THE PRESIDENT'S
NATIONAL SECURITY TELECOMMUNICATIONS
ADVISORY COMMITTEE

NSTAC Report to the President on the National Security and Emergency Preparedness Implications of a Nationwide Public Safety Broadband Network

May 22, 2013

TABLE OF CONTENTS

EXECUTIVE SUMMARY

In 2011, the National Security Staff (NSS), Executive Office of the President (EOP), asked the President's National Security Telecommunications Advisory Committee (NSTAC) to examine the national security and emergency preparedness (NS/EP) implications of a nationwide public safety broadband network (NPSBN). During the course of the NSTAC's scoping work, Congress passed Public Law (P.L.) 112-96, *The Middle Class Tax Relief and Job Creation Act of 2012*; Title VI, *Public Safety Communications and Electromagnetic Spectrum Auctions,* of the law authorizes funding and establishes a governance structure for the NPSBN. The NSTAC examined the new law, as well as a variety of related policy documents, and determined that the legislation would guide efforts to develop and deploy the NPSBN, but the Act did not directly address how the network would impact NS/EP communications now and in the future.

The NPSBN is the first effort to create a nationwide, standardized, private network with dedicated spectrum to provide public safety access to advanced broadband communications. Once deployed, the NPSBN will enable public safety communications to leverage commercial broadband standards, technologies, devices, and innovations. The NPSBN will also connect to commercial networks and the Internet.[1] Underlying this network will be next generation network (NGN) infrastructure that is converging to packet-switching technology for all forms of communication. Until recently, NS/EP and public safety users have not been able to significantly leverage Internet protocol (IP)-based applications technologies and services. The ability of public safety communications to leverage commercial innovation and traverse commercial networks presents a near-term imperative, and offers a strategic opportunity that could benefit both NS/EP and public safety communications.

NS/EP and public safety missions are complementary, and, at times, fully integrated when events escalate in significance. Users supporting both missions are planning for advanced IP-based communications capabilities to support their missions and often have similar requirements—for example, reliability, resiliency, security, and priority—that exceed those of commercial customers. NS/EP and public safety users should coordinate communications requirements to help meet their unique needs, improve interoperability, achieve economies of scale, and enable innovation to more effectively and efficiently fulfill their missions.

NS/EP and public safety users have historically had distinct forums for collaborating, developing, and prioritizing requirements. Just as there is a wide diversity of Federal NS/EP and Federal public safety communications users, there is, and will continue to be, a diverse set of organizations that represent their respective communications and policy interests. There are a significant number and variety of stakeholders and organizations from different geographies and at various levels of government, including the NS/EP Communications Executive Committee; the Emergency Communications Preparedness Center; the Department of Homeland Security's (DHS) emergency communications program SAFECOM; the Public Safety Advisory Committee; State and local government agencies and officials; the National Governors Association; and the National Public Safety Telecommunications Council. These stakeholders and organizations represent similar but not fully aligned interests in NS/EP or public safety communications. An opportunity exists to better organize within the Federal

[1] P.L. 112-96 § 6202 (b)(1)(B)(ii).

Government and incent coordination across the diverse set of stakeholders to take advantage of synergies and realize greater benefit from the NGN investments made across levels of government.

Coordination is particularly important in seeking to provide end-to-end priority communications for users across levels of government and networks. Priority communications services help ensure that NS/EP and public safety users have continuous communications to fulfill their respective missions when networks are congested or degraded. While this critical requirement has historically focused on voice communications, the need for reliable and prioritized data, image, video, and various other multimedia applications is increasing. Coordination of priority requirements will help ensure that the communications needs of diverse NS/EP and public safety users can be met as their services traverse various networks.

The development of the NPSBN creates an unprecedented opportunity to coordinate and align policies, requirements, and standards in order to enable innovation, create economies of scale, and ensure that both NS/EP and public safety users' unique communications requirements can be met. To fulfill this opportunity, the NSTAC recommends implementing a series of recommendations in the near-, mid-, and long-term. Near-term actions will help ensure that communications standards, technologies, and devices are interoperable, and will drive recognition of shared interests. In the mid- and longer-term, clarifying NS/EP policies and aligning NS/EP and public safety policies will enhance the abilities of NS/EP and public safety users to work together effectively and efficiently to serve the Nation's interests. If NS/EP and public safety stakeholders do not take advantage of this timely opportunity, achieving mutual benefits will be difficult and there will be an inevitable negative impact on NS/EP and public safety users' ability to fulfill their respective missions in the long-term.

The NSTAC recommends that the President advance recommendations that rationalize NS/EP and public safety **organizations and functions**, update and align **policies**, direct **technical initiatives**, require **reporting** to facilitate implementation, and address **funding** gaps. Specifically, the President should focus on the following areas and actions:

1. **Organizational Roles, Responsibilities, and Relationships.** Direct the NSS to evaluate and, as needed, recommend statutory or other policy improvements to functionally align and streamline Federal NS/EP and Federal public safety NGN communications organizations, and their responsibilities and functions. This alignment should be broadly focused across the Federal Government, but exclude independent authorities such as the Federal Communications Commission (FCC) and the First Responder Network Authority (FirstNet) Board. The evaluation and recommendations are intended to institutionalize coordination, improve mission effectiveness, and optimize the use of scarce resources for both NS/EP and public safety communications. The NSS should:

    a. Be informed by stakeholders through outreach and partnerships.

    b. Ensure that stakeholders include representatives from Federal, State, local, territorial, and tribal public safety organizations, service providers, product vendors, and other entities with relevant NS/EP and/or public safety communications expertise and knowledge.

    c. Establish a process enabling stakeholders to participate in or advise, as appropriate, the resulting functionally aligned and streamlined organization(s) so that NS/EP and State, local, territorial, and tribal public safety communications can complement each other as circumstances evolve.

d. Examine and make recommendations to ensure that the NSTAC membership and functions represent the full range of industry knowledge and expertise of NS/EP and public safety communications to provide the President with advice to ensure communications at all times and under all circumstances.

