October 12, 2011

DEPARTMENT OF COMMERCE
National Institute of Standards and Technology
[Docket No.: 110727437–1433–01]

Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network

AGENCY: National Institute of Standards and Technology, Department of Commerce.
ACTION: Notice and request for comment.

Comments of Nokia Siemens Networks US LLC

Nokia Siemens Networks US LLC ("Nokia Siemens Networks") hereby submits comments in response to the Request for Comment referenced above.

Nokia Siemens Networks is a global provider of mobile and fixed communications network solutions and services for the commercial and public sector markets. Our comments below respond to and track the questions raised in the RFC. We thank you in advance for considering our views.

Respectfully submitted,

Brian Kassa
Head of Technology – Public Safety Broadband
Nokia Siemens Networks

Derek Khlopin
Head of Government Relations – North America
Nokia Siemens Networks

To ensure resiliency in an emergency:

Resiliency: The ability of operable systems to recover from mishap, change, misfortune, or variation in mission or operating requirements.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that network resiliency is critical for a nationwide Public Safety Broadband Network (PSBN). However, resiliency is a matter of degree. For the most part, the techniques to make a network resilient are known and a matter of sound design, operation and cost. Utilizing commercial techniques will go a long way in this regards, but discussion needs to continue on just how resilient, at what cost and – more germane in this forum – what aspects are most unique to the Public Safety (PS) community.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: 3GPP Release 8 LTE networks are based on a long development history that has been driven by the wireless industry to dramatically increase resiliency. One of the major advances has

been the inclusion of Internet Protocol (IP), which, as demonstrated by the resiliency of the Internet, enables the network to find new paths to secondary network elements when the network suffers from a fault. LTE networks can be designed to overcome single points of failure and almost all contingencies save the failure of the actual cell site. Third Generation Partnership (3GPP) standards support "pooling" of network element and redundant paths supporting interconnection between elements. However, cell site outages are the primary failure that cannot inexpensively be designed around, while core network equipment is housed in hardened buildings with multiple backup systems, which make them highly resistant to failures. Therefore, Nokia Siemens Networks believes that one good use for research funds is to address the techniques of making the 'cell site' or RF as highly available as that of the rest of a well-designed network.

There are a number of things that can mitigate cell site failure in order of recovery time. First, a commercial carrier can be used as a backup via roaming during a Public Safety site failure. This can happen almost immediately but requires that an agreement be in place before the fault. Second, the network can utilize its Self Organizing Network (SON) features to modify the surrounding cells to attempt to extend coverage to fill-in for the affected cell site. This can occur automatically or with manual human intervention. Third, the local jurisdiction can bring in a Cell on Wheels (COW) or a Cell on Light Truck (COLT) to cover the affected area until repairs can be made. One may also be able to design and deploy networks with site overlap. While doubling the number of sites would generally be too expensive there may be certain areas which warrant developing overlay sites, perhaps leveraging HetNet (Heterogeneous Network) technologies. Additionally, hardening the cell site via various techniques including redundant equipment, more secure locations, etc. may address another class of more sensitive sites. Finally, if the failure is easily repaired, a technician can be sent to make repairs.

- Possible research and development that could take place to close any technical gaps;

  Response: Nokia Siemens Networks believes that network resiliency is more a matter of sufficient funding and proper design and operation rather than lack of technology, features or functionality in 3GPP Release 8 or the various vendors' implementations of those standards. With adequate funding, design and operation, the network can be implemented without single points of failure. However, there likely will be cases where such network design is outside of the financial reach of a Public Safety entity when moving from a centralized site system with few sites to a cellular system which has considerably more sites. Therefore, effort could be expended aimed at allowing for mitigating cell site failures such as in the scenarios detailed above. Specifically, research into using HetNet technologies to develop overlay solutions for PS may warrant investment in order to further development.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

