Before the
Department of Commerce
National Institute of Standards and Technology
Boulder, CO 80305

In the Matter of	)	
	)	Docket No: 110727437-1433-01
Soliciting Input on Research and Development	)	
Priorities for Desirable Feature of a Nationwide	)	
Public Safety Broadband Network	)	

COMMENTS OF SPRINT NEXTEL CORPORATION

I. INTRODUCTION AND SUMMARY

Sprint Nextel Corporation ("Sprint") respectfully submits these comments in response to the September 12, 2011, Public Notice seeking input on key features of a new national interoperable broadband communications network for public safety users. Sprint welcomes the opportunity to describe many of the key features and capabilities that such a network should include as the National Institute of Standards and Technology (NIST) determines research and development priorities in anticipation of the President's proposed Wireless Innovation Fund, and identifies NIST's future role in the process of setting protocols, standards and technologies for the eventual network.

As an operator of a nationwide broadband network with many of the same capabilities and technology currently contemplated for a nationwide broadband public safety network, Sprint has faced many of the important decisions on standards, protocols and development priorities NIST is now considering. In fact, Sprint recently announced the deployment of its own

nationwide LTE network, with build-out completed by the end of 2013.[1] Additionally, as a commercial operator eager to partner with the public sector to build, host, operate, and/or manage a nationwide broadband network, Sprint supports NIST's work in developing and evaluating the key features necessary to ensure that such a network is reliable, efficient, technologically-advanced and affordable to the public sector. In responding to NIST's Public Notice, Sprint emphasizes a number of recurring themes that directly relate to the overarching features and capabilities NIST should consider: most notably, the benefits of multiple commercial carriers and vendors; the importance of leveraging existing commercial infrastructure, services and technology; and the wide range of options for public safety entities in launching a network in collaboration with the private sector.

While all of the features NIST describes could be relevant in developing a reliable and robust nationwide broadband public safety network, Sprint focuses here on features especially crucial to the important public safety network goals of resiliency, availability and reliability, security, and affordability/commercial alignment. Although a subset of those features merit emphasis in this reply, Sprint would welcome the opportunity to discuss the entire range of features described in the Public Notice if desired.

II. A NUMBER OF FEATURES DESCRIBED IN THE PUBLIC NOTICE ARE ESSENTIAL TO THE OVERARCHING PUBLIC SAFETY GOALS OF RESILIENCY, AVAILABILITY AND RELIABILITY, SECURITY AND AFFORDABILITY/COMMERCIAL ALIGNMENT

In NIST's Public Notice, the overarching themes of resiliency, reliability and availability, and affordability/commercial alignment cover the majority of proposed public safety network

[1] News Release, "Sprint Accelerates Deployment of Network Vision and Announces National Rollout of 4G LTE: LTE deployment expected to reach 250 million people by 2013," Sprint Nextel, October 7, 2011, *available at*: http://newsroom.sprint.com/article_display.cfm?article_id=2064

features listed. As explained in greater detail below, these specific features are of paramount importance to a nationwide interoperable public safety broadband network, illustrate many of the greatest capabilities – and challenges – in the construction and operation of such a network, and inform many of the most important research and development opportunities that could be pursued.

A. Resiliency is essential to the successful operation of a nationwide public safety broadband network

Resiliency – the ability of network systems to recover from mishap, change, misfortune, or variation in mission or operating requirements – is a crucial feature in a nationwide public safety broadband network. One of the resonating lessons from Hurricane Katrina is the importance of resilient public safety communications networks. Specifically, an independent panel established by the Federal Communications Commission to review the impact of Hurricane Katrina on communications networks found that hardened networks – those relying on onsite backup power, agile communications mechanisms, redundant backhaul, and staff dedicated to the maintenance of backup capabilities – are less susceptible to failure.[2] In preparation for the 2011 Atlantic hurricane season, Sprint invested nearly $134 million to harden its wireless networks by deploying mobile cell sites for immediate restoration of service in the event of outage, installing permanent generators (including dozens of hydrogen fuel cell generators) with automatic cutover switches to immediately neutralize any loss of commercial power, and