2. **Policy Changes.** Direct the organization(s) with the appropriate responsibilities and functions identified as a result of Recommendation 1 to lead a cross-governmental, public-private, integrated effort to: (1) update NS/EP policies; and (2) align Federal NS/EP and Federal public safety communications policies, requirements, and standards to ensure that the interests of the Nation are best served. The alignment must support the ability of all stakeholders to coordinate and execute their NS/EP and public safety missions consistent with the National Incident Management System. To further this goal, direct the new organization(s), including stakeholders listed in Recommendation 1, to propose updates to overarching NS/EP policies, including the definition of NS/EP communications, the definition of NS/EP, and the mission and composition of NS/EP relative to public safety. As appropriate, make associated legislative and regulatory recommendations to:

   a. Reconcile priority communications policies and regulations (e.g., *FCC Second Report and Order providing Establishment of Rules and Requirements for Priority Access Service*) to account for and enable priority on all data types (e.g., voice, video, data) for NS/EP and public safety communications on commercial networks.

   b. Update national strategies (such as the *National Response Framework* and the *National Emergency Communications Plan*) and initiatives to account for advanced NGN communications capabilities, such as the NPSBN, and to reflect the evolving communications environment.

3. **Technology Initiatives.** Direct the organization(s) with the appropriate responsibilities and functions identified as a result of Recommendation 1 to lead a cross-governmental, public-private, integrated effort to:

   a. Identify similarities and differences in NS/EP and public safety NGN communications requirements, including those needed to meet "unique homeland security or national security needs" as required by Section 6206 (b)(2)(D) of P.L. 112-96 and in accordance with Section 3.3(a) of E.O. 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*.

   b. Review and recommend updates to priority schemas to account for and enable priority on all forms of NGN communications (e.g., voice, video, data) for NS/EP and public safety communications on commercial networks.

   c. Identify and recommend standards to meet requirements resulting from Recommendations 2 and 3(a).

   d. Identify and recommend opportunities for coordination and collaboration of research and development activities, grants, funding, pilots, and new standards that promote innovation to close the gap between commercial marketplace requirements and NS/EP and public safety requirements.

4. **Reporting Requirements.** Direct the NS/EP Communications Executive Committee, established by E.O. 13618, or its successor, to provide a status of the implementation of Recommendations 1, 2, and 3 above as part of the reporting requirements created in E.O. 13618, Section 3.3.

   a. Within six months, identify additional required tasks and develop and document a plan with milestones for addressing these tasks. Report these tasks and progress against milestones as part of the quarterly updates.

   b. Document tasks, milestones, and funding as part of the annual NS/EP communications strategic agenda.

   c. Distribute the quarterly updates and annual strategic agenda to the NSTAC chair to inform the NSTAC's ability to meet the functions defined in E.O. 12382, *President's National Security Advisory Committee.*

5. **Funding.** Request that Congress fully fund DHS' NGN priority service program(s) to ensure that advanced broadband communications priority services are fully developed, implemented, and operational before legacy priority systems are unable to support mission requirements.

1.0 INTRODUCTION

Public safety stakeholders, including Federal, State, local, territorial, and tribal emergency response personnel, realized a significant milestone toward addressing their needs for advanced Internet protocol (IP)-based broadband communications capabilities with the enactment of Public Law (P.L.) 112-96, the *Middle Class Tax Relief and Job Creation Act of 2012*, in February 2012. Title VI, *Public Safety Communications and Electromagnetic Spectrum Auctions*, of the law includes provisions to fund and govern a nationwide public safety broadband network (NPSBN) to provide a secure, reliable, and dedicated interoperable communications network for public safety users.

The NPSBN is the first effort to create a nationwide, standardized, private network with dedicated spectrum to provide public safety access to advanced broadband communications. Once deployed, it will provide public safety users the ability to leverage and build upon commercial broadband standards, technologies, networks, devices, and innovation. The NPSBN will also enable public safety communications to significantly leverage IP-based next generation networks (NGN) and technologies. The President's National Security Telecommunications Advisory Committee (NSTAC) has reported on the potential advantages and important considerations of NGN for national security and emergency preparedness (NS/EP) communications numerous times and has made recommendations to the President regarding steps that should be taken to meet NS/EP NGN user requirements.[2]

1.1 Scoping and Charge

In 2011, the National Security Staff (NSS), Executive Office of the President (EOP), requested that the NSTAC examine the then-proposed NPSBN to assist the Government's planning efforts. After preliminary scoping activities, the NSTAC determined that it would be appropriate to investigate the NS/EP implications of the network. During the scoping phase, the NSTAC met with Federal, State, and local officials, and representatives from non-governmental organizations (NGO), industry, and jurisdictions that were early adopters of broadband technologies. The NSTAC also began investigating current and emerging broadband capabilities that could be used to support NS/EP and public safety users as they execute their respective missions.

Coincident with the ongoing scoping work of the NSTAC, Congress passed P.L. 112-96 on February 22, 2012. After examining Title VI of P.L. 112-96 and a variety of related policy documents, the NSTAC determined that while the legislation would guide efforts to develop and deploy the NPSBN, it did not directly address how the network would impact NS/EP communications now and in the future. Given the critical responsibilities of Federal, State, local, territorial, and tribal officials in significant NS/EP events, the NSTAC decided to examine NS/EP policy implications that may arise from or be catalyzed by the NPSBN.[3] Through its examination, the NSTAC also recognized that the NPSBN is bringing public safety communications into a complex, converged IP communications environment. In May 2012, the NSTAC concluded its scoping effort by developing the following questions for further examination:

[2] Appendix E: Previous NSTAC Findings and Recommendations.

[3] Appendix F: NS/EP Policy Matrix.

1) What NS/EP policy changes should be considered to:
   a. Facilitate priority access that may be required across the diverse community of potential NPSBN users (Federal, State, local, tribal, and secondary users), particularly during NS/EP situations (e.g., emergencies and special events)?
   b. Support NPSBN access, interoperability, security, reliability, and resiliency?
   c. Help ensure the deployment and evolution of the NPSBN in a manner that accounts for jurisdictions' diverse capabilities, while helping to ensure scalability to the national level?
2) What policy changes should be considered that encourage the innovative evolution of NS/EP functions by or through the NPSBN?

The purpose of this report is to make recommendations to the President on policy changes to support priority, interoperability, security, reliability, resiliency, and scalability for NS/EP and public safety communications, and to enable continual evolution of communications capabilities for them in IP-based broadband networks, such as the NPSBN.

In this examination, the NSTAC addresses the potential implications of the NPSBN for NS/EP communications and opportunities to advance both NS/EP and public safety communications.

