation of Dynamically Controlled Routing (DCR) makes every switch in the Sprint network a candidate tandem if direct routes between switches are unavailable or congested. As upgrades to the Sprint network elements continue, Networx will share in these updates. The bottom line is, as transmission technology advances to higher speeds with better performance, or changes in switching technology improve performance and reliability, as Sprint moves to next generation Networks, Networx will move with and benefit from these changes as well.

Sprint based the creation of the three basic elements of its network (e.g., the switched network, the transmission network, and control and management systems) on the same design goals as GETS. These elements and the benefits that GETS will achieve appear in the following sections.

Network Switching and Access

The Sprint switched voice network is based entirely on Nortel DMS250 and DMS300 switching systems and provides all Networx switched voice services. The DMS250 is an all-digital, distributed processing switching system that conforms to the North American Pulse Code Modulation (PCM) digital transmission standards and supports all domestic signaling protocols. The DMS300 is identical to the DMS250 in hardware and configuration. However, the DMS300 is equipped with software that allows it to conform to ITU Telecommunication Standardization Sector (formerly CCITT) international digital multiplexing standards and signaling protocols. Sprint uses the DMS250 to process North American (Canada, United States and northern Mexico) switch traffic and uses the DMS300 for all other international traffic. The Nortel DMS family of switching products has an
Sprint chose Nortel for its outstanding reliability, software flexibility, excellent manufacturer's support, and reduced maintenance costs.

Sprint bases the switching architecture of the network on the concept of distributed intelligent software configuration and software driven enhancements. Distributing network intelligence outside of the switches has significant advantages. It allows the switches to provide more pure switch capacity by eliminating the requirement for the switch to process signaling and customer database information. The switch processor focuses on connecting calls, while Sprint provides call features on separate, redundant databases, either distributed throughout the network, or centrally located and accessed as required. This permits rapid development and deployment of both network and customer features in common feature databases.

There are 52 DMS250/300 switches at 30 locations in the Sprint network as illustrated in Figure 4.5.1-2. Three DMS300 switches located in Stockton, CA; New York, NY; and Fort Worth, TX serve as international gateways for switched traffic. The remaining switches provide switching and Integrated Services Digital Network (ISDN) functions for the Sprint domestic switched services.
The Sprint 100 percent fiber-optic backbone with digital switching architecture delivers a highly reliable, proven, and redundant network. We designed our network as a flat (non-hierarchical) network. Each DMS-250 feature switch (supporting services such as Toll-Free, etc.) has IMTs to every other switch. These IMTs are provisioned using 50/50 physical route diversity. For example, if there were 500 IMTs between the Sprint Chicago and Omaha DMS-250s, 250 would take the direct route from Chicago to Omaha. The second group of 250 would go from Chicago, through St. Paul to Omaha. This means a call from Chicago to Omaha would normally have two physical routes. Typically, calls pass through only two switches within the Sprint network, the originating and terminating switch. During mass calling events or network disruptions that have the potential to cause congestion, Sprint would tandem a call through an intermediary switch rather than block it. Continuing the example, if the IMTs between Chicago and Omaha were congested, Sprint
would send some Omaha-bound calls from Chicago to Kansas City. The Sprint Kansas City switch—having available IMT capacity to Omaha—would pass the call to its Omaha switch for termination. This automated process is known as Dynamically Controlled Routing (DCR).

DCR monitors the IMT network in near real-time and recommends tandem routes when direct routes are congested. This results in increased network efficiency and improved network survivability. The DCR system consists of a central Network Processor (NP), DCR-capable DMS-250 switches, and data links connecting the switches to the NP. The NP receives information regarding trunk capacity and CPU status from all switches every 10 seconds via the data links. The NP uses this information to recommend tandem routes for IMT overflow traffic.

In effect, DCR uses switches and transmission capacity that are not in their busy hour to carry additional traffic. This results in increased network efficiency and improved network survivability. Considering the Chicago to Omaha call, DCR coupled with 50/50 IMT route diversity means a call would have up to four physical routes between Chicago and Omaha – two normal routes Chicago to Omaha direct, and two additional physical routes if the call tandems through a third switch. As a final measure, alternate routing of overflows to emergency standby Wide-Area Telephone Service is available.

While the common perception of switched services is voice, the Sprint network also supports switched data. The Sprint network currently provides dial-up voice grade data transmission as a permissive service or function. The network is compatible with all modems designed for voice band telephone channels, including dial-up and leased line modems.
Switch Signaling

Use of the Sprint SS7 signaling system facilitates centralized intelligent processing and the routing of network traffic. Sprint bases its SS7 network on Common Channel Signaling (CCS) international standards recommendations set by the ITU Telecommunication Standardization Sector (formerly CCITT). Domestically, Sprint conforms to the American National Standards Institute (ANSI) standards, Issue 1.

The basis of CCS is the concept of "out-of-band" signaling where signaling is a data communications function and has its own channels on the network separate from the call transmission facilities. SS7 is strategically important for the following reasons:

- SS7 takes full advantage of fiber-optic transmission technology and meets the requirements of recent ITU Telecommunication Standardization Sector and North American standards activity.
- SS7 is a high-speed, reliable data network designed to support the call setup and intelligent network needs of the Sprint network.
- SS7 is a basic block required for ISDN, and allows the addition of an abundance of new features and services that depend on SS7 technology. Without common channel signaling, Sprint could not offer the variety of different services available with digital networks with transparent interconnection.
- SS7 is the signaling system transport mechanism for the ISDN, developed with the ultimate goal of combining all communications services into a single network that any customer can access over common facilities.
- SS7 is the foundation for the Distributed Intelligent Network Architecture (DINA).
• The SS7 architecture, shown in Figure 4.5.1-3, has hardware and database redundancy in its design. Sprint employs geographically diverse routing through the Sprint Internal Transport Network (SITNET) for maximum network reliability.

The three main components of an SS7 system are the following:

• Signaling Point (SP): The SS7 interface to the voice switch (the DMS-250 in the Sprint network).

• Signaling Transfer Point (STP): The STP, manufactured by Alcatel, is a specialized packet switch supporting all SS7 message routing in the Sprint network. The STPs are interconnected, have access to the Figure 4.5.1-3. Sprint Signaling System 7 Architecture

Sprint was the first long distance carrier to deploy SS7.
same database information, and afford look-ahead capability when routing switched calls. This look-ahead capability extends only to the terminating Sprint switch, if there is no SS7 established between Sprint and the LEC where the call terminates. There are four STP pairs as follows:

- **Central Region**: Chicago, IL and Ft. Worth, TX
- **Northeast Region**: Akron, OH and New York, NY
- **Southeast Region**: Atlanta, GA and Nashville, TN
- **Western Region**: Rialto, CA and Stockton, CA.

**Service Control Point (SCP):**
A database that contains customer-specific and network routing information (e.g., authorization codes, accounting codes, toll-free number translations) and is connected to network STPs. Non-switching information that previously resided in the switches is now stored in the SCP, thereby increasing the available capacity in the switches for switching functions.

The SCP Management System in Kansas City updates the SCPs installed in Atlanta, GA; Fort Worth, TX; Lenexa, KS; and Rialto, CA simultaneously.