[2] Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, Report and Recommendations to the Federal Communications Commission (2006) *attached to* Letter from Nancy J. Victory, Chair, Independent Panel Reviewing the Impact of Hurricane Katrina on Communications Networks, to Chairman Kevin J. Martin, Federal Communications Commission, EB Docket No. 06-119 (June 12, 2006), *available at*: http://transition.fcc.gov/pshs/docs/advisory/hkip/karrp.pdf

dispatching engineers and seasoned emergency personnel on-site to respond to any interruption or degradation in service.[3]

The competitive marketplace has ensured that broadband providers like Sprint offer highly reliable, resilient service. Indeed, while the 130 MPH winds and torrential rains of Hurricane Katrina paralyzed public safety communications networks, crippling thirty-eight 911 call centers and disabling 3 million phone lines in Louisiana, Mississippi and Alabama, commercial wireless networks often "proved to be the only communications systems still functioning on the Gulf Coast during the landfall of Katrina."[4] In this sense, it is no surprise that one of the insights of the National Broadband Plan is that resiliency is served not solely by 'hardening' public safety networks but also by allowing the public safety community "to roam and obtain priority access on other commercial broadband networks."[5] While creating a "hardened network" for public safety promotes resiliency by providing "reliable service throughout a wide area," the Plan noted that with the ability of emergency responders "to roam on commercial networks, capacity and resiliency will improve, at a reasonable cost."[6] As commercial carriers move swiftly to all-IP broadband networks, network resiliency is significantly strengthened. Inherently redundant and extremely dynamic, IP broadband networks, with their packet-switched method of transmission, provide much more resilient communications capabilities than traditional circuit-switched networks.

Moreover, a multi-vendor environment is crucially important for network resiliency. In creating a resilient public safety network, the benefits of a multi-sourced, multi-operator

---

[3] News Release, "Sprint's Florida and South Carolina Networks Prepared for Hurricane Irene," Sprint Nextel, August 22, 2011, *available at*: http://newsroom.sprint.com/article_display.cfm?article_id=2015

[4] "The Reliability of the Commercial Network," Connect Public Safety Now, March 3, 2011, *available at*: http://www.connectpublicsafetynow.org/reliability-commercial-network

[5] Federal Communications Commission, "Connecting America: The National Broadband Plan," at 315 (rel. March 16, 2010), *available at*: http://download.broadband.gov/plan/national-broadband-plan.pdf ("National Broadband Plan")

[6] *Id.* at 318.

environment are myriad. A multi-vendor, multi-operator environment promotes competition in the construction and possible hosting of a public safety network, lowering the price to public safety entities. A multi-vendor, multi-operator environment promotes redundancy, providing public safety entities alternative partners, equipment suppliers, and network maintenance partners during times of crisis. As discussed in greater detail in the section on Compatibility with Commercial Infrastructure, Sprint has firsthand experience with the benefits of a multi-vendor environment: Sprint chose three different partners to implement Network Vision, Sprint's plan to consolidate network technologies into one seamless network with the goal of increasing efficiencies and enhancing network coverage, call quality and data speeds for customers across the United States. By partnering with multiple vendors, Sprint benefits from the innovation, lowered cost, and redundancy of multiple competing providers.

Sprint's particularly proud of its Network Vision initiative, which promises to deliver many of the benefits described as essential to network resiliency by the independent panel reviewing Hurricane Katrina. Specifically, Network Vision provides infrastructure that is more agile, more efficient, and consumes significantly less power than a traditional cell site. The efficient, consolidated cell site enables operators to bring in technology like hydrogen fuel cells to provide back-up power and thereby promote redundancy and resiliency. The backhaul design for Network Vision further promotes network resiliency by relying on two distinct methods of backhaul: leased Ethernet provided to the cell site via fiber (which is more resilient than copper and T1), and Microwave from the cell site to the nearest fiber access point. With the ability to route a cell site via Microwave to more than one fiber point, redundancy is significantly increased in the event of potential fiber failures. Moreover, unimpacted by flooding or common

threats to cable, Ethernet Microwave can survive under severe weather conditions, even using adaptive modulation algorithms to reduce bandwidth to keep the link up.