2.0 COMMUNICATIONS ENVIRONMENT

Today's consumers, whether individual or enterprise, enjoy rich, seamless experiences enabled by an expanding variety of voice, image, video, and data services. These services are made possible through access to nearly ubiquitous broadband infrastructure and cloud-based services. Consumers often access these services remotely via mobile devices (e.g., smart phones and tablets) using sophisticated mobile applications. Personal devices are increasingly being used for professional activities, a trend often referred to as "bring your own device." Moreover, some communications do not involve users, as machine-to-machine transmissions are already common.

Underlying these rapidly evolving services are wireline and wireless NGN and infrastructure that are converging to packet-switching technology for all forms of communication. For the purposes of this report, the term "advanced communications" refers to IP-based broadband wireline and wireless networks, technologies, applications, and services. The volume of network traffic being created by advanced communications is dramatic and only continues to grow. Whether employed for personal use or in support of commercial and government enterprise needs, advanced communications require a significant and growing amount of capacity on commercial, high-speed broadband networks. As a result, data usage is increasing exponentially. For example, global mobile data traffic grew 70 percent in 2012 and video traffic exceeded 50 percent of all mobile data traffic for the first time in 2012. Experts forecast that the fourth generation of mobile communications technology standards (4G) will support 10 percent of connections, but account for 45 percent of total traffic by 2017.[4]

[4] Cisco, Cisco Visual Networking Index: Global Mobile Data Traffic Forecast Update, 2012-2017, February 6, 2013. Available from http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.html.

Until recently, NS/EP and public safety users have not been able to significantly leverage IP-based broadband networks, technologies, applications, and services. Communications for NS/EP and public safety users is discussed in detail in Sections 2.1 and 2.2 respectively. In exploring the potential implications of the NPSBN, the NSTAC received extensive briefings on various advanced communications capabilities that could support both NS/EP and public safety users. For example, the briefers highlighted new form factors (sizes, shapes, configurations, appearance, etc.) and highly resilient devices, changing communication trends (e.g., machine-to-machine communications, collaboration and social networking technologies, cloud computing) and the insights that may be gained through "big data" analyses.[5] The briefers anticipated a future communications environment for NS/EP and public safety users that differs greatly from today.

2.1 NS/EP Communications

The concept of NS/EP communications has existed at least since the creation of the National Communications System (NCS) in 1963. Current Federal law defines NS/EP telecommunications services as "those telecommunication services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international), which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States."[6] In addition, the NS/EP Communications Executive Committee (ExCom), established under E.O. 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, defines NS/EP communications as:

> Primarily those technical capabilities supported by policies and programs that enable the Executive Branch to communicate at all times and under all circumstances to carry out its mission essential functions and to respond to any event or crisis (local, national, or international); to include communicating with itself; the Legislative and Judicial branches; State, territorial, tribal and local governments; private sector entities; as well as the public, allies, and other nations. National security and emergency preparedness communications also include those systems and capabilities at all levels of government and the private sector that are necessary to ensure national security and to effectively manage incidents and emergencies.[7]

NS/EP users range from Federal, State, and local leadership, such as the President of the United States, governors, and mayors, to emergency responders and disaster recovery individuals. The types of events defined as NS/EP events, and the nature of NS/EP communications supporting responses to those events, continue to evolve. According to E.O. 13618, "Survivable, resilient, enduring, and effective communications, both domestic and international, are essential to enable the executive branch to communicate within itself and with: the legislative and judicial branches; State, local, territorial, and tribal governments; private sector entities; and the public, allies, and other nations. Such

[5] Appendix G: Advanced Communications Technologies.

[6] 47 C.F.R. § 201.2 (g).

[7] United States, Executive Office of the President, National Security and Emergency Preparedness Executive Committee, Letter to Mr. Chuck Donnell and attached Memorandum, signed by Mr. Michael Locatis and Ms. Teresa Takai, November 6, 2012. This memorandum provides the ExCom-approved definition of NS/EP communications.

communications must be possible under all circumstances to ensure national security, effectively manage emergencies, and improve national resilience."[8]

While the NS/EP communications mission was originally focused on national security emergencies when the NCS was established, an increase in the frequency and severity of various threats of national significance has resulted in its expansion to include all hazards, under all circumstances, at all times.[9] The increased role for public safety is implicit in this expansion of the NS/EP communications mission.

Past NSTAC studies have highlighted the implications to NS/EP communications as commercial and private networks transition to NGN technologies, including the benefits associated with the use of new voice, data, image, and video applications.[10] In response, DHS and private sector providers and vendors have begun to explore NGN broadband requirements and how such requirements should be incorporated into future priority communications programs.

2.2 Public Safety Communications

Public safety is composed of many entities, including jurisdictions, organizations, individuals, and stakeholders, each requiring communications to fulfill their distinct and often critical missions. First responders are central to public safety and generally include police, firefighters, emergency medical technicians, and other first responders across all levels of government. Public safety users often cross multiple jurisdictions, and numerous public safety entities exist both within and across states; some may be organized by discipline, while others may be organized based on geography. The situation is similar across tribal and territorial areas.

Public safety personnel have unique communications requirements, such as mission critical voice, which differ from those typically provided commercially because of their direct role in saving lives, preventing injury, and limiting property loss. These unique requirements are discussed further in Section 3.2. Public safety communications must interoperate and work with jurisdictions at all levels, from local to national. Public safety briefers consistently highlighted mission critical voice as their most important communications requirement. Public safety users rely on private land mobile radio (LMR) systems to support mission critical voice because neither commercial networks nor current Long Term Evolution (LTE) standards currently support it.[11] Most public safety organizations agree that the NPSBN, which will be based on LTE standards, will augment, not replace, LMR systems for some time. Eventual transition to LTE for voice will depend on the ability of advanced communications technologies to reliably meet mission critical voice

> Public safety officials agree that mission critical voice is their most important communications requirement, and public safety users will continue to use LMR for mission critical voice until LTE technology reliably supports it.

[8] E.O. 13618 § 1.

[9] United States, White House, *National Security Action Memorandum 252 - Establishment of the National Communications System*, July 11, 1963.

[10] Examples are cited in Appendix E: Previous NSTAC Findings and Recommendations, and are available on the NSTAC website: www.dhs.gov/nstac.

[11] LTE is a fourth generation wireless communications standard supporting high-speed data on mobile phones and data terminals.

requirements. Priority communications requirements in support of public safety users are discussed in further detail in Section 4.3.