Communication between the DMS250 switches and one of the four associated Service Control Points (SCP) in the SS7 system support the following generic network functions:

- **Transaction Processing.**

The primary function of an SCP is to provide the signaling network with information necessary to process a call through the network. In the GETS network, this call processing information is limited to validation of the internal Sprint authorization code provided by the GAP, but can include identification of special user privileges or restrictions. The SCP is a database transaction processor with an SS7 signaling point front-end. It accepts an inquiry
• SS7 Network Control and Management. The SCPs support various internal SS7 management signals. The SCPs are the focal point in the signaling system for Sprint control and management. They also provide a centralized location for the detection of authorization code fraud.

• Database Access for Sprint. The SCP provides Sprint centralized access to databases. Although there are four SCPs, a single access point for database administration maintains synchronization of databases between all SCPs. Sprint personnel perform both batch mode and single entry changes from a central location in the SCP network so that they cannot issue conflicting updates from two different sources. The SCP Management System (SCPMS) enforces this control.

• Point of Billing and Accounting. The SCPs (collectively) are a focal point for many of the types of calls in the network, which require special billing or accounting services. The SCP may (for applications that have yet to be developed) provide Sprint with a more efficient means of obtaining billing information for these calls than is currently provided through traditional switch-oriented call detail records. This is because billing information would be collected from each of the SCPs rather than from the DMS250 switches.

• Management of the SCPs. The SCPMS maintains SCP databases to ensure the synchronization of all SCP databases. Each SCP has an identical database and ensures that if there is an SCP failure, surviving SCPs can service the network load from any region. To accommodate
4.5.1.10 Voice Band Service

The service must provide voice band service in support of presidential communications.

The Sprint Network provides voice band service in support of presidential communications.

4.5.1.11 Broadband Service

The service must provide broadband service in support of NS/EP missions (e.g., video, imaging, web access, multimedia).

The Sprint broadband data services support NS/EP missions.

4.5.1.12 Scaleable Bandwidth

NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.
4.5.1.13 Affordability

The service must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).

Sprint provided Networx voice, data, and video services are COTS based on existing Sprint infrastructure and priced to provide the best value possible to Networx customers.

4.5.1.14 Reliability/Availability

Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

Sprint can take down individual spans, rings by putting traffic on the protected or working channel while performing maintenance on the other span. Prior to this technology, scheduled maintenance required the complete shutdown of the entire circuit during the scheduled maintenance window, which shut down all traffic traversing that system.

The SONET/SDH transmission equipment generates at least 25 percent fewer span switches (electronics failures). Fewer optical amplifiers and only
Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

Volume 1 Technical—4, Networx Architecture
Event Analysis Overview

The Sprint Network consists of many different technologies and elements carrying many different services that span literally thousands of miles across the United States and abroad.
Sprint automated the process in 1999 by documenting the EAs and housing them in a database. We enhanced and expanded the automated tool in 2000. Today, the Event Analysis Database is a single repository for the analysis of Sprint Network Events. The database houses essential information regarding the root cause, corrective action plans, lessons learned, and process changes in order to enhance the efficiency and reliability of the Sprint network.

Event Analysis Process

The Event Analysis process picks up where the event resolution ends. Upon resolution, the control center responsible for resolving the event provides a recap and summary. The center opens an EA based on criteria of the event. The EA includes a list of action items and questions related to the event. Depending on the magnitude of the outage, action items in the EA are assigned either to the manager level, or to a director for significant events. Any manager or director whose group has had an impact on the event can be assigned an EA action item. The manager or director researches the action items to determine their group's impact on the event and enters a detailed response directly into the EA database. On completion of the action items, the event is closed out with closing categories and the data is used for trending and analysis purposes. Detailed discussion of significant EAs are in the bi-weekly Executive Briefing with the Vice President of Network Operations that reviews each action item.

Events that meet the criteria for an EA

- A Manager-level event meets the following general criteria:
  - Single DS-3 outage for 4+ hours
  - Four or more DS-3 outages
  - Fiber cuts
• 20,000 or more blocked calls

• Any outage that appears to be caused by procedural errors.

Director-level (also known as significant) events meet the following criteria:

• FCC reportable

• Switch isolations (DMS, ATM)

• SS7 Network isolations (STP, SCP)

• Fiber POP, ADM isolations

• Fiber cuts with customer impact.

Sprint provides voice, video and data services to a wide variety of Government Agencies including elements of the Justice Department, DOD, State Department, and others. Considering the mission of these Agencies, most of these are NS/EP services. In the data realm, these services include managed security and Firewall services and encrypted IPVPN capabilities.

The Sprint Next Generation Network (NGN) planning focuses on merging voice, data and video now provided on independent physical facilities into a single physical network platform, operating with packet protocols. In such a network, priority services in general will be offered through use of Class of Service (CoS) or Quality of Service (QoS) mechanisms in the protocols.

Currently, GETS is the only true voice NS/EP service being provided by Sprint and the only service that Sprint continues to support with specific NS/EP features such as HPC, exemption from management controls, and egress trunk queuing. Enhancements such as Dynamically Controlled Routing (DCR) and SONET survivable ring architecture are applied to the Sprint network overall and benefit all customers with improved call completion Grade of Service (GOS) and service reliability. As Sprint evolves to NGN, Sprint will accommodate GETS and its unique NS/EP features.
following paragraphs, we discuss what Sprint is able to release about NGN at this time. NGN efforts will continue in two principal areas: transport and switching.

**Transport**

Transport work includes the addition of new SONET rings, investment in state-of-the-art Wave Division Multiplexing (WDM) equipment to increase transmission capacity on existing fiber, and attention to evolving trends in Optical Networking.

**SONET and WDM**

Sprint continues to install SONET on the fiber rings in its network – leveraging its investment and endorsing its original vision of a 100 percent digital, fiber-optic network with powerful ring architecture. Sprint has deployed 567 OC-48 SONET rings and 19 OC-192 SONET rings.

Implementation of WDM has provided Sprint with two advantages. First, WDM has significantly reduced the number of physical devices per system required to implement a transmission span. A traditional transmission span of 310 miles in the 1997 timeframe allowed one 2.5 Gbps (OC-48) system per fiber using six devices. In 2003, 80-wavelength WDM allows implementation of 80 10 Gbps (OC-192) systems on a single fiber. What now requires only six devices would previously have required 720 devices. This also brings a dramatic improvement in system reliability and availability. Sprint continues to evaluate new WDM systems.

**Optical Networking**

For the NGN, Sprint is defining the use of optical network technologies to improve the transport network. Principal goals are to:

It is noteworthy that since 1996, Sprint has nearly doubled its Asynchronous/SONET DS-3 miles each year.
• Improve quality of service by further reducing the number of network elements in the circuit path and improve service restoration times
• Increase operational flexibility by simplifying provisioning and by enhancing network performance visibility and control
• Increase product/service flexibility, e.g., Wavelength or sub-wavelength on demand possibilities.

The Sprint initial focus is on ultra-long haul systems that can significantly reduce exposure of customer traffic (through switching and grooming centers) and reduce overall transit delay/latency; and with true optical switching, allow wavelength management and greater control.

