COMMENTS OF
NORTHROP GRUMMAN INFORMATION SYSTEMS, INC.

NIST DOCKET 110727437-1433-01

NORTHROP GRUMMAN INFORMATION SYSTEMS, INC.

7575 Colshire Drive
McLean, Virginia 22102
(703) 449-3993

October 12, 2011

Summary

Northrop Grumman Information Systems, Inc. ("Northrop Grumman") is pleased to provide its input to the National Institute of Standards and Technology (NIST) docket number 110727437–1433–01 "Soliciting Input on Research and Development Priorities for Desirable Features of a Nationwide Public Safety Broadband Network", henceforth referred to as NIST's request. Our input is focused on areas of expertise where there is an intersection of our corporate experience with specific areas of challenge to building the future national public safety network. In this document we will relate our responses to the four overarching themes outlined in NIST's request - adaptability and resiliency ("resiliency in an emergency"), prioritization and quality of service ("reliability and availability"), network security and strong dynamic access control ("security"), and network sharing and scalability ("affordability/commercial alignment").

Introduction

Northrop Grumman Information Systems, Inc. is a wholly-owned subsidiary of Northrop Grumman Corporation. As a leading provider of IT, systems engineering and systems integration services, we serve the Department of Defense, national intelligence, state and local agencies, and commercial customers. For more than 50 years, Northrop Grumman has assisted the public sector in building and operating IT systems that support critical missions that deliver services and protect citizens. Northrop Grumman is a leader in public safety communications systems, including being the integrator of some of the world's largest 9-1-1 First Responder Computer-Aided Dispatch systems.

Our participation in the public safety700 MHz band proceedings began from their commencement, and we support the strategy to create an open standards solution for the national public safety broadband network (PSBN). Northrop Grumman has deployed next-generation secure broadband wireless networks and interoperable voice communications solutions for

defense, intelligence, and public safety agencies across the world. We have gained valuable experience in the future architecture and technologies for next generation public safety communications through our design, implementation, and operation of the nation's largest public safety broadband network known as the New York City Wireless Network (NYCWiN). In total, Northrop Grumman has deployed over 30,000 mobile data units to law enforcement and emergency response agencies nationwide through various integration programs. In addition, Northrop Grumman has a major presence in domestic security initiatives, and we are the number one provider of security solutions to the federal government.

Northrop Grumman appreciates the opportunity to advise NIST on topics for research and development priorities in anticipation of the President's Wireless Innovation (WIN) Fund. Our team is prepared to assist NIST, public safety organizations, and industry in overcoming the difficult barriers to success that may delay or even stop the progress of the PSBN.

Adaptability and Resiliency

Public safety agencies rely on their networks to provide them critical information and communications under any conditions. Adaptability of the user equipment and the network will provide flexibility to continue communications when changes occur.

Adaptability via Interoperability

Significant user equipment adaptability can be provided through the ability to interoperate between the PSBN and commercial carriers. This scenario will be particularly important during the PSBN build out, where coverage gaps will be common. By adopting LTE as the standard for the PSBN and aligning the solution with the commercially chosen standard, the capability to utilize commercially available wireless systems will be critical to early success of the PSBN. However, coverage associated with commercial LTE deployments is far from ubiquitous and is still in the early roll-out phases. In the interest of maximizing usability and

adaptability, exploring interoperability through the use of alternate commercially deployed technologies, such as 3G, is warranted.

As part of the interoperability investigation, and as discussed to some extent later in this document, investigation will need to encompass the differences in, or lack thereof, Quality of Service implementations and the associated user experience/performance expectations, device, backhaul, and core security profiles and associated opportunities for cyber attacks, and the impact of billing on public safety budgets.