2.3 The NPSBN

Title VI of *The Middle Class Tax Relief and Job Creation Act of 2012* establishes the First Responder Network Authority (FirstNet) Board, an independent authority within the National Telecommunications and Information Administration (NTIA).[12, 13] The FirstNet Board is charged to take "all actions necessary" to build, deploy, and operate the network, in consultation with Federal, State, tribal, and local public policy entities.[14] P.L. 112-96 authorizes the FirstNet Board to oversee the construction and operation of a nationwide broadband network that "enables police, firefighters, emergency medical technicians, and other first responders to effectively communicate with one another during emergencies and to use new technology to improve response time, keep communities safe, and save lives."[15] When operational, the NPSBN will provide broadband services—data, image and video initially, followed by voice.[16]

In order to ensure technical interoperability, P.L. 112-96 directed the Federal Communications Commission (FCC) to establish a Technical Advisory Board for First Responder Interoperability (Interoperability Board) to recommend minimum technical requirements for the NPSBN. Released in May 2012, the Interoperability Board's report recommended technical requirements or considerations in eight areas to ensure nationwide interoperability for the NPSBN: (1) LTE standards and interfaces; (2) user equipment and device management; (3) testing; (4) network/technology evolution; (5) handover and mobility; (6) grade of service; (7) prioritization and quality of service (QoS); and (8) network security.[17]

The Interoperability Board based its recommendations on commercial LTE standards. Importantly, while LTE standards make available many features, they were not specifically designed for the unique functional requirements of public safety users; LTE standards may require extensions to satisfy certain requirements that may be unique to public safety users. The NPSBN will also need to be designed to meet a different set of performance criteria (e.g., coverage and reliability) than those typical for commercial networks.

P.L. 112-96 states that the NPSBN will be based on a single, national network architecture that evolves with technological advancements. Initially, the network will consist of a core network and radio access networks (RAN), as well as connectivity between those two networks, with the public Internet, and with

[12] P.L. 112-96 § 6204 (a).

[13] Appendix D: Overview of FirstNet.

[14] United States, Department of Commerce, *First Responder Network Authority Fact Sheet*, August 2012. Available from http://www.commerce.gov/news/fact-sheets/2012/08/20/fact-sheet-first-responder-network-authority-firstnet.

[15] FirstNet Board Charter (September 25, 2012, FirstNet Presentation). Available from http://www.ntia.doc.gov/files/ntia/publications/firstnet_fnn_presentation_09-25-2012_final.pdf.

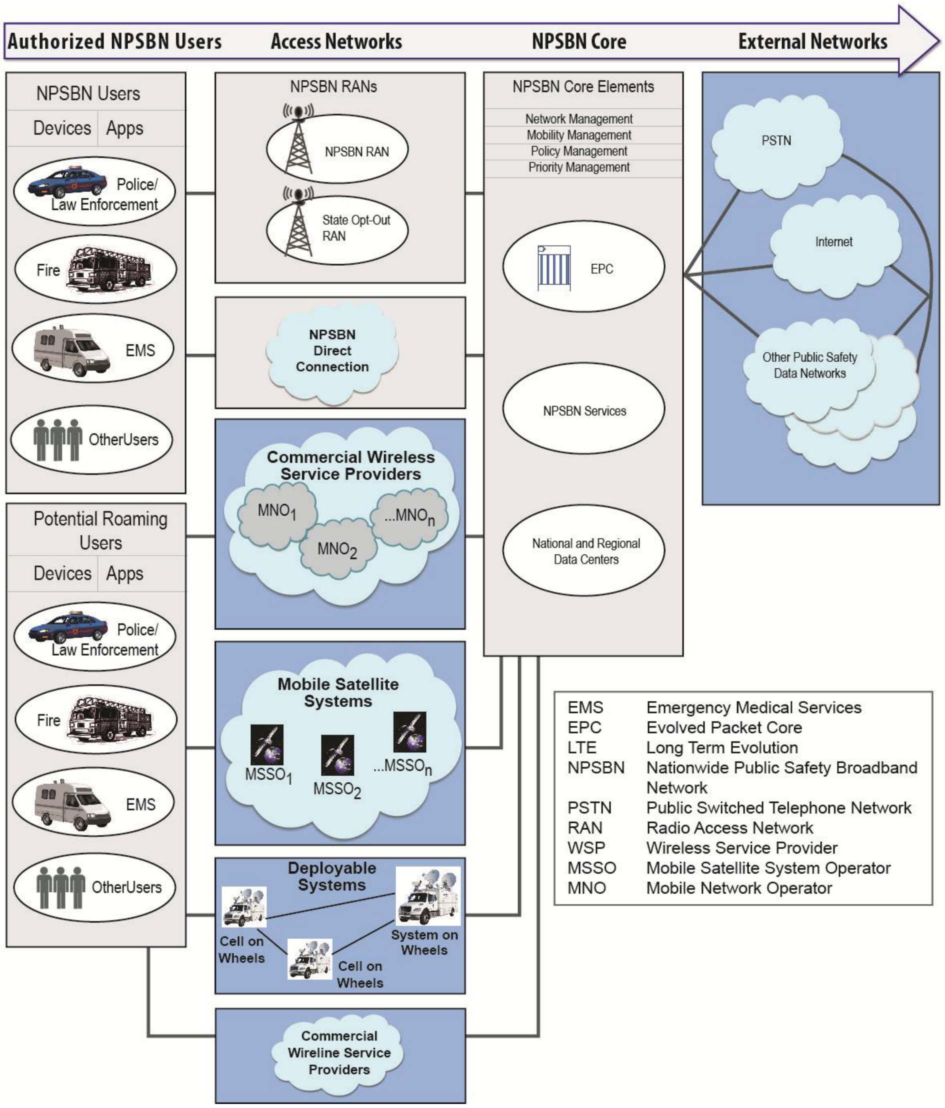
[16] P.L. 112-96 § 6503 (e)(5)(B).

[17] United States, Federal Communications Commission, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network*, released May 22, 2012. Available from http://www.fcc.gov/document/recommendations-interoperability-board.

other switched networks.[18] The core network and the RAN will include national and regional data centers and other equipment required to enable wireless communications (e.g., cell site equipment, antennas, and backhaul equipment). The law also emphasizes that the NPSBN will be based on commercial LTE standards.[19] The FirstNet Board will determine the specific network architecture of the NPSBN, in consultation with State and local government representatives.