  Response: The primary concern is one of affordability. Network element providers can design and build extremely fault tolerant networks but must do so at some cost with a quickly diminishing rate of return. If roaming onto commercial networks is allowed, then terminals may need to support multiple bands and radio technologies beyond Public Safety's base LTE radio. Assuming that commercial networks themselves may also have congestion due to an event the enhancement of NGN-GETS may be required. One area that may need coordination if not research funding, is which Public Safety areas can afford how much resiliency. For instance, it may be fine to cover Manhattan in New York City with overlapping cell sites, but Montana – perhaps not. A good understanding of what level of resiliency is affordable in what circumstances may yield systemic issues of the current and upcoming commercial offerings in addition to those areas already identified.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

Response: The design principles that Internet Content Providers, Internet Service Providers and both fixed and wireless telecommunications carriers use to achieve 99.999% (five nine's) reliability are directly applicable to Public Safety Broadband deployments. Commercial Networks provider operations and planning practices should be studied and adapted to reach the availability needs of Public Safety.

Self-Organizing: Self-organizing networks dynamically manage their own configuration by automatically making changes to ensure messages reach their destinations.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that Self Organizing Network (SON) technology is of critical importance to a Nationwide Public Safety Broadband Network. Specifically, one purpose of SON is to help with the operation and deployment of a network and it is financially important to minimize the effort in deployment and operation scenarios. On the other hand, SON also reconfigures the network when there are disasters that may impact the viability of some sites (despite efforts to make sites more resilient). This provides the double impact of getting optimal usages of the available equipment – automatically.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: Commercial wireless carriers are heavily driving SON technology. These technologies are critical to their ability to meet both their technological as well as commercial growth requirements. We believe that the carriers will continue to drive these requirements much faster than Public Safety will be able to keep up with. Public Safety will benefit in those areas without having to drive technological advancement through research and development efforts. However, Public Safety has interest in certain aspects applicable to SON which may not be as critical to a commercial venture. For instance, natural disasters which cripple large areas of equipment may be so rare that the commercial entities in effect can afford to take a conservative approach whereas the Public Safety community must be operational during such a disaster and likely has to take a more proactive stance. Those features specific to a largely compromised network self healing, offering best effort in a compromise to priority traffic, preferring priority traffic, and aiding in rapid deployment may be areas where Public Safety participates actively in the standards process and perhaps even sponsors research.

- Possible research and development that could take place to close any technical gaps;

  Response: Nokia Siemens Networks has not identified specifics for suggested research in this area.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

  Response: Public Safety may face challenges in deploying these technologies due to feature and implementation costs associated with them. It may become a simple trade-off between deploying an additional 10 sites or spending on technology that enhances the functionality of existing sites. Perhaps this is an ideal area for the sharing of best practices and learning throughout the Public Safety community. No doubt there will be particle issues that need to be dealt with and industry expertise will be developed – perhaps in so doing the need for some capability will become evident as well.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

Response: Nokia Siemens Networks believes that Public Safety should leverage and follow what the commercial carriers are implementing within their networks as well as sharing the learning within the PS community.

Meshing (ad-hoc device-to-device communication): A type of networking where each node must not only capture and disseminate its own data, but also serve as a relay for other sensor nodes, that is, it must collaborate to propagate the data in the network.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Meshing can be a highly beneficial feature in relation to a Nationwide Public Safety Broadband Network. While meshing typically has been utilized in base station networks, it can also apply to devices so as to allow devices to mesh together in a unit-to-unit "Direct Mode Operation" as well as to connect to the rest of the network should one node be in range of a fixed site. Sensor nets could well fall under the same category as user devices meshing until the data can be linked to the larger fixed network. Ad Hoc communications networks weather for sensors or voice communications between points need are subsets of a Direct Mode Operation. The device itself can be a gateway or bridge to pass data back to the network.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: 3GPP Release 10 Relaying was only approved during 2011. Industry currently is working on implementing those features into their respective products. Much of the research is done and now Public Safety must wait for the development and implementation of these features.