Adaptability via Design

The PSBN should be designed with the flexibility to adapt. The ability to quickly add temporary capacity, designed layers of redundancy and failover mechanisms, the ability to perform emergency changes to network parameters, and clear procedures to do these tasks are recommended. The LTE standard provides many of these features, such as cell-on-wheels for additional temporary capacity and the ability of enhanced Node Bs (LTE base stations) to connect to multiple gateways. However, the processes to do so in an interoperable multi-jurisdictional environment need to be determined.

Resiliency via Survivable Core

A fundamental component of adaptability is the ability to continue providing service during failures. From cyber attacks to natural disasters, critical central system components can be taken offline, impacting the ability to communicate and ultimately crippling emergency operations. As a fail-safe mechanism, a survivable core of essential infrastructure should be developed. This core needs to provide "a small, rigorously isolated set of very basic capabilities that can be relied on"[1] Investigations into what these basic capabilities are and how to provide

[1] President's Council of Advisors on Science and Technology, Report to the President and Congress (Dec. 2010) (*http://www.whitehouse.gov/sites/default/files/microsites/ostp/pcast-nitrd-report-2010.pdf*), pp. 55–56.

them is strongly recommended.

There are several approaches to providing a survivable core. One approach is to build and maintain a backup core that is a separate system of core equipment independent of the operational core. In the event of a core failure, or, as an example, the need to quarantine the core due to a cyber infiltration, the separate core would be brought on-line to provide minimum interfacing and functionality. A separate survivable core has the advantage of being independent of the operational network and would not be immediately affected by failures. As with any backup system, detailed failover procedural steps must be developed and the process must be exercised regularly in order to assure that it operates when needed. Also, if the operational core is brought down by a cyber attack, the backup core once added could also be susceptible to the same attacks unless appropriate isolation is provided. The investigation related to using multiple vendors and different implementations for a stand-alone core is strongly suggested (diversity). By having different providers, exploits in one solution may potentially be avoided by another. Northrop Grumman also recommends investigating what components of the survivable core would require synchronization with live data (e.g. authentication) and the means to achieve this while mitigating risks from cyber threats. Northrop Grumman has extensive experience with large, multi-vendor systems and can provide guidance in this area.

Another approach is to provide redundancy within the operational core. By distributing key functions throughout the network, a successful cyber attack can be mitigated by removing only the affected section of the network and still maintaining operational effectiveness. As discussed with an independent, off-line core, using open standards and various vendors can aid in protecting against exploits at the expense of operational complexity. Northrop Grumman believes that having these distributed, secure, operational cores is the most effective way to provide continuing service to users. Investigation on how to provide this across jurisdictions is

an area for study.

Resiliency – Modeling, Simulation, and Design Patterns

As stated by NIST, resiliency refers to the ability of operable systems to recover from mishap, change, misfortune, or variation in mission or operating requirements. A highly resilient system is essential given the unknown and unexpected nature of emergencies. The PSBN system may potentially be exposed to conditions beyond design specifications in ways that cannot easily be foreseen. How a system degrades, fails, and recovers is determined by the technical design as well as human and operational factors. On the technical front, resiliency is achieved with conservative and robust designs, diversity, simplicity, and systems that can be extended or augmented. With respect to the human / operational aspect, well trained personnel and well established Standard Operating Procedures (SOP) form the necessary foundation for a quick and successful recovery. At the intersection of these two domains lies the simplicity of the system; the simpler the system, the easier it is for the personnel to repair, replace, and return it to operational status. The following are a set of topics related to resiliency that should be studied:

- Design Margins and Robust Design Methods – Use of generous de-rating factors and safety margins minimize the likelihood of permanent damage and facilitate recovery operations. Many assumptions are made in the design of large complex systems and many attempts are made to optimize the design for performance and/or cost. During the design phase, care must be taken to ensure that the system retains graceful degradation characteristics. Careful modeling and simulation of the system must be performed to characterize system performance over a broad set of conditions and identify design limitations and weak links. These limitations can then either be mitigated or removed completely prior to implementation. Designs must also take into account the accumulation of margins to over-engineering solutions that could

challenge cost efficiency.