Commercial initiatives like Network Vision promote resiliency not only for commercial networks, but also for public safety users that, as the National Broadband Plan observes, will need to roam on commercial networks during times of emergency. By facilitating and promoting a multi-vendor, multi-operator environment, the federal government can ensure that public safety users have more hardened, resilient networks of their own – in addition to a wide and competitively-priced range of commercial partners on which to roam or to partner with for network hosting.

B. Prioritization is an indispensable feature in ensuring the reliability and availability of a nationwide public safety broadband network

Prioritization – the ability to prioritize network traffic based on assigned priority schemes – is a crucial feature in the design of any broadband network for emergency first responders. Emergency first responders must have certainty that their mission critical communications will be transmitted without interference or undue latency. In designing a reliable and immediately available public safety broadband network, prioritization will certainly be a central feature.

Nonetheless, a tremendous amount of misinformation exists with respect to prioritization – and specifically the ability of commercial systems to implement priority access schemes for first responders. To be sure, past emergency situations have often highlighted the congestion of both commercial and public safety voice systems, as networks are faced with dramatic increases in traffic in a short time period. These past experience, however, are not illustrative of the true ability of a commercial IP-based broadband data network, with proper prioritization schemes

implemented in advance, to handle emergency communications during surge times or emergencies.

Most notably, a recent study demonstrates conclusively how priority access can work on commercial networks and meet public safety requirements.[7] It shows that commercial networks implementing priority access schemes can dependably and easily prioritize network traffic. Specifically, use of the Long Term Evolution (LTE) network technology by both public safety and commercial networks allows for dedicated access for public safety communications across shared commercial spectrum (or, for that matter, across shared public safety spectrum). Such spectrum sharing adds to dedicated broadband spectrum already allocated to public safety, significantly increasing available capacity during emergency situations.

On a more granular level, at its heart, LTE can manage prioritization with relative ease through the use of Quality of Service Class Identifiers (QCIs) which act as signals for admission control of Evolved Packet System Bearers – the packet-switched communications data transmitted on the network. A traffic bearer is associated with a set of parameters that reflect the expected user experience defined in terms of Quality of Experience – that is, the quality of service necessary for the service, as well as the user priority associated with it.[8] By creating a hierarchy of QCIs, an LTE network can dynamically and reliably prioritize emergency transmissions, obviating any concern that commercial users will disrupt or delay the flow of mission critical communications.

Through Service Level Agreements (SLAs) and Key Performance Indicators (KPIs), public safety entities and commercial partners can develop detailed and dependable priority

[7] "Public Safety Priority Access to Shared Commercial Networks," Roberson and Associates, LLC (March 2011) *attached to* Ex Parte Presentation of T-Mobile and Sprint Nextel, PS Docket No. 06-220 (March 2, 2011).
[8] "Public Safety Priority Access to Shared Commercial Networks," Roberson and Associates, LLC at 21-22 (March 2011) *attached to* Ex Parte Presentation of T-Mobile and Sprint Nextel, PS Docket No. 06-220 (March 2, 2011).

management processes in advance that designate corresponding user priority, usage priority, and application types. A wide range of prioritization schemes exist – indeed, the range of possible prioritization schemes on LTE is nearly infinite. Under such an arrangement, if a commercial provider is offering additional capacity to public safety users, LTE (with SLAs and KPIs formulated ahead of time) can support the automatic handover of public safety users from congested dedicated public safety networks to shared commercial networks without any degradation or interference. The result is an expansion of broadband capacity for first responders, with an assurance that mission-critical or other essential public safety traffic will have priority over lower priority traffic given LTE standard preemption parameters. Exactly the same set of circumstances holds if public safety entities were to allow commercial providers to use excess public safety network capacity during non-emergency periods. With agreements in place to establish traffic class priorities, key performance indicators and automatic handover during times of congestion, public safety entities can safely and confidently depend on their communications working, regardless of whether the spectrum being used is denominated commercial, public safety, or a combination of both. The inherent prioritization capabilities of LTE can effectively and reliably support public-private partnership networks among cooperating public safety and commercial operators.