  Direct Mode Operation (DMO) is in its infancy; during the summer of 2011 it was proposed as a 3GPP study item. Since DMO is a feature really applicable to Public Safety, the interest to prioritize in international standards bodies is not as high as other commercial features in comparison. The Alliance for Telecommunications Industry Solutions (ATIS), which creates standards for North America and is a 3GPP partner, would likely be better able to place priority to Public Safety work as a precursor to bringing the work to 3GPP.

- Possible research and development that could take place to close any technical gaps;

  Response: Relaying is being implemented currently. Public Safety should focus its research and development efforts on Direct Mode Operation due to its importance as a precursor to Mission Critical Voice-over-LTE.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

  Response: Neither relaying or DMO are commercially available today. Relaying potentially will become a very important Fire Ground or Incident Site technology but Public Safety will have to fully understand it to determine how it should be deployed as part of typical emergency response equipment. Mission Critical Voice-over-LTE will require DMO or some functionality that allows device-to-device communications.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

  Response: Public Safety is breaking new ground here so there are no best practices to leverage. If Public Safety lags the commercial carriers in Relaying, then the lessons learned by the carriers

should be leveraged.

Adaptability: The ability of the network and/or device to modify/ change behavior based upon external conditions.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that Adaptability can be achieved though Self Organizing Network and through Dynamic Policy and QoS control. Please refer to our discussion on Self Organization for our opinion of its importance and please see our discussion on QoS for our opinion on its importance.

To ensure reliability and availability:

Prioritization: The ability to prioritize network traffic based on assigned priority schemes.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Please see our response for QoS as we believe that Prioritization and QoS cannot be considered separately.

Quality of Service (QoS): The set of standards and mechanisms for ensuring high-quality performance for critical applications. By using QoS mechanisms, network administrators can use existing resources efficiently and ensure the required level of service without reactively expanding or over- provisioning their networks. The goal of QoS is to provide preferential delivery service for the applications that need it by ensuring sufficient bandwidth, controlling latency and jitter, and reducing data loss.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that Prioritization and QoS are of critical importance a Nationwide Public Safety Broadband Network.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: Currently there is considerable functionality within 3GPP Release 8 for end-to-end QoS and Prioritization. In our many discussions with Systems Integrators, Public Safety and the various groups that have convened to work on this topic like NPSTC, we have not been made aware of gaps in the current standards. As a highly active member company of 3GPP, we are prepared to fully support any deltas and additional functionality needs that Public Safety may identify in the 3GPP standardization process.

  We believe that the fundamental problem facing Public Safety with regards to Prioritization and QoS is that there are so many different ways that the available features can be utilized and implemented. Without guidance, each Public Safety jurisdiction may implement something different which could lead to significant roaming and interoperability issues.

- Possible research and development that could take place to close any technical gaps;

  Response: Nokia Siemens Networks believes that effort should be spent on helping Public Safety to understand and implement a Prioritization and QoS Framework that can be implemented

nationwide in each jurisdiction or on the National Public Safety Broadband Network. Once this is done and if gaps are identified, then effort should be expended to resolve those gaps.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

  Response: The complexity of the 3GPP Release 8 Priority and QoS Features suggests efforts should be placed on establishing appropriate guidelines for network and device profiles to ensure interoperability.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

  Response: Full implementation of Priority and QoS is typically not done by Wireless Carriers so Public Safety may be breaking new ground in this area.

To enable security:

Strong, Dynamic Access Control: Access control lists can be configured to control both inbound and outbound traffic on networks and authentication/ verification of users/devices on the network.7 The level of access control should be sufficient to allow for entree into a broad set of systems and databases needed by public safety (e.g., criminal history databases, medical records, public work records, etc.).