- Diversity – This includes path diversity, design diversity, and supplier diversity (another reason for open interfaces and open standards). In this context, an example would be mesh technology. Mesh technology employs path diversity to avoid nodes becoming isolated from the rest of the network. Mesh technology has a potential role at the edge/user device level as a capability that provides a localized meshed WiFi (IEEE 802.11s or similar) coverage. This would enable communication within a localized area with a potential gateway back to the extended network if a mesh node also had a cellular link.
- Simplicity – Simplicity pays off in a number of ways. The simpler a design is, the easier it is to analyze and understand its behavior in stressful and degraded conditions. The simpler a system is, the easier it is to test, operate, and repair.
- Extensibility - The ability to deploy additional infrastructure when the existing infrastructure has been devastated by an incident provides a direct and quick path to recovery. As an example, a portable cellular base station with a generator set and a SATCOM terminal provides a quick reaction communication solution that connects the incident to local, regional, or national resources.

Prioritization and Quality of Service

A nationwide public safety broadband network must support prioritization and quality of service (QoS) to give public safety agencies the capability to prioritize network resources based on factors important to their mission operations. This required support must further have the appropriate configuration, management, and dynamic controls and interfaces necessary to ensure that user traffic flows of critical information related to a time-sensitive emergency event are prioritized. Further, this prioritization must not only be isolated to the last mile services

associated with a given solution but extend from the user device to the command and control entity requiring the information.

Thus, the need to establish priorities based on the application, agency, and responder roles especially when disaster strikes becomes even greater as first responders use a multitude of broadband devices that may attach to various technologies at the advent of the PBSN, and run applications with varied bandwidth demands and latency requirements over multiple sub-networks.

Recent LTE network test results[2] released by a regional public safety agency showed that within the currently allocated 10MHz broadband spectrum at 700 MHz the network can become overloaded. A typical incidence scene will comprise a multitude of first responders with the need for enhanced situational awareness prompting increased need for high bandwidth applications. Without optimal prioritization and QoS mechanisms, the mission-critical needs of public safety will not be fully addressed. Additional research and development (R&D) work is required to investigate methods and solutions that prioritize resource allocation and optimize QoS during emergencies when the need for resources is the greatest.

Prioritization and QoS are two network access control and resource allocation mechanisms that previous 3GPP standards and legacy public safety communications systems did not adequately address. However, LTE supports both prioritization (with pre-emption) and QoS to enable public safety first responders to receive preferential treatment in the access and use of network resources based on their roles, applications type, end-user device type, geographic location where the request was initiated, and whether the user is on home network or roaming. Implementation of LTE QoS and Priority features (such as ARP, QCI, etc) as defined in 3GPP Release 8 and above, will enable optimal network resource allocation that should strongly

[2] http://urgentcomm.com/networks_and_systems/mag/bay-area-network-test-201107/

enhance the availability and reliability of public safety communications networks in meeting first responders' mission needs. As Prioritization and QoS functionalities in commercial carrier-grade LTE networks are typically not tuned to public safety applications and incidence scenarios, there is a need to expand on the basic implementation of the Prioritization and QoS specifications to address stringent public safety performance requirements. To this end, Northrop Grumman applauds the on-going work by the NIST led QoS Working Group in determining additional methodologies and processes for mapping QoS and prioritization parameters to first responder use case scenarios.

Because the nationwide PSBN may comprise an interconnection of regional LTE networks, each with local control on users and applications prioritization, there is a need to provide a framework for implementing Prioritization and QoS across jurisdictional network entities so as to achieve interoperability especially when first responders roam out of their home networks. The implementation framework should provide enough flexibility for the jurisdictions to "localize" their Prioritization and QoS policies commensurate with their network operational objectives. In defining the requirements for implementing priority rules, Northrop Grumman recommends that more work be performed towards understanding sustainable and efficient methods of network resource allocation and pre-emption that can evolve as public safety applications and user requirements continue to evolve as well.