Switching

The true evolution for the Sprint NGN is in the form of converged network services of voice and data. All services move first to IP packets over ATM switching and Dense WDM transmission and finally to an IP/MPLS system with DWDM. The Sprint strategy is for its voice network to migrate to this packet-based network with VoIP integration.

The initial step for voice convergence is to offload services from the DMS250 switches. Offloading involves transition to soft switch architecture as illustrated in Figure 4.5.1-5. Sprint starts with less complex call types and gradually develops support for more complex call types. GETS will likely fall into the latter category. While no schedule for such a transition exists, it is likely that soft switch implementation will occur within the next five years. It is uncertain whether full DMS250 deactivation will occur during the life of the GETS contract or at what time GETS is implemented on the soft switch architecture.
Sprint designed this packet-based architecture, and expects to implement it during the Networx period of performance. Through the Sprint Standards Committee, Sprint participates in the development of external technical standards. The committee, a companywide matrix organization of subject matter experts, reports to the Standards Committee Chairman, the Manager of Standards, and the Vice President of Technology Planning. The committee participates in the six technical subcommittees of ANSI, Accredited Committees on Telecommunications-T1, as well as their working groups and sub-working groups to develop national telecommunications standards in the post-divestiture environment. Sprint participates indirectly in the ITU for international standards, via liaison activities with ITU US Study Group C and T1 technical subcommittees. Through this extensive participation, the planning, design, implementation, and maintenance of the Sprint network and by derivation GETS and Networx, keeps current with evolving standards.
4.5.1.15 NS/EP Functional Requirements Self-Assessment

Sprint offers the following self-assessment of the required Networx services against the 14 basic functional requirements:

**Voice Services (VS)**
Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

Volume 1 Technical—4, Networx Architecture
### Audio Conferencing Service (ACS)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Sprint Approach to Meet NS/EP Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enhanced Priority Treatment</td>
<td>As contracted and directed by the NCS, priority for NS/EP voice traffic and low speed data is provided by the GETS and WPS. Sprint has been a vendor to the NCS for GETS since 1994 and has positioned the service on our Distributed Intelligent Network Architecture (DINA) to evolve with the Sprint next generation network and accommodate converged services. In this manner Sprint will eventually be able to support priority not only for voice, but data and video services as well.</td>
</tr>
<tr>
<td>2. Secure Networks</td>
<td>Consistent with best commercial practices, Sprint has taken every possible measure to protect physical and proprietary corporate resources from any threat that might impact the reliability/availability of Sprint network services to our customers. These measures extend to our customer services and address threats from both within and external to Sprint. Included are a variety of access, authentication, and authorization measures applicable to both customers and Sprint...</td>
</tr>
</tbody>
</table>

---

*Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.*

Volume 1 Technical—4, Networx Architecture

Page 118

March 5, 2007
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.</td>
<td></td>
</tr>
<tr>
<td>Volume 1 Technical—4, Networx Architecture</td>
<td></td>
</tr>
<tr>
<td>Requirement</td>
<td>Sprint Approach to Meet NS/EP Requirement</td>
</tr>
<tr>
<td>-------------</td>
<td>------------------------------------------</td>
</tr>
<tr>
<td>8. Nationwide Coverage</td>
<td>Sprint wireline voice, data, and video services are generally accessible throughout the United States through POPs in more than 720 locations. Please see Appendix B and C for Domestic and International POPs.</td>
</tr>
<tr>
<td>9. Survivability/Endurability</td>
<td>The total digital, fiber-optic transmission network has been designed to ensure network efficiency, exceptional growth capacity, and operational survivability. The network has been designed with a high degree of robustness to ensure that it can survive traffic surges and specific plant failures such as cable cuts. It also includes extensive performance monitoring systems and control systems that manage problems as they occur. In our voice network, the implementation of Dynamically Controlled Routing (DCR) makes every switch in the Sprint network a candidate tandem if direct routes between switches are unavailable or congested. The bottom line is, as transmission technology advances to higher speeds with better performance, or changes in switching technology improves performance and reliability, as Sprint moves to Next Generation Networks, Networx will move with and benefit from these changes as well.</td>
</tr>
<tr>
<td>10. Voice Band Service</td>
<td>Per the Networx RFP, this requirement is not applicable to ACS.</td>
</tr>
<tr>
<td>11. Broadband Service</td>
<td>Per the Networx RFP, this requirement is not applicable to ACS.</td>
</tr>
<tr>
<td>12. Scalable Bandwidth</td>
<td>Per the Networx RFP, this requirement is not applicable to ACS.</td>
</tr>
<tr>
<td>13. Affordability</td>
<td>GETS is funded and supported by the NCS at no cost to the individual user. WPS incurs reasonable charges to the individual users based on setup, a per month fee, and a usage rate for authorized calls. Other Sprint provided Networx voice, data, and video services are COTS based on existing Sprint infrastructure and as such, inherently minimize costs to provide the best value possible to Networx customers.</td>
</tr>
</tbody>
</table>
| 14. Reliability/Availability | The Sprint transport equipment has logic at the site to reverse the flow of traffic and restore service in milliseconds without having to send data to a central processor for analysis and decisions. This survivability gives Sprint greater flexibility for maintenance and maintains high availability. Sprint is continuing to install SONET on the fiber rings in its network—leveraging its investment and endorsing its original vision of a 100 percent digital, fiber-optic network with powerful ring architecture. Sprint has deployed 567 OC48 SONET rings and 19
Frame Relay Service (FRS)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Sprint Approach to Meet NS/EP Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enhanced Priority Treatment</td>
<td>Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic. SprintLink Frame Relay does not differentiate traffic types. The customer, however, can use its SEDs to classify and differentiate traffic at the customer edge. Sprint will then take the traffic and tunnel it across the network, treating all traffic as premium traffic, such as voice. The SprintLink Frame Relay will encapsulate all customer CoS information as payload. It will not add or subtract any CoS to treat it differently upon entering the network. Once delivered to the destination, the customer SED can once again treat the different traffic types based upon classifications they have established.</td>
</tr>
<tr>
<td>2. Secure Networks – Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.</td>
<td>Security associated with Frame Relay occurs at two key levels: 1) at the customer level, associated with WAN overlay, and 2) at the level of the underlying transport network. With regard to the Frame Relay overlay WAN at the customer level, various forms of data security are inherent to the nature of Frame Relay. As Frame Relay by nature is designed to operate at Layer-2, by definition, an Agency user is subscribing to controlled point-to-point connectivity across the underlying transport—with no unknown connections. With regard to underlying transport networks, consistent with best commercial practices, Sprint has taken every possible measure to protect physical and proprietary corporate resources from any threat that might impact the reliability/availability of Sprint network services to our customers. These measures extend to our customer services and address threats from both within and external to Sprint. Included are a variety of access, authentication, and authorization measures applicable to both customers and Sprint personnel. Much of the Sprint network is intrinsically secure from corruption concerns such as denial-of-service because of the robust routing capabilities of switched network components and survivability features employed for both switching and transmission facilities. Physical security measures are instituted throughout Sprint. Sprint buildings housing critical network equipment or administrative/management support functions are universally protected by security guards and/or electronic...</td>
</tr>
</tbody>
</table>
3. Non-Traceability – Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).