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that Strong, Dynamic Access Control is of critical importance a Nationwide Public Safety Broadband Network. However, it is only a part of the much larger security topic. Public Safety must ensure the security of the network, the applications, the end-user-devices and the physical infrastructure. One additionally important area that does not obviously fit within the list of items but seems to fit best here is a Denial of Service (DoS) attack at the wireless access layer. Such an attack could cripple the PSBN if someone wants to seriously disrupt emergency response services relying on said network.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: 3GPP Release 8 Security is built upon a long history of successful security implementations. Wireless Carriers have driven 3GPP to ensure that their networks are deployed with the ability to control which users and devices can access their networks. The security mechanisms that were initially developed for GSM were enhanced with UMTS/WCDMA and then again further enhanced with LTE.

  LTE security depends on strong security associations between devices and the network; between the network's elements and protection of the network from other networks it touches. If you consider that a security association is effectively a tunnel, then a user's traffic is carried in a tunnel which is surrounded by tunnels within tunnels. This provides for a very secure transport of the user traffic. Public Safety must also look at the security of the applications, the end devices, and the protection of the LTE network as it touches other networks. These topics fall within the more classical security practices that any entity connected to the Internet must contend with.

  There is one fundamental security issue that 3GPP Release 8 cannot solve. It has long been a problem in the wireless industry that if another user surreptitiously gets access to your device or Subscriber Identification Module (SIM or USIM), that user will have access to your data and services. There is no way to authenticate the user to his device. If you assume that 3GPP Release 8 ensures the security and access of the device to the network and the user's traffic through the

network you are essentially left with an open door to mission critical data and communications if the user cannot be authenticated to the device. One way around this issue is to authenticate the user to each application such as most users do currently to access email. However some applications and services do not provide a user interface with which to authenticate the user. Another method would be to create a Virtual Private Network between the user's device and the network but that tunnel remains open until it times out or is closed.

At present, there is no significant answer to handling a Denial of Service attack at the radio access layer. Reliable and consistently used methods of identification that such an attack is underway and proactive steps to mitigate any such attacks are generally absent in the commercial wireless operator networks because it is a very difficult problem to address in a cost effective and reliable manner for commercial systems.

Nokia Siemens Networks believes that Authentication of a user to a device is critical to protect a Nationwide Public Safety Broadband Network. We also believe that DoS attack countermeasure options need to be explored.

- Possible research and development that could take place to close any technical gaps;

  Response: The wireless carrier community has not seen authentication of a user to the device or network as a critical need because at most the damage caused by breeches in this area are only damaging to the end user from an identity perspective and damaging to the carrier in small losses of revenue from fraudulent use of the network. However, for a Nationwide Public Safety Broadband Network carrying sensitive and mission critical data these types of breaches are unacceptable.

  Nokia Siemens Networks believes that security must be assessed from an end-to-end perspective to include the LTE network with special emphasis on the radio physical layer where a DOS attack is most likely to occur, Applications, End-User Devices, and network-to-network interfaces. The complexity of the topics could be beyond the ability of Public Safety to address so research and development of end-to-end security framework or guidance would be extremely valuable.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

  Response: Public Safety will be able to fully implement the security protections provided in 3GPP Release 8.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

  Response: The wireless carriers have been quite successful, with a few notable exceptions that make their way into the media, in implementing security for their networks. Their best practices should be examined for applicability to Public Safety.

To ensure affordability/commercial alignment:

Compatibility with Commercial Infrastructure: The utilization of a variety of commercial services when public safety is in areas not covered by the public safety broadband network.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that compatibility with commercial infrastructure is critical to a Nationwide Public Safety Broadband Network. Initial Public Safety deployments will

create small islands of coverage that will take a number of years to completely fill in. Until this happens, Public Safety must be able to utilize the coverage provided by commercial carriers. Also the commercial carriers can be further utilized to provide backup capacity and even backup coverage should a Public Safety cell site fail.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: The primary issue preventing compatibility with commercial networks is one of physics which hampers the ability to put multiple 700 MHz band classes into a small device. Device manufacturers have been able to put multiple bands outside of 700 MHz into a single device however, but there are always challenges that have to be overcome. The secondary issue is that roaming onto Commercial Carriers requires that network be compatible, that governance models exist to ensure roaming functionality and agreements exist between entities and the wireless carriers. One of the major issues with regards to compatibility will be Public Safety's Prioritization and QoS Framework which, if not carefully designed, may not be compatible with commercial carriers.