Although 3GPP Release 8 provides a list of attributes such as bandwidth, packet latency, and packet loss that are used to derive optimal QoS parameter settings for various mixes of end-user applications, there are no real world results of optimal QoS parameter settings for incidence scenarios with varying network conditions. Thus, the NIST-PSCR lab-based Public Safety LTE Demonstration Network needs to be replicated in other environments to enable additional tests and optimization of the QoS parameters under extreme conditions of mixed user traffic demand

and network loading. This will help in optimizing the LTE network deployment architecture and parameter settings for various environments and diverse first responder use cases.

QoS and Network Security

Northrop Grumman has observed through performing network security operations on a broad range of mission critical networks that certain types of attacks on network security have significant effect on application performance and QoS. However, it is the mission of QoS to ensure application performance and therefore, the two are inextricably linked. For example, both security and QoS can utilize common access control lists (ACL) for rules on how to treat traffic. Thus, a security mechanism that discovers abnormal traffic patterns could alert a QoS system to treat that traffic according to those rules. Furthermore, incorporating QoS within the network security policies will strengthen the public safety network against potential cyber attacks. Northrop Grumman recommends that additional R&D be directed towards integrating QoS and Security policies and automation to enhance and simplify the implementation of policy-based rules to securely manage network behavior. In order to ensure security across the entire segment of the PSBN, user and signaling data are traditionally protected in ways that may not enable granular QoS provisioning. Northrop Grumman is currently leading the PSBN Network Security working group and recommends a joint effort with the PSBN Prioritization and QoS working group to define a more inclusive framework for performing prioritization and QoS when end-to-end security is enabled. This way, the nationwide PSBN will more efficiently serve the mission-critical communication needs of first responders in a highly secure environment.

Network Security

Security of broadband wireless communications is vitally important to public safety and must be approached in a holistic manner to address the public safety's fundamental mission of protecting property and saving lives. As is noted in the NIST's request, Access Control List

(ACL) provides control over network resources by limiting access only to authorized users. Although ACL is an important element of network security, it, however, represents only one aspect of network security. Other equally significant aspects of network security include a comprehensive network wide identity management scheme for user authentication, standards for protecting the end-to-end privacy and integrity of user information as it traverses different parts of the network , technology and associated security policies and procedures for protecting the network from cyber attacks, and physical security of the network assets such as communication towers, Network Operations Centers and Security Operations Centers. Although many of these security aspects fall outside of LTE specifications, they are critically important to public safety's mission and Northrop Grumman strongly recommends that NIST take an active role in promoting research and developing standards for them. Northrop Grumman also realizes that network security has an important bearing on network availability, a key requirement for first responders who rely on the 24x7 availability of the communications to carry out their mission. Weak and compromised network security reduces network reliability and hence network availability. Without the proper security measures in place no amount of reliability features, such as site hardening and backup power, can assure the highest degree of availability required of the public safety communications networks.

Northrop Grumman also notes that the use of globally deployed standards such as the Internet Protocol (IP) that form the core of an LTE network helps achieve the important goal of interoperability. However, it also significantly increases the vulnerability of the public safety networks to malicious cyber attacks, further underscoring the need for research in robust security mechanisms to protect these mission-critical networks. It is also important to note that a security feature important to public safety may be specified in the standard but may never be implemented because the commercial carriers that drive the infrastructure market may not have a

need for that feature. To the extent that the LTE standard or its implementation does not address the security and requirements of public safety emergency communications, there is a need to research, develop, and integrate additional security features so that the security requirements of public safety are fully met.