To inform its analysis of the NS/EP implications of the NPSBN, and based on the input from multiple briefers, the NSTAC developed a notional diagram (Figure 1 below) that illustrates different NPSBN users, the multiple pathways for network access, the various networks that users' communications may traverse, and connectivity with other networks.

Figure 1: Notional NPSBN Diagram Depicting Ecosystem



[18] P.L. 112-96 § 6202 (b)(1) and (2).
[19] Ibid. § 6203 (c)(2).

2.3.1 NPSBN Policy and Regulatory Environment

The NPSBN will utilize spectrum that is licensed to the FirstNet Board by the FCC.[20] The terms of that license are governed by Part 90 of the FCC's rules, which pertain to private land mobile radio services.[21] Since the NPSBN is not a commercial network, FCC rules applicable to commercial mobile radio service providers likely do not apply to the FirstNet Board. For example, wiretap provisions of the *Communications Assistance for Law Enforcement Act* and FCC regulations for 911 services and priority access services do not apply to the NPSBN.[22]

2.3.2 NPSBN Users

As the governing body for the NPSBN, P.L. 112-96 authorizes the FirstNet Board to determine, "in consultation with Federal, State, tribal, and local public safety entities, the Director of NIST, the Commission, and the Public Safety Advisory Committee," how to manage NPSBN access and usage for both public safety and non-public safety users, as well as the levels of priority afforded to each.[23] Access, usage, and priority determinations will apply to NS/EP users that the FirstNet Board may authorize to use the NPSBN.

In defining public safety users, P.L. 112-96 noted the original definition of public safety services from the Communications Act of 1934, "services the sole or principal purpose of which is to protect the safety of life, health, or property."[24] The Act also expanded the range of possible NPSBN users by including emergency response providers as defined in the *Homeland Security Act of 2002*. Emergency response providers include "Federal, State, and local governmental and non-governmental emergency public safety, fire, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies and authorities."[25]

2.3.3 Traversing Between the NPSBN and Commercial Networks

Deployment of the NPSBN will likely take many years; public safety users can be expected to use commercial networks during that build-out phase and also try to use those networks when the NPSBN becomes congested. Figure 2 (below) illustrates the likely utilization trends as the NPSBN evolves and its construction is completed over time. In early years, commercial network usage is expected to be significant due to limited NPSBN coverage. The utilization of dedicated public safety spectrum will gradually increase as the NPSBN continues to be built. In later years, commercial networks may provide additional capacity during significant events when the NPSBN may be overloaded. During these events, NPSBN users may seek to use commercial broadband networks to off-load non-critical traffic and/or meet their mission requirements. Connectivity and interoperability with commercial networks will

[20] United States, Federal Communications Commission, *700 MHz Public Safety Broadband Nationwide License: WQQE234: First Responder Network Authority*, released November 15, 2012. Available from http://wireless2.fcc.gov/UlsApp/UlsSearch/searchLicense.jsp. Search by call sign WQQE234.

[21] 47 CFR § 90: Private Land Mobile Radio Services.

[22] 47 CFR § 64.402. "Policies and procedures for the provision of priority access service by commercial mobile radio service providers. Commercial mobile radio service providers that elect to provide priority access service to NS/EP personnel shall provide priority access service in accordance with the policies and procedures set forth in Appendix B to this part."

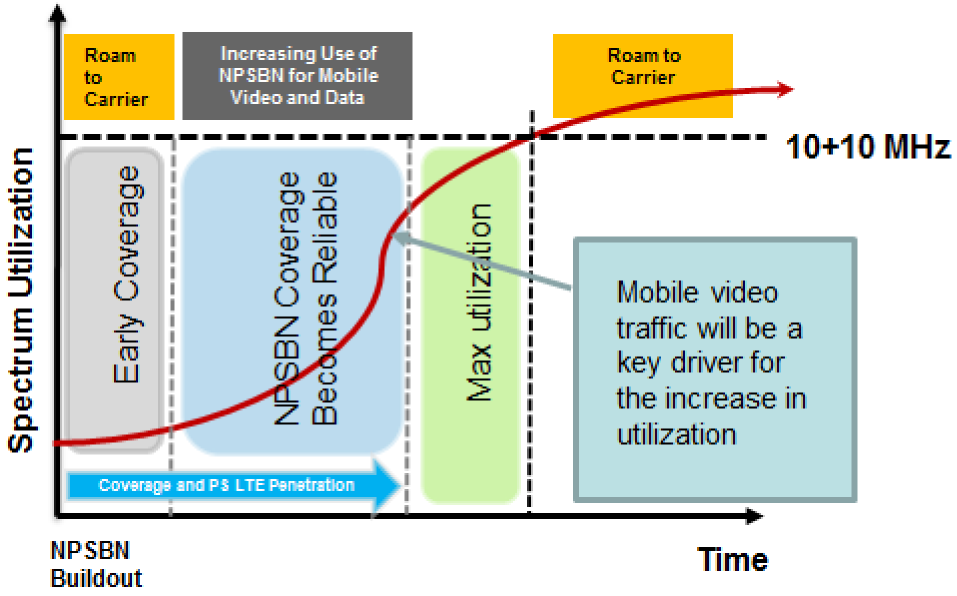
[23] P.L. 112-96 § 6206 (b)(1).

[24] Communications Act of 1934 § 337(f) as codified in 48 Stat. 1064.

[25] 6 U.S.C. 101 § 2 (Definitions)(6).

support the nationwide scalability of the NPSBN and help improve the resiliency of public safety communications.

Figure 2: Notional Depiction of NPSBN and Commercial Spectrum Utilization[26]


Roam to Carrier
Increasing Use of NPSBN for Mobile Video and Data
Roam to Carrier
10+10 MHz
Spectrum Utilization
Early Coverage
NPSBN Coverage Becomes Reliable
Max utilization
Mobile video traffic will be a key driver for the increase in utilization
Coverage and PS LTE Penetration
NPSBN Buildout
Time

Agreements with commercial carriers will be required to enable authorized NPSBN users to leverage commercial networks. P.L. 112-96 authorizes the FirstNet Board to "negotiate and enter into, as it determines appropriate, roaming agreements with commercial network providers to allow the nationwide public safety broadband network to roam onto commercial networks and gain prioritization of public safety communications over such networks in times of an emergency."[27] A broader discussion of priority communications is provided in Section 4.0.