- Possible research and development that could take place to close any technical gaps;

  Response: The physics issues likely will diminish over time but the commercial market is not necessarily going to evolve in this direction absent incentives for it to do so. Research and development effort in this area should greatly help Public Safety. A Nationwide Public Safety Broadband Network's controlling entity must solve the secondary issues as mentioned above.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

  Response: Public Safety devices may need to be certified on multiple networks and/or certification bodies.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

  Response: Public Safety needs to work with handset conformance bodies like the Global Certification Forum (GCF), PTCRB, and with the GSM Association and CTIA for interoperable services.

Network sharing: The shared use of infrastructure between commercial and public safety users.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that, outside of roaming, this likely should be done only for tower space and backhaul. Commercial carriers must balance the needs of their subscribers against those of Public Safety. There are federally mandated services that carriers provide today like GETS (Government Emergency Telecommunications Service), but beyond those it will be hard to ensure Public Safety will have the capacity, features, prioritization and QoS required to mitigate incidents. Tower space and backhaul networks can be shared as they can be engineered to separate commercial from Public Safety traffic and usage.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: In the roaming case, governance and either commercial or governmental relationships need to be agreed to ensure needs are met. Limited extra tower capacity may prevent a 1:1 sharing

approach everywhere. Backhaul agreements and available transmission capabilities at sites may be constrained.

- Possible research and development that could take place to close any technical gaps;

  Response: Nokia Siemens Networks does not believe that research and development can solve these issues.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;
- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

  Response: Public Safety can look to the wireless carriers and roaming clearinghouses for examples of how roaming agreements can be realized.

Multi-Modal: The ability of the network to support voice, video, data, and multimedia simultaneously.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believe that a 3GPP Release 8 network, if properly designed, engineered and implemented, will support multiple applications simultaneously during normal operations. During times of network stress, proper implementations of Priority and QoS will ensure that the most critical applications are able to utilize the available network capacity.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: There are several issues here that will hinder Public Safety's realization of a multi-modal network. First, there are very few standards in Public Safety for compatibility of applications. Very typically, each jurisdiction purchases the application that best meets its needs at the time of purchase but each application may not be compatible for resources from neighboring jurisdictions or resources that come into the jurisdiction to mitigate an incident. Second, there is currently no standard for Mission Critical Voice-over-LTE. There are several commercial offerings but there is no compatibility between them.

- Possible research and development that could take place to close any technical gaps;

  Response: Nokia Siemens Networks believes that research and development effort should be expended on both of these issues.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;
- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

  Response: There are several standards bodies like the Open Mobile Alliance that could potentially be utilized as examples for a Public Safety applications standards body. Mission Critical Voice-over-LTE standardization should be patterned after the GSM-Railroad methodology that was used to define those standards. In that case, the interested parties worked together outside of 3GPP to define the standards and bring them as a group back to 3GPP.