An important consideration related to network security is the potential use of the nationwide PSBN by the federal government users. During an emergency event, multiple agencies from all levels of government including federal, state, and local will need to communicate and share information with each other in order to mount an effective and coordinated response. Such users introduce new security requirements, as the federal government follows its own standards and guidelines for exchanging and securing information as codified in the Federal Information Processing Standards (FIPS)[3]. FIPS 140-2 is a NIST standard that specifies security requirements for cryptographic modules within a security system protecting sensitive but unclassified information. Because LTE's encryption schemes do not adhere to these standards in all cases, FIPS validated and certified solutions will need to be integrated with the public safety network in order to meet the government requirements for secure communications.

An important challenge for the PSBN lies in integrating the various solutions, each addressing a different requirement of network security, into a cohesive and comprehensive security architecture – an architecture that is scalable and flexible to meet public safety security requirements as they evolve over time. While the details of the overall architecture of the nationwide PSBN are still being worked at the standard bodies, Northrop Grumman recommends that to a public safety user, the PSBN appears as one single network – a seamless public safety

[3] Federal Information Processing Standards (FIPS) are standards and guidelines for information processing issued by National Institute of Standards and Technology (NIST) for use government-wide. NIST develops FIPS when there are compelling Federal government requirements such as for security and interoperability and there are no acceptable industry standards or solutions.

enterprise network – that provides secure and interoperable communications capability regardless of the user's geographical location on the network.

Based on Northrop Grumman's R&D activities in the area of wireless security, participation in public safety organizations and user groups such as National Public Safety Telecommunications Council, and interactions with the public safety community we recommend that the NIST provides its support to research in the following security related areas:

- A Nationwide Identity Management Scheme – Network users should be identified on the network via common industry mechanisms (such as SIM cards), with extensions for further identification details. By using a common format nationwide users can be treated by the system across the entirety of the network as verified users, and the system can make decisions about security, QoS, and access in a straightforward process. Each jurisdiction or agency will then be responsible to connect their existing enterprise to the LTE network using a clearly defined interface for identity and credentialing. Without this mechanism in place it is hard to see how a truly nationwide interoperable network can be created.
- Role and Context based Access Control Schemes – Access Control Schemes exercise control over access to the network resources after the user identity has been authenticated by the network. Examples of network resources include bandwidth, classes of service, QoS, applications, and databases of information. In the public safety domain user role is typically used to determine access to various resources. As an example, an explosives expert at an incident scene involving a live bomb may be accorded higher priority and therefore a higher class of service and more bandwidth than a crime scene investigator; and information accessible to emergency medical

personnel may not be made accessible to law enforcement officials. Context based access control schemes become important when sensitive information is accessible only on a need-to-know basis.

- Integrated Security Architecture for the Nationwide Network – Northrop Grumman recommends that research in this area should be premised on treating the nationwide PSBN logically as a single public safety enterprise network. Research is required in developing a comprehensive security architecture for this public safety enterprise network that incorporate the best-in-class solutions for the various security components discussed above such as identity management, access control schemes, end-to-end privacy and integrity of user communications, device security, and tools for mitigating cyber security threats. This will also involve conducting a detailed gap analysis between public safety requirements for security and LTE security specifications

Public safety communications networks are vital to the safety, security, and well being of the country and must be secured and safeguarded with the same heightened level of importance as any other critical infrastructure. As is well known, malicious attacks on our critical information and communication networks, also known as cyber attacks have increased significantly in the past few years and they continue to grow in scope, complexity, and sophistication. The need for increased cyber vigilance has never been greater. Increasing network connectivity and interoperability improves information sharing and enhances situational awareness, but it also increases the vulnerability of these networks to externally mounted attacks. A large scale denial of service attack on the public safety communications networks just when it is needed the most during a crisis could have a crippling effect on the mission of our first responders. These networks needs

to be strongly safeguarded and proactively monitored in an end-to-end fashion to avert casual as well as advanced persistent threats.