P.L. 112-96 does not require network providers to preempt commercial traffic. Whether public safety users will achieve their goal to be granted priority treatment for their communications on commercial networks in a manner that is as close as possible to what they are afforded on the NPSBN remains to be seen.

2.3.4 Necessary Policy Evolution

Communications among those responding to a natural disaster, terrorist attack, or other large-scale event is essential. Responders must have reliable, resilient, and interoperable communications to be prepared for large-scale and day-to-day responses. DHS identified communications as one of the key national priorities to achieve the National Preparedness Goal and emergency response communications

[26] DeRango, M., Vice President, Advanced Systems Architecture, Chief Technology Office, Motorola Solutions, *Response to the NSTAC NPSBN Subcommittee Questions on Wireless Broadband Technology Demonstrator Broad Agency Announcement - BAA 12-10*, September 20, 2012.

[27] P.L. 112-96 § 6206.

as an essential capability to respond to a major event.[28] Depending on the NPSBN's final architecture and deployment, numerous policies related to national communications will be impacted.

As the NPSBN continues to be developed and deployed, and plans for future NS/EP and public safety communications become clearer, Federal policy makers should work jointly with representatives from Federal, State, local, territorial, and tribal public safety organizations, service providers, product vendors, and other entities with relevant NS/EP and or relevant communications expertise and knowledge, and in coordination with the FirstNet Board, to review and, as appropriate, update applicable policies. For example, response and communications policies that affect Federal, State, local, territorial, and tribal stakeholders, such as *National Response Framework* and the *National Emergency Communications Plan*, should be updated to account for advanced communications capabilities, including the NPSBN, in support of NS/EP and public safety missions.

3.0 COORDINATING NS/EP AND PUBLIC SAFETY FOR MUTUAL BENEFIT

The development of the NPSBN creates a near-term imperative as well as a strategic opportunity to coordinate and align NS/EP and public safety communications. Coordination will enable all levels of government to reduce costs and maximize the benefits gained through investments in NGN communications and will enable users to more effectively execute their missions.

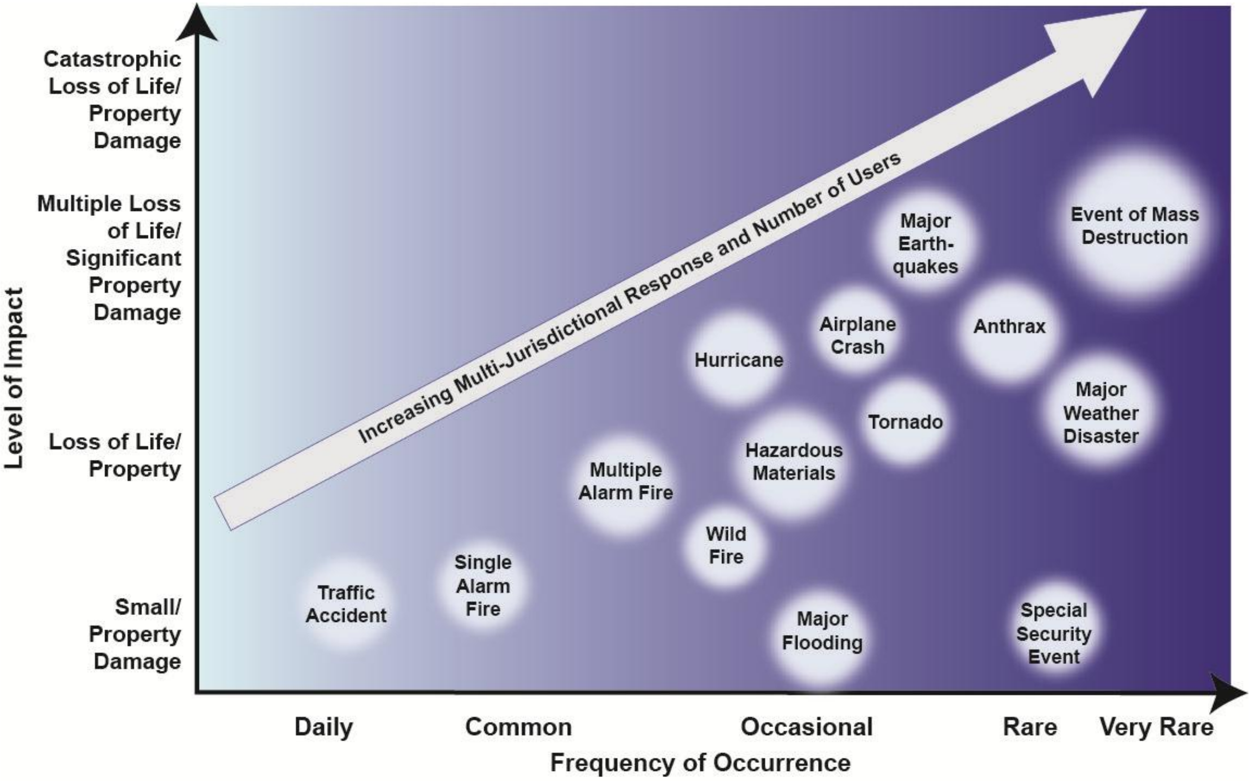
3.1 Complementary Missions

Different incidents require different responses and, as a result, the appropriate response structures for incidents vary, including whether responsibilities lie with NS/EP users, public safety users, or both. The incidents that occur most frequently, such as traffic accidents, emergencies requiring medical services, and small fires, are managed by public safety. As incidents escalate, the potential for loss of life and property damage also increase, requiring a greater number of responders to engage, often from multiple jurisdictions (whether geographical or by discipline), and multiplying the complexity of the response process. Figure 3 illustrates various events requiring response, the relative frequency and level of impact of these events, as well as the increasing number and diversity of public safety and /or NS/EP users involved in the response.

> "Incidents typically begin and end locally, and are managed on a daily basis at the lowest possible geographical, organizational, and jurisdictional level. However, there are instances in which successful incident management operations depend on the involvement of multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines. These instances require effective and efficient coordination across this broad spectrum of organizations and activities."
>
> *National Incident Management System, December 2008*

[28] DHS. *DHS Announces First National Preparedness Goal*. October 7, 2011. The goal states: "A secure and resilient nation, with the capabilities required across the whole community to prevent, protect against, mitigate, respond to, and recover from the threats and hazards that pose the greatest risk." Available from http://www.dhs.gov/news/2011/10/07/dhs-announces-first-national-preparedness-goal.