Scalability: The ability of a system, network, or process to handle growing amounts of work in a graceful

manner or its ability to be enlarged to accommodate that growth. At the design phase, this could include requirements to ensure that scalability can be achieved, to the extent possible, by software enhancements and upgrades as opposed to by hardware replacements. Scalability also includes the need, in the case of a large scale event, to accommodate a rapid increase in the number of users in a limited geographic area.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that this is a critical issue for a Nationwide Public Safety Broadband Network. However, a majority of the equipment that will be used to build out the network is the very same equipment that wireless carriers use to build commercial networks. This equipment is capable of supporting subscriber numbers in the hundreds of thousands through millions and traffic densities in excess of hundreds of gigabits. Typically wireless carriers will have 4-5 core sites for the entire United States. Nokia Siemens Networks believes that scalability should not be a concern for a Public Safety core network built under the national Public Safety Broadband Corporation proposal but there are research opportunities to develop solutions for addressing rapid deployments for large-scale events. Nokia Siemens Networks believes that the research should be conducted with respect to the rapid deployment of temporary cells. While commercial operators have long deployed CoWs and CoLTs (cells on wheels/light trucks) the development of small cell deployments utilizing the integration of LTE HetNet and SON capabilities warrants further research and development to address more rapid deployment of more portable equipment.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: Extremely rapid deployments to address abnormally high capacity demands for smaller scale incidents or rapid multiple deployments in a larger area.

- Possible research and development that could take place to close any technical gaps;

  Response: Integration of HetNet and SON capabilities tailored to PS deployment needs.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

  Response: Slower integration of larger scale, more expensive solutions.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

Power Awareness: The ability of network/devices to control power functions.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that power awareness is of critical importance to a nationwide Public Safety Broadband Network. However the wireless carrier community is driving the network element providers to develop these features. We believe that Public Safety should follow the wireless carrier community in this area and focus its research and development efforts on other topics.

- Current gaps that exist preventing the realization of the full potential of the feature;
- Possible research and development that could take place to close any technical gaps;
- Any challenges that public safety could face in realizing the full potential of these features given

currently implemented solutions;

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

Standardized Common Interfaces: Protocols, Application Program Interfaces, application platforms, radio capabilities, etc. that allow for competitive provisioning.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that protocols, Application Program Interfaces, application platforms, and radio capabilities are of critical importance to a Nationwide Public Safety Broadband Network. Standards are the key for interoperability and for allowing wide flexibility in choosing equipment for Public Safety use at the lowest price.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: There are numerous industry standards available from different organizations which would create common interfaces. The gap exists today in that Public Safety needs to choose which ones will be implemented within the Public Safety National Broadband Network.

- Possible research and development that could take place to close any technical gaps;
- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;
- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

Uniform, Universal Access: The ability to access the network and data anywhere at any time through any device.

- Your assessment of the importance of the feature in relation to a Nationwide Public Safety Broadband Network;

  Response: Nokia Siemens Networks believes that this is an important feature for a Nationwide Public Safety Broadband Network but is an implementation issue rather than one that requires research and development. If the nationwide network is designed and implemented along with proper governance models, uniform, universal Access will be available to all network subscribers whether they are local or itinerant.

- Current gaps that exist preventing the realization of the full potential of the feature;

  Response: Nokia Siemens Networks believes that this will be a matter of proper governance which will ensure that each subpart of the network will enable itinerant access.

- Possible research and development that could take place to close any technical gaps;

  Response: If research and development effort is expended for this area, it should be on defining a proper network identifier scheme and governance model that will ensure a non-local or itinerant user can access the services and applications required wherever that user is attached to the network.

- Any challenges that public safety could face in realizing the full potential of these features given currently implemented solutions;

  Response: Public Safety jurisdiction's belief that they must have local control combined with the natural tensions between agencies and jurisdictions may make realization of uniform, universal access quite difficult. Applications built on open protocols (e.g. https as used on the web etc.) can be accessed from any device technology (WIFI, LTE, etc.). This allows some re-use of existing security controls and access methods.

- Best practices from other industries that could be leveraged to expedite public safety's realization of these key features.

  Response: Wireless carriers have been able to, through GSMA, create a global reaching GSM network that simply works when a user steps off of an airplane in a different country. We recommend following these best practices when designing the nationwide network and the governance model.

Additionally, NIST is requesting input on the following further considerations for the nationwide public safety network:

- What is the importance of employing open standards for the nationwide public safety network?