Network Sharing

Shared use of network infrastructure between commercial and public safety users has been proposed as a cost-effective way to build the broadband network infrastructure for public safety. Adoption of the same broadband technology standard (LTE) by both public safety and large commercial wireless carriers creates significant opportunities for infrastructure sharing. Opportunities for sharing include radio communication tower facilities and equipment including shelter, power, coaxial cables and antennas, the LTE core network, and backhaul. Sharing of some of the RF equipment such as antennas and cables is possible because both public safety and commercial carriers are using frequencies in the same 700 MHz frequency band.

The cost savings resulting from infrastructure sharing may be especially significant for rural jurisdictions that may not have access to adequate funds to build enough number of sites required to meet the coverage and capacity requirements of public safety. A sound and well executed public-private partnership model could address some of the funding challenges. Commercial carriers could be incentivized to enter into a partnership with public safety by allowing them access to public safety spectrum on a secondary basis. In addition, they could also be financially compensated for the shared use of their network infrastructure. The FCC released a technical paper[4] in May 2010 under the Omnibus Broadband Initiative where they explained how public safety agencies can leverage the deployment of 4G commercial wireless networks to greatly reduce the overall costs of constructing a nationwide broadband network. The paper developed a cost model that estimated the capital cost of public safety broadband network build to be about $6.5 billion under the public-private partnership model compared to $15.7 billion for

[4] A Broadband Network Cost Model: Basis for public finding essential to bringing nationwide interoperable communications to America's first responders OBI Technical Paper No. 2

a stand-alone network.

While Northrop Grumman realizes the significance of cost savings that result from network sharing with commercial carriers, we are also cognizant of the fundamental differences that exist between the public safety and commercial carrier requirements with respect to network availability, security, QoS, and user priority and preemption. Network infrastructure sharing must not compromise any of the key requirements related to the safety and security of public safety's mission. A public-private partnership will need to address the technical, logistical, and administrative issues as well as the cost implications of addressing any differences that exist between commercial and public safety requirements. Network infrastructure sharing requires investigation of how to reconcile commercial and pubic safety's requirements differences in areas including RF site hardening, core network resiliency and survivability, backhaul network redundancy, and security architecture. Additionally, investigation is required in administrative, procedural, and technical controls needed to preempt commercial users from public safety spectrum during emergency incidents in case the public safety spectrum is being shared by commercial carriers. Sharing of core infrastructure would also require solutions to separate sensitive public safety communications from commercial user traffic to ensure the security of public safety communications. Administrative arrangements and technical controls would also be needed to facilitate roaming of commercial users on public safety network and vice versa. Increased maintenance and stronger physical security of shared network assets would also have to be addressed.

Northrop Grumman recommends NIST to support research in the areas outlined above to ensure the overall reliability and availability of public safety network in a shared network infrastructure environment. Sharing of network infrastructure between public safety and commercial users is an economically attractive concept that could be viable provided strong

measures are taken to ensure the key requirements of public safety's mission are not compromised in any manner.

Scalability

The architecture of the PSBN, although not yet finalized, is envisioned to be a network of networks where individual jurisdictional networks will be interconnected via a public safety enterprise network to create a nationwide interoperable broadband network. It is only reasonable to expect that the usage, and consequently the traffic, over the public safety network will increase over time as more agencies and public safety users connect to the public safety network to realize the benefits of broadband wireless for their mission.

The network and the underlying technologies need to be scalable in order to accommodate this growth in a graceful and cost-effective manner. All interfaces between the various network elements of LTE are based on Internet Protocol (IP) technology which has proven to be a very scalable and robust technology as demonstrated by the explosive growth in Internet and its use over the last two decades. However, not just the network interfaces but also the individual components of the LTE network must be able to scale with demand without requiring expensive hardware replacements. Hardware architecture should be modular and flexible enough to handle higher capacity demands simply through the addition of new cards to the existing hardware. Software should automatically reconfigure itself to accommodate the new cards.