C. Compatibility with Commercial Infrastructure, Network Sharing, and Scalability are all indispensable features in ensuring the Affordability/Commercial Alignment of a nationwide public safety broadband network

Of the features listed in the Public Notice, Compatibility with Commercial Infrastructure, Network Sharing, and Scalability are among the most important for ensuring that a nationwide public safety broadband network is both affordable and aligned with commercial networks and

technologies. A recurring challenge for the public safety community has been access to state-of-the-art technologies and devices and the ability to enjoy the same benefits of scale that commercial network operators currently enjoy. Compatibility with Commercial Infrastructure and Network Sharing, in particular, help overcome some of these obstacles. Scalability, meanwhile, offers public safety the network flexibility and 'future-proofing' that commercial providers like Sprint strive for.

1. Compatibility with Commercial Infrastructure

As described in the Public Notice, Compatibility with Commercial Infrastructure involves, at a minimum, utilizing a variety of commercial services when public safety users are in areas not covered by the public safety broadband network. Put another way, the Public Notice describes the importance of the ability to roam on commercial networks. Another aspect of Compatibility with Commercial Infrastructure that relates to affordability, however, is the opportunity for public safety entities to use existing commercial infrastructure.

(a) Leveraging Existing Commercial Infrastructure

With respect to the latter, it seems highly likely that a nationwide public safety broadband network will come with a Congressional mandate to leverage existing commercial infrastructure, products and services. With the cost of a 'greenfield' stand-alone public safety network estimated at nearly $48 billion over its first 10 years, according to the Federal Communications Commission, significant attention has been paid to the opportunities for an "incentive-based partnership approach" to make a nationwide public safety broadband network more affordable.[9]

[9] Federal Communications Commission, "A Broadband Network Cost Model: A Basis for Public Funding Essential to Bringing Nationwide Interoperable Communications to America's First Responders," OBI Technical Paper at 5 (May 2010), *available at*: http://download.broadband.gov/plan/fcc-omnibus-broadband-initiative-(obi)-technical-

Incentive-based partnerships would, according to the National Broadband Plan, involve partnerships using existing commercial infrastructure, encouraging public safety entities to enter into infrastructure-sharing agreements.[10] These partnerships would help public safety agencies leverage the same economies of scale as commercial providers, as an "incentive-based partnership approach leverages the commercial assets of cellular firms that have large economies of scale by serving 40-100 million customers. By contrast, a separate public safety network would not be able to leverage the same assets nor have the same economies of scale, since it would effectively serve only a few million first responders while providing similar nationwide coverage."[11]

Not surprisingly, both the House and Senate drafts of current legislation for an interoperable public safety broadband network emphasize such partnerships. The House draft calls for co-location "with the infrastructure of commercial mobile broadband service networks and other public safety communications networks" where practical and efficient and stipulates that recipients "shall use, to the maximum extent practicable, public-private partnerships between the State and providers of commercial mobile broadband services."[12] Similarly, S.911 would not only require the newly-created Public Safety Broadband Corporation to consider "the advantages offered through partnerships with existing commercial providers"[13] but would require, in a section titled "Leveraging Existing Infrastructure," that the Corporation "enter into

---

paper-broadband-network-cost-model-basis-for-public-funding-essential-to-bringing-nationwide-interoperable-communications-to-americas-first-responders.pdf

[10] Federal Communications Commission, "Connecting America: The National Broadband Plan," at 318 (rel. March 16, 2010), *available at*: http://download.broadband.gov/plan/national-broadband-plan.pdf

[11] Federal Communications Commission, "A Broadband Network Cost Model: A Basis for Public Funding Essential to Bringing Nationwide Interoperable Communications to America's First Responders," OBI Technical Paper at 5 (May 2010).