For IP-based services, like SprintLink Frame Relay, non-attributable IP addresses are assigned to core elements (like network core ports or L2TPv3-headers) assigned to specific customers. Frame Relay also provides virtual connections between locations that do not intrinsically identify users or the locations themselves. The security of this information is the responsibility of the using Agency.

4. Restorability – Should a service disruption occur, voice and data services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.

Sprint services provided through Networx meet service level agreements for reliability and restoration as defined in the service sections of this proposal, namely Volume 2, Section 5, Network Management. Critical NS/EP services have Telecommunications Service Priorities (TSP) assigned to ensure priority provisioning or restoration where authorized and needed. Sprint fully complies with the TSP system for priority provisioning (i.e., installation of new circuits), restoration of previously provisioned circuits, and priority level or design change of circuits, including coordination with local access providers. Sprint will fully comply with any future TSP replacement system.

5. International Connectivity – Voice and data services must provide access to and egress from international carriers.

Per the Networx RFP, this requirement is not applicable to the Frame Relay service.

6. Interoperability – Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks which will be identified after contract award.

Due to its maturity, the Frame Relay service has been widely adopted in a standards-based manner, providing several options for interconnectivity and interoperability between Government facilities, systems, and networks. Certain applications, such as voice and video, can simply be managed as frames with associated discard eligibility, or even just PVCs, to operate across more than one carrier network—provided that the carrier-to-carrier gateways are present and the necessary quality of service mappings are in place between the carrier networks. The depth of cross-carrier interoperability based on adherence to standards makes the process of interconnecting very simple for an Agency. Sprint has many Frame Relay carrier-to-carrier, or Network-to-Network Interface (NNI) arrangements in place today.

7. Mobility – The ability of voice and data infrastructure to support transportable, deployable, or fully mobile voice and data communications (i.e. Personal Communications Service (PCS), cellular, etc.).

Sprint has rapidly become the foremost vendor of wireless mobility services. With its recently-completed merger with Nextel, Sprint is uniquely positioned to offer Networx a variety of PCS and land mobile radio (LMR) solutions that not only satisfy priority calling requirements, but also enable FIPS-compliant encrypted transmission. The Sprint Frame Relay service is uniquely able to utilize underlying IP transport and its various connections to other mobile networks.
Satellite, high frequency (HF) radio. Services like Sprint wide-area wireless (3G CDMA PCS services), portable satellite links, or public and private 802.11 WiFi hot spots.

8. Nationwide Coverage – Voice and data services must be readily available to support the national security leadership and inter- and intra-Agency emergency operations, wherever they are located.

The Sprint Frame Relay solutions enable truly global network reach, resulting both from the Sprint-owned deployment of switch sites and network resources and, secondarily, from the multitude of carrier-to-carrier Frame Relay arrangements in place today. With the ability to interconnect an Internet PVC to a SprintLink Frame Relay WAN, secure connectivity would be available to authenticated users from virtually anywhere the Internet is reachable.

Sprint is also a pioneer in wireless mobile access technologies, first with the rollout of a nationwide 3G CDMA1xRTT network (providing 50-70kbps average), and now with the ongoing deployment of 3G CDMA EV-DO technology (providing 2.4Mbps peak downlink, 300-500kpbs average). Wireless access to Frame Relay has now become available through a product called DataLink and allows users to connect to Frame Relay anywhere they can place a digital voice call on the Sprint nationwide PCS network.

9. Survivability/Endurability – Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.

It has been widely discussed that today's Internet is a commercial derivation of protocols and technologies (such as TCP/IP) which had origins and applications to networks (such as ARPANET) whose objectives were to provide survivable communications in the event of a nuclear war. In the Sprint next-generation design for Frame Relay, the service is an overlay on such underlying IP transport. So, with Sprint, Frame Relay customers benefit from the inherent survivability afforded by IP networking.

The Sprint network architecture has been developed with a single fundamental objective in mind—to ensure the provision of unequaled network service and performance at reasonable cost. This objective is implicit in every engineering decision and operational activity for services provided by Sprint. Virtually all of the service, performance, and survivability attributes of the Sprint network are directly applicable to Networx telecommunications objectives. (By way of historical example, the SprintLink IP network suffered an outage on 11 backbone OC-48 links in the Baltimore tunnel fire several years ago, yet not a single packet was dropped on SprintLink as a result of the outage, even as Sprint peering routers absorbed an unusual increase in traffic from other carriers whose networks had service impacting outages.)

In addition to its outstanding performance characteristics, the Sprint total digital, fiber-optic transmission network has
been designed to ensure network efficiency, exceptional growth capacity, and operational survivability. The network has been designed with a high degree of robustness to ensure that it can survive traffic surges and specific plant failures such as cable cuts. It also includes extensive performance monitoring systems and control systems that manage problems as they occur. The Sprint voice and data network architecture is composed of three elements:

1. The switched network
2. The transmission network
3. Control and management systems.

Although these basic network elements are common to all networks, in the Sprint network they were designed and built with a single plan and objective from the ground up, rather than piecemeal by replacing pieces to accommodate changing demands. Therefore, each element of the Sprint network represents the latest in design philosophy and technology, resulting in an application of technology that is unique in the industry. This uniqueness is based on the fact that the same technology, and therefore capability, currently exists everywhere in the network and provides the flexibility to support changing requirements and technologies in the future. These characteristics are important to Networx. Since the Networx network will continue to be a subset of the Sprint network, it means that every switch in the network will continue to be a "Networx" switch, and every transmission link is capable of providing Networx service. Dedicated or hybrid designs result in a stranded network whose technology remains fixed. Because Networx is an integral part of the Sprint network, Networx shares in the technological evolution of the Sprint network. In the last ten years Sprint has made major network enhancements benefiting our customers. As Sprint network elements continue to be upgraded, Networx will share in these updates. The bottom line is, as transmission technology advances to higher speeds with better performance, or changes in switching technology improve performance and reliability, and as Sprint moves to Next Generation Networks, Networx will move with Sprint and benefit from these changes as well.

10. Voice Band Service – The service must provide voice band service in support of presidential communications. Per the Networx RFP, this requirement is not applicable to Frame Relay.
11. Broadband Service
The Sprint broadband data services support NS/EP missions. Today, Sprint provides a variety of broadband services to the Federal Government and Military services, both domestically and overseas. IP services include access to the World Wide Web as well as private networking established using both MPLS VPN and Frame Relay.

12. Scalable Bandwidth
NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements. Today, the Sprint next-generation Frame Relay service takes full advantage of Sprint IP networks which offer port bandwidths (over various access protocols) ranging from 56kpbs up to SONET OC-192 (10 gigabits per second). The Sprint IP backbone is based on a simple, yet highly scalable, architecture. Sprint IP networks can accommodate capacity augment either by adding additional parallel bandwidth routes at OC-48 or OC-192, or by introducing even higher-speed technologies (such as OC-768) in the future. As early as June 2004, Sprint demonstrated the feasibility of OC-768 links by operating next generation Cisco backbone routers in the production SprintLink (Internet) network.