Figure 3: Various Events Requiring Response by NS/EP, Public Safety, or Both[29]



Events requiring Federal engagement are less frequent than public safety events because of the daily nature of their mission. Furthermore, events such as the Boston Marathon terrorist attack, Hurricane Sandy, and the California wildfires demonstrate that even most mid- to large-size incidents start and end with local public safety responders.[30] NS/EP events are most often perceived as those with high or large-scale impacts, but also may include smaller events that have serious implications for national security or public safety, for example, national special security events.[31] When emergencies escalate and require greater response resources, local first responders often interact with emergency services personnel in surrounding jurisdictions. State and Federal responders may also augment response efforts. Successful incident response depends on professional execution of responsibilities, local or

[29] United States, DHS, National Security Telecommunications Advisory Board, *Report to the President on Emergency Communications and Interoperability*, January 16, 2007 (Figure 3 derived from Figure 1, page 4 of the 2007 NSTAC Report). Available from http://www.ncs.gov/nstac/reports/2007/NSTAC%20Report%20on%20Emergency%20Communications%20and%20Interoperability.pdf.

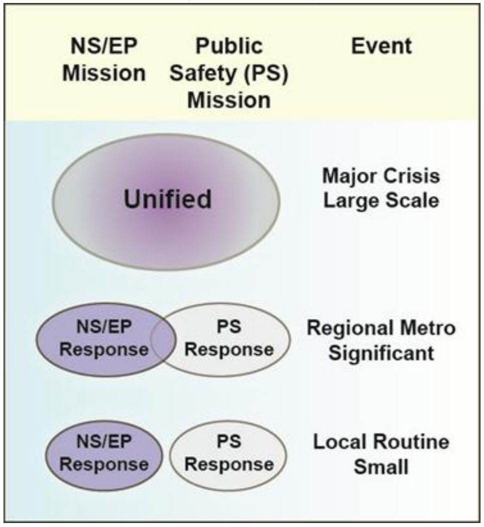
[30] NS/EP communications is not dependent on the size of the event, but the nature of the event and the need to communicate during network congestion, for example, a national special security event.

[31] Major events that are considered to be nationally significant may be designated by the President, or his representative, the Secretary of the DHS, as National Special Security Events (NSSE). Some of these events have included Presidential inaugurations, Presidential nominating conventions, major sports events, and major international meetings. Available from http://www.fas.org/sgp/crs/natsec/RS22754.pdf.

Federal, in an integrated and nearly seamless fashion, making most effective use of available and sometimes unique capabilities and resources.[32]

Consistent with this multi-jurisdictional model, NS/EP and public safety missions are frequently linked, particularly during responses to NS/EP events (Figure 4). Response for these events requires extensive coordination, even in the most difficult circumstances. Most activities for NS/EP events, though led by Federal officials and responders, require and depend on the integrated contributions of responders across all levels of government.

Figure 4: Relationship Between the NS/EP and Public Safety Mission as Part of Integrated Response



NS/EP and public safety users prepare for, operate, coordinate, and fulfill their respective missions within the National Incident Management System (NIMS).[33] It provides a consistent nationwide template to enable Federal, State, local, territorial, and tribal governments, NGOs, and the private sector to work together to prevent, protect against, respond to, recover from, and mitigate the effects of incidents, regardless of cause, size, location, or complexity. NIMS represents a core set of doctrines, concepts, principles, terminology, and organizational processes that enables effective, efficient, and collaborative incident management.[34]

3.2 Synergistic Communications Capabilities and Requirements

NS/EP and public safety subject matter experts (SMEs) described numerous and varied scenarios of how advanced communications currently help them perform their respective missions, and how advanced communications could be used in the future. Some of the necessary communications capabilities described by the SMEs include:

- **Prediction, Detection, and Situational Awareness:** Effective communications, information management, and incident-specific intelligence to foster rapid identification and understanding of events and the environment (i.e., a common operational picture) to coordinate and streamline response across Federal, State, and local levels, as appropriate.
- **Warning and Alerts**: Broadcast, sound, radio, television, and mobile alerts to inform people likely to be affected and to assist local, regional, and central authorities responsible for warning officials and the public.
- **Cross Organizational Coordination and Resource Management:** Ability to share information and communicate across organizational boundaries, and efficiently and effectively deploy

[32] United States, DHS, *The National Incident Management System*, December 2008. Available from http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

[33] United States, DHS, *The National Incident Management System*, December 2008. Available from http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

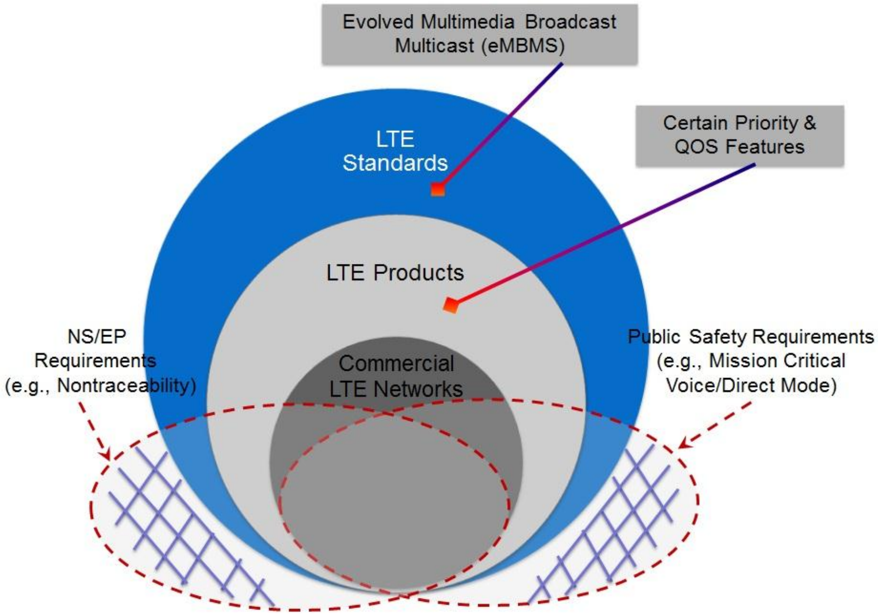
[34] Of note, a broad and diverse range of stakeholders across all levels of government, and involving the private sector and NGOs, developed NIMS.

resources (e.g., responders, infrastructure, devices, and applications) available from numerous organizations when and where they are most needed to enable response and restoration.[35]

NS/EP and public safety users are currently defining communications requirements to deliver these capabilities, as well as others, as part of their respective transitions to advanced broadband networks. While commercial standards, technologies, and innovation will meet some of these requirements, NS/EP and public safety users will still have unique requirements necessary to fulfill their missions that exceed those satisfied by the broad, commercial marketplace.