  Response: Nokia Siemens Networks believes that open standards are absolutely essential to creating and maintaining a competitive marketplace, which in turn establishes a cost efficient ecosystem for the industry. Openness as facilitated by 3GPP for GSM, UMTS, and now LTE ensures a large number of equipment choices, by multiple suppliers, based on high levels of interoperability and competition. It allows for interworking and interoperability between networks, and a level of interchangeability of equipment. Finally, open standards reflect a broad set of market requirements, which ensures robust feature development for the industry.

- What is the need, if any, for commonality of functions across the system?

  Response: This is critical for Interoperability. 3GPP Release 8 LTE networks have the benefits of tremendous features and functionality. If left to their own devices, each Public Safety Jurisdiction could potentially configure these features and functionalities in different ways leading to a nationwide network that is not interoperable. A common system design and operational feature set is needed with room for regional/local variations, which are built on top of a common national base.

- What is the importance of a multi-vendor environment for the network and what are the lessons learned in deploying a multi-vendor environment from the cellular and other industries?

  Response: A multi-vendor environment is very important for the nationwide PSBN. Commercial cellular networks have been multi-vendor due to interoperability built into the GSM and 3GPP standards. Multi-vendor networks have allowed operators to leverage competition to build best of breed networks. In a multi-vendor environment, services and feature roadmaps for the network need to be defined to allow all the vendors to align feature releases to meet the network's deployment plans. Having a robust competitive environment and bringing in new competitors would be highly beneficial to ensure that Public Safety and all of the covered populations have the best solutions at highly competitive rates.

- What can be done to ensure both short- and long-term affordability of the network for all types of public safety agencies?

Response: There are a number of things that can be done to ensure affordability. First, ensuring that multiple deployment models are available to Public Safety like Hosted Core, Managed Service, Shared Radio Access Networks or a typical complete build out will ensure that each jurisdiction is allowed to utilize a purchase methodology that meets its unique financial needs. Secondly, defining a set of features that the network will utilize will ensure interoperability but also utilized capital on features that will truly benefit Public Safety. Thirdly, aligning a majority of the features and functions along with the wireless carrier community will enable Public Safety to access the economies of scale that wireless carriers enjoy. Finally, there will be some features, functionality and user devices that will be specific to Public Safety. Ensuring that these are common across Public Safety will ensure that some economy of scale can be realized.

- In a recent report, the President's Council of Advisors on Science and Technology suggested the need to develop methods for implementing a ''survivable core'' of cyber-infrastructure that would be relied upon to provide truly essential services in the event of a catastrophic cyber-attack.9 Please comment on how NIST should pursue this recommendation. Among other things, commenters should address whether the goal should be to design a separate survivable core that is integrated and interoperable with the primary public safety network, or instead to design the primary network such that it can reconstitute rapidly— following a catastrophic event—to achieve some ''core'' level of service.

  Response: Proper network design will ensure that there are no single points of failure. Design principles like Geographic Redundancy with failover, multiple IP paths between elements and state of the art cyber security will ensure that the network is there when it is most needed.

- What is the marginal cost of the feature/functionality versus equipment available today?
- What network features or requirements have not been identified above, the lack of which may impair the network's ability to adequately serve the needs of public safety?

  Response: Support for Non-Voice Emergency services (NOVES), Commercial Mobile Alert Services, location services using A-GPS and OTDOA, and broadcast video (MBMS) appear to be needed to complete the services which public safety will need for users.

- How should NIST engage public safety practitioners and technologists as part of the planned R&D projects to ensure proper prioritization of efforts and effectiveness of developed solutions?

  Response: Currently there are a number of working groups organized through NIST, NPSTC, APCO and some regional entities that are doing excellent work. Between now and the potential establishment of a National Corporation for Public Safety, this work should continue. Nokia Siemens Networks will continue to support these efforts but also would be open to a more formal approach of directed research and development.