13. Affordability – The service must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services). As SprintLink Frame Relay leverages existing underlying IP transport services, they take advantage of COTS technologies which themselves benefit from the scale of supporting commercial and public services as well. As a result, the services make full use of one of the largest IP networks in existence, and thus the economies of scale that go along with such a network.

14. Reliability/Availability – Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence. The Reliability and Availability of SprintLink Frame Relay depend on two key components: 1) The reliable operation of Agency-specific managed components (assuming an Agency elects to have Sprint manage these devices) comprising the network (primarily SEDs), and 2) the reliable operation of underlying IP transport services. Agency-specific Managed Components. Reliable operation of the VPN overlay is facilitated by a design process which produces a well-defined and agreed-upon Statement of Work (SOW). The discipline enforced by the SOW process produces a solid foundation for network design, ongoing management, and future design changes. Beyond the initial design stage, key to the reliable ongoing operation is a disciplined and mature Managed Network Services organization that has the tools and processes to not only monitor and maintain device configurations, but also one that manages on a customer-by-customer basis,
Sprint Approach to Meet NS/EP Requirement

Rather than a product-by-product focus, maintaining a customer network-centric focus results in better insight by Sprint Managed Network Operations personnel. If an Agency elects to manage their own SEDs, then this responsibility lies with the Agency.

Underlying IP Transport Services.

In the access and backhaul portions of IP networks, Sprint can take down individual spans or rings by putting traffic on the “protect” or “working” channel while performing maintenance on the other span. Sprint’s success at restoring communications traffic has been due to its deployment of SONET technology in survivable rings, which it pioneered. Sprint transport equipment has logic at network sites to switch the flow of traffic and restore service in milliseconds without having to send data to a central processor for analysis and decisions. Prior to this technology the entire circuit had to be taken down during the scheduled maintenance window, completely shutting down all traffic riding that system. This survivability gives Sprint greater flexibility for maintenance and maintains high availability.

Sprint Core IP networks utilize layer 3 protection schemes based on the IS-IS protocol. Core routes also typically rely on multiple point-to-point IP over Wave Division Multiplexing (WDM) links. Sprint continues to be an industry pioneer in deploying such techniques for network redundancy and reliability, with an architecture that can outperform other techniques such as MPLS Fast Re-Route. Indeed, by using a well-established protocol like IS-IS, in conjunction with appropriate network architecture, backbone links on Sprint IP networks ultimately have multiple redundant backup paths for re-routing network traffic, rather than just a single path per backbone link.
Internet Protocol Services (IPS)

<table>
<thead>
<tr>
<th>Requirement</th>
<th>Sprint Approach to Meet NS/EP Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enhanced Priority Treatment Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic.</td>
<td>The NCS has not contracted for an Enhanced Priority Treatment for voice and data services supporting NS/EP missions for IP services. The public Internet primarily consists of interconnections between the IP networks of Tier 1 carriers. Today, there is not a standardized mechanism to signal between Tier 1 carriers preferential treatment for packets providing NS/EP missions. While there are several possible technical approaches to meet this requirement, Government and Industry coordination will be required to deploy an interoperable solution. Sprint works closely with the NCS on an ongoing basis, and will work with them to support their requirements in the future. Within the Sprint IP network, NS/EP traffic will have a very low probability of packet loss or call block. As described in this proposal response, our IP network nodes are connected by diverse trunks that are run at 40% capacity. This permits full operation in the event of a failure of a backbone trunk with the IP traffic routed around the outage. Sprint's network design based on over capacity will ensure critical NS/EP traffic will not be blocked between points on our network during periods of congestion. Additionally, Sprint IP service includes class of service (CoS) functionality. This permits users to have 6 queues on their access link into the Sprint IP network. When the traffic load exceeds 75% of the access link, traffic is prioritized, utilizing the 6 queues. The customer can define how traffic (by application, destination, or source) is mapped to the different priority queues. This permits the prioritization of traffic at the most bandwidth constrained portion of a customer's network, the access link to the carrier's backbone.</td>
</tr>
<tr>
<td>2. Secure Networks – Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.</td>
<td>Consistent with best commercial practices, Sprint has taken every possible measure to protect physical and proprietary corporate resources from any threat that might affect the reliability/availability of Sprint network services to our customers. These measures extend to our customer services and address threats from both within and external to Sprint. Included are a variety of access,</td>
</tr>
</tbody>
</table>
3. Non-Traceability – Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).

The NCS has not contracted for Non-Traceability data services supporting NS/EP missions for IP services. However there are several intrinsic features of IP services which can be utilized to minimize the risk of a user or location being identified. These include the use of various IP VPNs, encryption and Network Address Translation (NAT). Additionally, Sprint makes use of Private (RFC 1918) IP addresses for customer IP ports (CE WAN interface) and Sprint router ports (PE) to minimize visibility on the public Internet. Knowledge of customer locations is limited to individuals who are required to deploy and support IP services.

4. Restorability – Should a service disruption occur, voice and data services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.

Sprint services provided through Networx meet service level agreements for reliability and restoration as defined in the service sections of this proposal, namely Volume 2, Section 5, Network Management. Critical NS/EP services have Telecommunications Service Priorities (TSP) assigned to ensure priority provisioning or restoration where authorized and needed. Sprint fully complies with the TSP system for priority provisioning (i.e., installation of new circuits), restoration of previously provisioned circuits, and priority level or design change of circuits, including...
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sprint Approach to Meet NS/EP Requirement</td>
<td>Coordination with local access providers. Sprint will fully comply with any future TSP replacement system.</td>
</tr>
<tr>
<td>International Connectivity – Voice and data services must provide access to and egress from international carriers.</td>
<td>Sprint provides significant international data service coverage using its own network resources. Additionally, we have agreements with international carriers around the world to provide IPS Service as well as numerous international peering partners as described in this RFP response. Sprint partners with companies that have robust global networks and services that complement our offerings. We apply stringent qualifications and specifications to our partners to ensure that our customers consistently obtain superior performance Internet Service.</td>
</tr>
<tr>
<td>Interoperability – Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks which will be identified after contract award.</td>
<td>Sprint is committed to addressing all Networx requirements for interoperability. As a Tier 1 IP service provider, Sprint IP services are standards-based and follow industry best practices. Sprint has years of experience providing IP services that interconnect with government and private IP networks. Interfaces with other government or private facilities, systems, and networks must be defined in detail by the GSA and may require development projects depending on the specifics required. Sprint will work with GSA to satisfy these needs when presented.</td>
</tr>
<tr>
<td>Mobility – The ability of voice and data infrastructure to support transportable, redeployable, or fully mobile voice and data communications (i.e. Personal Communications Service (PCS), cellular, satellite, high frequency (HF) radio)</td>
<td>Sprint IP service can be utilized to support transportable, redeployable, or fully mobile voice and data communications such as PCS, cellular, satellite, and land mobile radio traffic. This traffic can be native IP, or non-IP and transported using various tunneling techniques. Today, Sprint IP networks transport the data traffic for our own wireless networks, as well as satellite and land mobile radio traffic for numerous commercial and government customers.</td>
</tr>
<tr>
<td>Nationwide Coverage – Voice and data services must be readily available to support the national security leadership and inter- and intra-Agency emergency operations, wherever they are located.</td>
<td>Sprint IP services are generally accessible throughout the United States through POPs in more than 1,000 locations.</td>
</tr>
</tbody>
</table>
NS/EP Requirement

Sprint Approach to Meet NS/EP Requirement

9. Survivability/Endurability – Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.

As described in the IP Services section of our RFP response, Sprint’s IP network is based on a highly survivable design. Each IP node is served by multiple diverse OC-192 or OC-48 links. Traffic loads on each link is kept at 40% to permit a surviving diverse path to carry the entire load if one link fails. The TCP/IP protocol suite was developed as part of DARPA’s research into developing highly survivable packet networks. Sprint’s IP networks are based on TCP/IP and as such, highly survivable. In the event of outages, traffic is routed around the effected portion of the network to its destination.