[12] U.S. House. *Spectrum Innovation Act of 2011*, Discussion Draft at 42-43 (112th Congress, 1st Session), July 12, 2011, *available at*: http://republicans.energycommerce.house.gov/Media/file/Hearings/Telecom/071511/DiscussionDraft.pdf

[13] U.S. Senate, *Public Safety Spectrum and Wireless Innovation Act,* Discussion Draft at 27 (112th Congress, 1st Session).

agreements to utilize to the maximum extent economically desirable, existing…commercial or other communications infrastructure."[14]

One of the most important facets of leveraging commercial infrastructure is ensuring a multi-vendor environment for the network. One of the lessons learned from the cellular industry in deploying in a multi-vendor environment relates to Sprint's Network Vision program. Cognizant of the benefits of sourcing network construction, operation and other services to multiple vendors – including the competitive benefits of lower cost, greater resiliency, and greater innovation as vendors strive to differentiate themselves – Sprint chose three different vendors, dividing Network Vision implementation among them on a market-by-market basis.[15]

Leveraging existing commercial infrastructure and services offers substantial cost-savings to the public safety community. Sprint is optimistic about opportunities to partner with public safety to reduce the cost of build-out by offering a variety of incentive-based partnerships to construct a public safety network. In particular, Sprint's Network Vision initiative, based on software-defined radio technology and the ability to co-locate different frequencies and air interfaces on the same equipment and towers, was intentionally built with the capability of hosting multiple networks, thereby offering significant cost-savings and speed-to-market to public safety and commercial communications operators.

(b) Compatibility with Commercial Infrastructure in the context of roaming

Another salient aspect of the Compatibility with Commercial Infrastructure feature is the ability of public safety to enjoy commercial services in areas not covered by the public safety broadband network – that is, to roam on the networks of commercials providers. Sprint believes

[14] *Id.* at 30.
[15] News Release, "Sprint Announces Network Vision: A Cutting-Edge Network Evolution Plan with Partners Alcatel-Lucent, Ericsson and Samsung," Sprint Nextel, December 6, 2010, *available at*: http://newsroom.sprint.com/news/sprint-announces-network-vision-network-evolution-plan.htm

one of the foremost challenges to the full realization of this feature for public safety is ensuring interoperability across the upper 700 MHz band.

As one of the 15 operational requirements identified by the U.S. Department of Justice Community Oriented Policing Services (COPS) report, interoperability figures prominently in the design of a successful nationwide public safety broadband network. Sprint recognizes the importance of interoperability for public safety users and for this reason encourages NIST to work to eliminate the unwarranted costs and roaming-limitations that would be imposed on public safety as a result of the restricted band classes being imposed on the 700 MHz spectrum band. Sprint believes that a nationwide interoperable public safety broadband network is best achieved – at the lowest cost to public safety – through open, non-proprietary protocols and standards, including those associated with band classes. For full interoperability, and to allow public safety to enjoy the benefits of scale in purchasing devices, NIST should consider whether restrictive band classes create gaps that prevent the full realization of interoperability – and by extension, the realization of Compatibility with Commercial Infrastructure.

By exploring the issue of interoperability across the 700 MHz spectrum, NIST can ensure that public safety entities enjoy similar economies of scale and advantages as commercial providers serving many more customers. In particular, possible research and development opportunities in the manufacture of cheaper, less battery-intensive, and smaller multi-band chipsets might be worthwhile. Interoperability, at the heart of Compatibility with Commercial Infrastructure, offers public safety entities more flexibility (ensuring that they won't get 'locked in' to one-off, proprietary devices), full roaming capability (a major priority as identified by the National Broadband Plan), and less costly public safety devices.

2. Network Sharing

The shared use of infrastructure between commercial and public safety users offers enormous cost-savings opportunities for a nationwide interoperable public safety broadband network. Particularly in the context of network hosting agreements, Network Sharing will significantly reduce the initial capex and ongoing operations costs of a nationwide public safety network. Indeed, in relation to the overarching theme of affordability/commercial alignment, Network Sharing is perhaps the most cost-effective and important feature for NIST to consider.

At a time of increased political sensitivity to large budgetary outlays, the political commitment to both a large upfront grant and ongoing support payments – even for a nationwide public safety network – is in doubt. As described above, both the Senate and House drafts bills for public safety broadband networks emphasize the leveraging of commercial infrastructure as a cost-savings measure. The prospect of Network Sharing, consequently, is especially attractive – both as a political option and as a genuine and effective cost-savings measure for the public safety community.