The requirement for scalability, however, needs to be balanced against advances in technology. Mobile broadband technology will continue to advance at a fast pace to satisfy the user demand for better and faster networks and a point in time will arrive in the future where it will simply not be possible to meet the processing demands of the new technology with existing hardware and software. It is desirable, however, to optimize the lifespan of the hardware and

software by incorporating architectural principles that anticipate both the technology advances and the growth in user demand to the extent possible. A hardware platform that is build purposefully and optimized for a specific technology runs the risk of becoming obsolete quickly as the technology advances. This is particularly true in the mobile wireless industry where the air interface standards have gone through complete revisions several times in the past, from Time Division Multiple Access based GSM technology to Code Division Multiple Access based UMTS technology to the current Orthogonal Frequency Division based LTE technology. This technology progression has required the wireless carriers to go through expensive hardware and software upgrades prompting a need for a solution that addresses the challenge of hardware obsolescence. Advances in Software Defined Radio (SDR) technology may eventually provide a viable solution to this issue. Performing most of the signal processing tasks in software running on general purpose computing platform rather than specially designed hardware is the fundamental principle of the SDR technology and a key to increasing the scalability and longevity of the network components while keeping pace with technology changes. Northrop Grumman conducts research and provides expertise to the US government in the area of digital signal processing and SDR technology and recommends that NIST support a research program in this area to reduce the risk of hardware obsolescence with technology advancement.

Another issue with regards to the scalability of the network is its ability to handle unpredictable surges in network traffic when an emergency incidence occurs in a limited geographical area. The localized nature of the incidence coupled with lower site count due to superior propagation characteristics of the 700 MHz frequency band relative to other higher frequencies such as 2.5 GHz and 1.9 GHz implies that the incident area will likely be served by the combined capacity of a small number of sites. Enough capacity needs to be available in the sites serving the incident scene to meet the communication requirements of hundreds, if not

thousands, of first responders. However, for a given technology the available capacity is limited by the amount of available spectrum. For public safety, this currently stands at10 MHz in the 700 MHz band but may increase to 20 MHz depending on the legislative outcome of the D-block reallocation. Studies conducted by various public safety organizations including NPSTC have indicated that 10 MHz of spectrum may not provide adequate capacity to meet the public safety demands for data and video during a crisis situation. However, these studies are based on certain assumptions about the traffic requirements during an emergency situation. While traffic patterns for commercial networks have been extensively studied and analyzed and traffic models have been developed to help the carriers proactively plan for surges in traffic demands, such models are lacking for public safety. Northrop Grumman strongly recommends that NIST support research in developing scenario based simulation models of public safety network traffic that can be used by public safety to accurately forecast and proactively plan for capacity upgrades and technology enhancements to accommodate future growth.

Northrop Grumman has done some pioneering work in developing traffic models for public safety that have been used in public safety and Northrop Grumman responses to FCC's requests for comments and strongly recommends that NIST support research activity in this very important area.

The ability of various network hardware and software components to scale is extremely important for public safety to manage the inevitable growth in user demand in a cost effective manner. Also, given the mission-critical nature of the network, it is equally important to be able to forecast future capacity requirements with a reasonable degree of accuracy to ensure that adequate network capacity is available during emergency situations when it is needed the most.

Conclusion

Northrop Grumman supports NIST's efforts to engage with a wide range of different

types of users, industry participants, and academic organizations. Industry investments, combined with government R&D investment (such as the future WIN Fund), and through cooperation with major Universities, provide the basis for solving many of the serious challenges to the future the PSBN as articulated in this response. In this document we concentrated on responses from the four overarching themes presented, specifically adaptability and resiliency ("resiliency in an emergency"), prioritization and quality of service ("reliability and availability"), network security and strong dynamic access control ("security"), and network sharing and scalability ("affordability/commercial alignment"). We look forward to the opportunity in the future to partner with NIST and others in the industry to solve some of these key issues for purposes of creating a truly secure, operable, public safety broadband network that transforms the future operations of our first responders and other government agencies.