10. Voice Band Service – The service must provide voice band service in support of presidential communications.

Per the Networx RFP, this requirement is not applicable to IP Service.

11. Broadband Service

Sprint IP service is available over a range of speeds to include Optical speeds up to OC-192. Our IP Service is capable of supporting NS/EP missions requiring high bandwidth such as video, imaging, web access and multimedia.

12. Scalable Bandwidth

NS/EP users are able to manage the capacity of Sprint IP service up to the physical capacity of the access line and port they have contracted for. Capacity can be managed via the premise based router through which they access Sprint IP services. In the event additional bandwidth beyond what they have contracted for is required, NS/EP users can contact Sprint to have their bandwidth requirements supported.

13. Affordability – The service must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).

Sprint IP Services are COTS based on existing Sprint infrastructure and as such, inherently minimize costs to provide the best value possible to Networx customers.

14. Reliability/Availability – Services must perform consistently and precisely according to their design requirements and specifications, and must be usable with high confidence.

Sprint IP services perform consistently and precisely according to their design requirements and specifications, permitting their use with high confidence. Sprint’s highly reliable network design is backed up with the industry’s leading commercial service level agreements, demonstrating our commitment to providing reliable, high performance IP services.
Network-Based IP VPN Services (NBIP-VPNS)

1. Enhanced Priority Treatment Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic. IP Data Class-of-Service (CoS), provides four standard levels of ingress/egress queuing on access links. Includes a Low Latency Queuing (LLQ) class which takes priority over other classes.

2. Secure Networks – Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.

   Key factor #1: Agency-specific managed components make up the secure VPN overlay. As NBIP-VPNS by nature are designed to deliver secure networking over even public IP networks, they by definition have multiple techniques and technologies at their disposal to insure the security and integrity of transported data.

   Key factor #2: Security is provided in underlying IP transport services.

   Network security: Secure core network components both physically and from a connectivity perspective. Appropriate use of passwords, access control, denial of service protection, etc… Includes oversight by independent Corporate Security organization.

   Customer Service Security: Institutes practices to secure communications with customers. Authentication appropriate to communication channel to verify moves, adds, changes are valid.

3. Non-Traceability – Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).

   By definition, NBIP-VPNS are designed to provide Virtual Private Network services, and thus be used within a known closed user community. However, when secure Internet gateway services are employed for outbound access from within the VPN, such access is provided via a gateway which provides services like NAT (Network Address Translation).

4. Restorability – Should a service disruption occur, voice and data services must be capable of being re-provisioned, repaired, or restored to Sprint services provided through Networx meet service level agreements for reliability and restoration, as defined in the Network Management section of the Sprint proposal.
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Sprint Approach to Meet NS/EP Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>5. International Connectivity – Voice and Data services</strong></td>
<td>must provide access to and egress from international carriers. Not applicable.</td>
</tr>
<tr>
<td><strong>6. Interoperability</strong></td>
<td>Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks which will be identified after contract award. A variety of architectures and techniques would be employed to make NBIP-VPNS interoperable with other government or private facilities, systems, and networks. Secure IP gateways using public IP services combined with encryption and tunneling (e.g. IPSEC) facilitate interoperability. Private gateways are very feasible as well, enabled principally through the exchange of traffic using standard IP data networking mechanisms.</td>
</tr>
<tr>
<td><strong>7. Mobility</strong></td>
<td>The ability of voice and data infrastructure to support transportable, deployable, or fully mobile voice and data communications (i.e. Personal Communications Service (PCS), cellular, satellite, high frequency (HF) radio). NBIP-VPNS services are able to utilize a variety of IP transport services through either private gateways or via secure gateways to public IP services. This is possible whether through truly mobile services like Sprint wide-area wireless (3G CDMA PCS) services, or other wireless services such as portable satellite links, or public and private 802.11 WiFi hot spots.</td>
</tr>
<tr>
<td><strong>8. Nationwide Coverage</strong></td>
<td>Voice and data services must be readily available to support the national security leadership and inter- and intra-Agency emergency operations, wherever they are located. Sprint NBIP-VPNS is readily available on a nationwide basis. Sprint is also especially adept at providing fixed and mobile wireless access to NBIP-VPNS via the Sprint PCS nationwide network.</td>
</tr>
</tbody>
</table>
| **9. Survivability/Endurability** | Voice and data services must be robust to support surviving users under a broad range of circumstances, from the Item 14 “Reliability/Availability” below also lists other measures and techniques applicable to Survivability and Endurability. By way of historical example, the SprintLink IP
<table>
<thead>
<tr>
<th>Requirement</th>
<th>Sprint Approach to Meet NS/EP Requirement</th>
</tr>
</thead>
<tbody>
<tr>
<td>1. Enhanced Priority</td>
<td>Priority for NS/EP voice traffic and data is provided by the</td>
</tr>
</tbody>
</table>
Volume 1 Technical—4, Networx Architecture

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.

FTS NETWORX
Enterprise
TQC-JTB-05-0002

NS/EP Requirement

Sprint Approach to Meet NS/EP Requirement

Treatment Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic.

Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS). Sprint has been a vendor to the NCS for GETS since 1994 and has positioned the services to evolve with our next generation network and accommodate converged services. In addition, Sprint offers advanced Public Safety services to provide Federal Agencies with supplemental system features that will enhance their ability to effectively respond to emergencies, as well as improve continuing operations.

GETS and WPS allows authorized NS/EP personnel to make PSTN and cellular calls, respectively, during an emergency when channels may be congested. Only individuals in NS/EP positions are authorized to use these NCS services.

Five categories have been established in order to identify critical NS/EP leadership functions and determine eligibility. The NCS decides which subscribers are eligible for GETS and WPS service. The NCS categories are:

- Executive Leadership and Policy Makers
- Disaster Response/Military Command and Control
- Public Health, Safety and Law Enforcement Command
- Public Services/Utilities and Public Welfare
- Disaster Recovery

Customers must have leadership roles in NS/EP to use GETS and WPS. Key requirements are as follows:

- Customer must be a Sprint subscriber
- Customer must request GETS or WPS service at http://wps.ncs.gov/ or call 1-866-NCS-CALL to apply.
- NCS will inform Sprint of those subscribers that are approved for NS/EP services and at what Priority Level.
- Sprint cannot add, delete or modify a subscription without NCS consent.

Sprint supports GETS; additionally, WPS is currently available on the Nextel National iDEN network and will soon be operational on the CDMA network.