As discussed in the context of Prioritization, with the latest in LTE technology, public safety users can have reliable and consistent priority access on a network shared with a commercial user. There are no technical obstacles to providing public safety communicators with the capabilities they need – indeed, a shared commercial network can provide overflow capacity and an *enhanced* geographic coverage footprint in addition to the capacity and coverage of the dedicated public safety network. And crucial for public safety, agreements between public safety entities and commercial providers could easily allow for automatic hand off to commercial networks when the public safety network is congested – all while using the same priority levels established by first responders for their own public safety network. And, of course, Network

Sharing, more than any other feature discussed in the Public Notice, has the potential to substantially accelerate the timeframe in which public safety can deploy broadband networks.

Sprint's Network Vision offers precisely the cost-savings and commercial infrastructure leveraging contemplated by the pending legislation in both houses of Congress. It offers the flexibility for public safety to determine the exact hosting scheme that suits its needs. With Network Vision, Sprint offers public safety a platform with myriad options that can be tailored to suit the particular needs of different public safety jurisdictions. Put simply, Sprint has the infrastructure platform that can be used by public safety agencies to build broadband networks tailored to their needs cheaper and faster than virtually any alternative. At the most basic level, Network Vision allows Sprint to build public safety a network that they control, run according to their dictates and specifications.

3. Scalability

The ability of a system, network or process to handle growing amounts of work in a graceful manner and the ability of the network to be enlarged to accommodate growth are critical aspects of a successful and robust public safety broadband network. As the Public Notice correctly recognizes, software enhancements and upgrades (as opposed to onerous and expensive hardware replacements) represent a breakthrough in network Scalability – and, perhaps more importantly, in ensuring that a public safety network can be modified, enhanced or upgraded in an affordable and commercially-aligned manner.

Needless to say, Scalability figures prominently in any public safety broadband network. Large impact events like the attack on the World Trade Center vividly illustrate the need for dynamic network management practices that can accommodate a rapid increase in the number of users within a limited geographic area. What's more, as the needs of first responders expand to

include data-intensive applications, Scalability will involve not only dynamic changes in the capacity of the network, but dynamic changes in how network resources are allocated – specifically, what frequencies and air interfaces are best for particular applications. Accordingly, NIST should devote resources to assuring that a public safety broadband network has the scalability needed for both surge situations and future technology developments.

As noted above, Sprint's Network Vision initiative can deliver scalability to public safety both in the near-term and long term. By migrating to a multi-modal platform utilizing all frequencies available to a provider on a single base station, a network can be managed flexibly, dynamically directing users to the most appropriate frequencies and air interfaces based on the data speeds needed by users and the signal penetration necessary to reach the user – all while taking into consideration the capacity needs and resources of the entire network.

The network flexibility provided by Network Vision provides precisely the Scalability features described in the Public Notice, allowing for the accommodation of a rapid increase in users in a limited geographic area. The benefits of a multimodal platform directly relate to Scalability. By decoupling the air interface-frequency relationship, Network Vision allows a network operator to load users into spectrum bands based on signal strength – dramatically increasing coverage and capacity and delivering applications and services via the most appropriate air interface and frequency for their effective use.

Network Vision enables network operators not only to change network settings, capabilities and capacity in the near-term to respond to emergency situations; it also provides public safety with a solution to their future (and potentially unexpected) needs, 'future proofing' their public safety network for the first time.

III. CONCLUSION

While all of the features described in NIST's Public Notice are relevant to the successful deployment of a nationwide public safety broadband network (and in the near-term, to help NIST in determining research and development priorities), Sprint respectfully submits that the features describe above represent the most salient and critical factors to the realization of a robust, interoperable, and reliable public safety network. Sprint appreciates the opportunity to contribute to the process and looks forward to exploring opportunities to partner with public safety to deliver an effective, reliable, and affordable public safety broadband network as quickly as possible.

Lawrence R. Krevor
Vice President, Government Affairs, Spectrum
Richard B. Engelman
Director, Government Affairs

900 7TH Street, NW Suite 700
Washington, D.C. 20001
(703) 433-8124

October 12, 2011