2. Secure Networks – Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as Sprint provides a level of security for its customers that meets or exceeds industry standards and best practices. While applicability of some countermeasures may be specific to a particular network, device, operating system, etc., our networks in general were designed with confidentiality and integrity as cornerstones.

Confidentiality

Confidentiality is the prevention of the intentional, unintentional, or unauthorized disclosure of information. Some of the elements used to ensure confidentiality are:
Device Authentication

Each device has an Electronic Serial Number (ESN) that is matched to its Mobile Identification Number (MIN). At power-up, this pair of numbers is sent to the network for validation on the Home Location Register (HLR). Once authenticated, the device is allowed to make data connections. The network actively monitors all HLR registrations. When multiple instances of an ESN/MIN pair are detected, all devices using that pair are hot-lined and disabled. This technique, coupled with the difficulty of eavesdropping ESN and MIN combinations, reduces the opportunity for fraud by cloning a Vision-enabled Sprint PCS Phone or Device.

User Authentication

All Vision-enabled Sprint PCS Phones and Devices are programmed with a default user name and password. Without a valid user name and password, Vision-enabled Sprint PCS Phones and Devices are not allowed to use data services. As an additional security measure, mobile customers should change the default password or configure their device to require a password entry before every data connection. When the user of a device requests a data connection, the device presents the user name and encrypted form of the password to the Foreign Agent for relay to AAA server. The Foreign Agent accesses the AAA server using the RADIUS protocol. The AAA server authenticates a user's credentials, and returns the user profile designating the services that the user name is authorized to use.

Additional Handset Security

Vision-enabled Sprint PCS Phones support SSL to accommodate secure Web transactions. Customers may also choose to use token or strong authentication for application layer user authentication. These features allow all corporate transactions to perform key exchanges, user authentication, and encryption.

Client Initiated VPNs

Sprint PCS Connection Cards are limited only by the capabilities of the devices to which they are attached. The enhanced Nationwide Sprint PCS Network supports client-initiated VPNs. Perimeter firewalls do not block IPSec traffic on the ports commonly used for VPNs. However, it is important to note that since the data is encrypted across the entire connection it is not possible for the data to be optimized or compressed by Sprint bandwidth optimization servers. Customers using client-initiated VPNs should also expect lower speeds due to the overhead created by encryption and encapsulation of the payload. Additionally, Sprint recommends that users of the network install
Sprint Approach to Meet NS/EP Requirement

1. Integrity
   Integrity is the guarantee that the message sent is the message received, and that the message was not intentionally or unintentionally altered. Some of the controls used to ensure integrity are:
   - Tunneling/Encryption
     Sprint PCS CDMA Phones are equipped with a hardware implementation of Secure Socket Layer (SSL) 3.0. SSL is the standard security mechanism for establishing secure tunnels through the Internet. This feature allows mini-browsers to make SSL encrypted connections to secure Web sites. SSL sessions on the enhanced Nationwide Sprint PCS Network are encrypted end-to-end. Laptops and PDAs may use any tunneling/encryption method that their device supports.
   - Disable Transcoding and Rendering
     The 3G Gateway performs transcoding and rendering operations for many Sprint PCS Phones and Devices by default. However, customers who prefer 100% integrity of their data can instruct the network to omit any modifications. These instructions are provided through the use of standard HTTP responses.

2. Non-Traceability
   - Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).
   - Non-traceability support for NS/EP services are driven by NCS requirements for the applicable NS/EP program. Sprint will work with Networx users as required to explain options for non-traceability (e.g. ANI suppression) or traceability (e.g. location-based services) as required based on the needs of the Federal Agency.

3. Restorability
   - Should a service disruption occur, voice and data services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.
   - Sprint has an established service restoration priority and process. Should a service disruption occur, Sprint first reprovisions, repairs, and/or restores the backbone, Telecommunications Service Priority (TSP) circuits, and critical life circuits. As it pertains to NS/EP specifically, Sprint fully complies with the TSP system for priority provisioning (i.e., installation of new circuits), restoration of previously provisioned circuits, and priority level or design change of circuits, including coordination with local access providers. Once these facilities are returned to service, Sprint works closely with account teams to establish customer prioritization for facilities not already covered by TSPs.

4. International Connectivity
   - Voice Sprint services provide voice access to and egress from international carriers similar to other PSTN calls.

Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal.
NS/EP Requirement

Sprint Approach to Meet NS/EP Requirement

and data services must provide access to and egress from international carriers. PCS Vision network provides access to the global internet, allowing data connectivity to international locations. Additionally, Sprint offers voice services while roaming internationally in more than 160 countries.

6. Interoperability – Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks which will be identified after contract award. Sprint voice and data services are mature and based on numerous standards. Voice services interconnect and interoperate with the PSTN and are capable of providing service to Government or private facilities, systems and networks. Similarly, Sprint data services interconnect with our data networks. In addition to basic, standards-based internet connectivity, Sprint provides a variety of customizable services that allow data users to interconnect and interoperate with Government or private facilities, systems and networks. Sprint will work with the Government to satisfy specific needs when presented.

7. Mobility – The ability of voice and data infrastructure to support transportable, redeployable, or fully mobile voice and data communications (i.e. Personal Communications Service (PCS), cellular, satellite, high frequency (HF) radio).

Sprint maintains a fleet of redeployable, fully mobile Satellite Cells on Light Trucks (SatCOLTs) and Cells on Wheels (COWs) to augment coverage due to increased capacity demands or emergency events. These solutions enable us to provide voice, and soon data, communications wherever required.

8. Nationwide Coverage – Voice and data services must be readily available to support the national security leadership and inter- and intra-Agency emergency operations, wherever they are located. Sprint has one of the largest voice and Mobile Broadband data wireless networks in the world supporting both CDMA and iDEN platforms. In addition, the Sprint Emergency Response Team (ERT) is readily available to support emergency operations, wherever they are located. The Sprint ERT is an experienced, cross-functional group of dedicated, full-time personnel who may be augmented by reservists across the country during an event. The ERT provides wireless telecommunications equipment, infrastructure and personnel operations support to federal, state and local public safety, law enforcement, military agencies and Private Sector Organizations. ERT services are provided specifically during declared emergencies (including 22 Presidential Declared Emergencies since 2002), field training exercises, agency-specific events and National Special Security Events. The ERT designs and implements the internal policies and procedures necessary to enable timely and effective deployments of Sprint products and services. The ERT fully supports high-volume, short-notice equipment needs of...
9. Survivability/Endurability – Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.

Sprint voice and data services are robust under a broad range of circumstances. We have an established Business Continuity and Disaster Recovery Program that includes a collection of business resumption and disaster response plans designed to ensure we have implemented risk reduction strategies for crucial assets such as employees, network components, processes, and facilities.

10. Voice Band Service – The service must provide voice band service in support of presidential communications.

Sprint has a long history supporting the NCS and is able to provide voice band service in support of presidential communications through WPS or GETS as appropriate.

11. Broadband Service Per the Networx RFP, this requirement is not applicable to CPCS.

12. Scalable Bandwidth Per the Networx RFP, this requirement is not applicable to CPCS.

13. Affordability – The service must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).

Sprint extensively uses its own network capabilities, including wireless network infrastructure, spectrum, and global IP backbone, to minimize costs. In addition, we are a leader in standards development and work to use standards, best practices, and COTS technologies in our services to improve reliability, interoperability and cost effectiveness.

14. Reliability/Availability – Services must perform consistently and precisely according to their design requirements and specifications, and Sprint services are highly reliable and available to support the Federal Agencies. Some of the components of availability are:

Fault Tolerance

The core telecommunications network is comprised of elements that are specified for 99.999% reliability. This telecommunications carrier-grade infrastructure helps assure
4.5.1.16 Business Process to Support NCS Initiatives

Sprint supports the following business processes for supporting current and future NCS initiatives.

- Sprint's network is rapidly evolving to a packet switched technology that will support data networks and other applications. Concurrently, the communications needs of Federal, State, and Local personnel assigned National Security and Emergency Preparedness (NS/EP) mission responsibilities are expanding beyond the largely voice and voice-band data requirements of the last several decades. The Networx RFP recognizes this trend and requires application of NS/EP features to all commercial off the shelf services (COTS) requested. Many NS/EP features such as ubiquity, reliability and survivability are available today on COTS products; however, others such as priority treatment for Networx Critical Users are not. For an interim period, Networx Critical users should become GETS and WPS users.

- Given ongoing changes in both communications technology and the needs of NS/EP communications users—in part influenced by expectations derived from the availability of technologies—the Office of the Manager,
National Communications System (OMNCS) is reexamining the GETS requirements and developing requirements that reflect the emerging environment. Sprint is a partner with the NCS in this effort and will similarly evolve Networx services applying NS/EP features wherever reasonable and feasible.

Executive Order (EO) 12472 established the need for NS/EP telecommunications services, in response to which, the Telecommunications Service Priority (TSP) and GETS programs were created. The basis of NS/EP telecommunications services requirements has subsequently been updated and revalidated in order to respond to legal, policy, security, and technical developments.

NS/EP telecommunications services support the National Communications System (NCS) member organizations and other Federal departments and agencies in their NS/EP missions. NCS member organizations, such as the GSA, may also sponsor other organizations with NS/EP responsibilities such as state and local governments, private industry, and the American Red Cross. The NCS, however, retains overall responsibility for NS/EP service development and authorization of users. Sprint, through current contracts such as GETS and WPS, is the NCS’ partner in developing NS/EP service requirements. Sprint takes its direction for NS/EP projects directly from the NCS.

4.5.2 Protecting SS7 Signaling Systems and Satellite Command Links (L.34.1.3.5) (b))

Describe how the offeror’s approach will satisfy the requirements in Section C.5.2.5 for protection of SS7 signaling systems and satellite command links (if employed).

Sprint provides physical protection of SS7 links against external intrusion, manufactured and environmental stresses, as described in NCS TIB 87-24 and NCS-TIB 93-9.
4.5.3 Assuring Service to the National Capital Region (L.34.1.3.5) (c))

Describe how the network architecture will satisfy the requirements in Section C.5.2.7 for assured service in the National Capital Region.

Sprint has provided assured service features within our network since the original FTS2000 contract.

- Users experience two percent or less blocking for access and one-half percent or less blocking for transport under PSN overload conditions. This assumes an undamaged Sprint network; we understood that there would be appropriate adjustments in the requirements in areas where damage occurred.
- With the exception of the network switches serving Washington, DC, the loss of a single network switch will not result in a disruption of more than 15 percent of network traffic. Because of the high concentration of
traffic in and out of the Washington, DC area, Sprint uses two network switches. One switch is within the District and the other approximately 30 miles north at Elkridge, MD.

- Both the Washington, DC and Elkridge, MD switches are on multiple SONET self-healing rings.

Assured service involves an end-to-end management and design process. Components include customer premises equipment, access and egress arrangements, inter-exchange network, and network management and control. Details on these components, i.e., access, network and egress, which Sprint can control to achieve the stated requirements will be in Part B of our NS/EP Functional Requirements Plan (FRIP) and will constitute the Sprint Assured Service Plan. (J.9 ID 34509)

4.5.4 Meeting Section 508 Provisions (L.34.1.3.5) (d))

Describe the offeror’s approach for providing the capabilities needed to meet Section 508 provisions for each of the services identified in Section C.6.4.

In today’s competitive business environment, Sprint understands the need for delivering Section 508 compliant electronic information technology (EIT) products and services. Sprint's vision is to achieve the highest standard of Section 508 compliance. As a leader in communication solutions, Sprint understands the need for individuals with disabilities to have the same access as everyone else in both business and family life and in response to the need, has developed the suite of products known as the Relay Solutions. Sprint Relay Solutions provide the ability for callers who are deaf, hard-of-hearing, deaf-blind, or have a speech disability to make calls anywhere or anytime to an individual with a standard telephone. An individual using Relay Solutions has the choice of using a
Sprint Relay Solutions are a comprehensive suite of products that meet the various styles of communication through the following products:

- Sprint Relay Services
- Sprint Video Relay Services
- Sprint Relay Online
- Sprint Relay Wireless
- CapTel Relay Services
- Sprint Relay Conferencing Captioning.

Sprint strives to be a leading provider of customized communications solutions, which are Section 508 compliant and available to those with both disabilities and use assistive technologies. In keeping with the Sprint vision of aligning with the best-in-class and commitment to quality, we collaborated with Criterion 508 Solutions, Inc., (Criterion) an industry leader who will bring skills and expertise to the Networx team.

Criterion's founder Ms. Anna Bradley is a nationally recognized expert in the field of Section 508 accessible design, development and governance. Criterion's organization has been providing the Federal Government with comprehensive Section 508 compliance solutions since 2001. Criterion has assisted more than 100 Government Agencies and contractors in the design, development and repair of Section 508 compliant web sites, web applications, hardware, software, PDFs and fillable forms.

Sprint and Criterion have worked jointly to develop a baseline for Section 508 compliance, which is in the completed Voluntary Product Accessibility Templates in Appendix A for the following Sprint services:

- Call Center/Customer Contact Center Services (CCS)
Sprint will provide reporting and training in accordance with the requirements in RFP Section C.6.5 to address the reporting requirements specified in RFP Sections C.3.2 through C.3.9 and RFP Section C.7.
In the design phase, all aspects of programming, business rules and both functional and technical requirements from the Section 508 perspective will be addressed. Upon completion and approval of the design phase, the Web Portal will enter the development phase. As components of the Networx Web Portal are completed, they will undergo testing and validation through a first pass audit. Sprint will identify any areas that need remediation at that time and will implement the appropriate changes, such as programming, specifications, functionality, etc. Sprint will do additional second pass audits on the various Networx Web Portal components on an as-needed basis until the entire web portal reaches a compliant state. The organizational plan is Sprint’s blueprint for identifying all steps and identifying the types of risks associated with the Networx Web Portal. By identifying, prioritizing, and planning throughout the organizational plan for the Networx Web Portal, Sprint will provide a compliant solution for the Government. Criterion will mentor Sprint and provide their expertise in Section 508 compliance throughout the development, testing, validation, remediation, documentation, and management of the Networx Web Portal.