This gap between functional requirements to serve the commercial marketplace and the unique requirements for NS/EP and public safety communications is illustrated below (Figure 5). The concentric circles show how technologies implemented in commercial LTE networks are a subset of the available LTE products, and that products are developed using only a subset of the functionality defined in the LTE standards. Complex business decisions, considering return on investment factors such as costs, expected user base, and pricing, are made to determine the scope of functionality provided by these technologies. Commercial LTE service providers and product vendors will provision LTE products to satisfy the needs of their user base.

Figure 5: Illustration of NS/EP and Public Safety Requirements Relative to Functionality Provided by the Commercial Marketplace[36]


Evolved Multimedia Broadcast Multicast (eMBMS)
Certain Priority & QOS Features
LTE Standards
LTE Products
Commercial LTE Networks
NS/EP Requirements (e.g., Nontraceability)
Public Safety Requirements (e.g., Mission Critical Voice/Direct Mode)

[35] Surma, T., Senior Director and CTO Microsoft Disaster Response, *Microsoft Disaster Response*, October 4, 2012; Miller, T., Chief Technology Office, Motorola Solutions, *NSTAC Priority and QoS on the NPSBN*, August 14, 2012; Patrick, P., Chair, Communications Technology Committee, National Association of State EMS Officials, *21st Century EMS Communications Systems: 'Brick' to the Tricorder*, August 30, 2012.

[36] United States, Federal Communications Commission, *Recommended Minimum Technical Requirements to Ensure Interoperability for the Nationwide Public Safety Broadband Network*, May 22, 2012. Available from http://apps.fcc.gov/ecfs/document/view?id=7021919873. Graphic modified to illustrate notional NS/EP requirements.

From a commercial standpoint, implementation of additional unique requirements for a relatively small number of users cannot be cost-justified by the service providers or product vendors. Investments are often necessary to foster development of products and services to satisfy unique NS/EP and public safety communications requirements. For example, the Government helped fund the capabilities for the Government Emergency Telecommunications Service (GETS) and the Wireless Priority Service (WPS) programs[37] to provide priority for NS/EP communications (see Section 4.2 for additional information). From the public safety perspective, SAFECOM Guidance on Emergency Communications Grants identifies allowable costs to support public safety under DHS grants administered by the Federal Emergency Management Agency (FEMA) Grant Programs Directorate.[38]

As demonstrated in Figure 6, some of the NS/EP and public safety requirements that exceed the functionality provided by commercial offerings are similar and possibly synergistic, while others are different.[39] The synergistic requirements include:

- **Interoperability:** End-to-end communications across private and commercial networks, devices, applications, and services.
- **Security:** Confidentiality, integrity, and availability of communications under all circumstances.
- **Priority Communications**: Ability for eligible communications to be treated with higher priority than other communications traffic.
- **Ubiquitous/Nationwide Coverage**: Access to communications from anywhere in the United States.
- **Reliability and Resiliency**: Communications perform consistently and according to design requirements, including at acceptable levels during impact to or failure of one or more components or a significant increase in traffic.

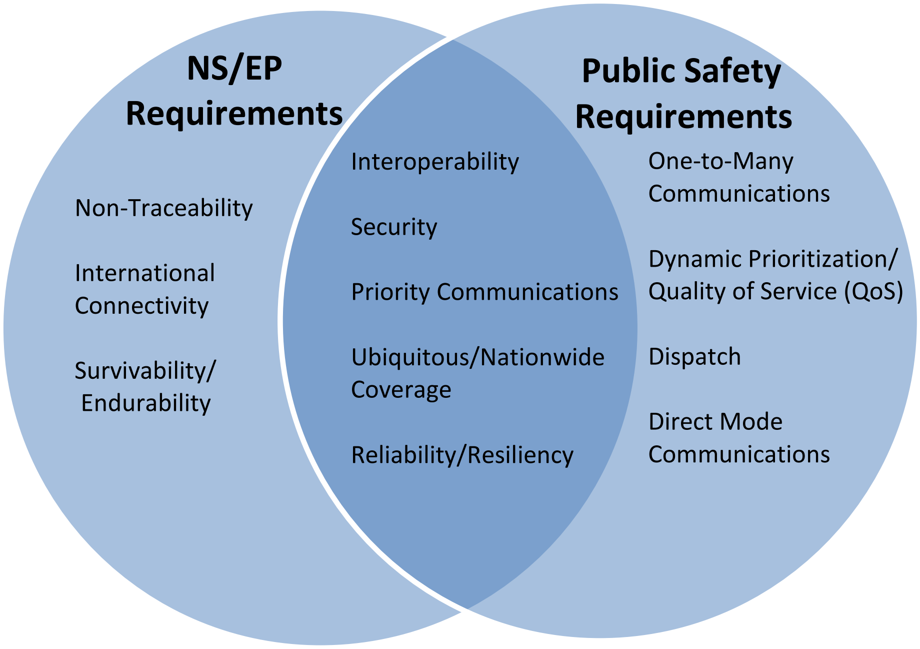
Additional detail on NS/EP and public safety requirements can be found in Appendix I, *NGN NS/EP Telecommunications Services Functional Requirements*.

[37] Appendix H: Lessons Learned from GETS/WPS.

[38] United States, DHS, *SAFECOM Program* Home Page. Available from http://www.safecomprogram.gov/grant/Default.aspx.

[39] This list of requirements is not exhaustive, but is provided to illustrate similarities and differences in NS/EP and public safety communications requirements.

Figure 6: Notional Diagram of Several NS/EP and Public Safety Functional Requirements[40]


NS/EP Requirements
Non-Traceability
International Connectivity
Survivability/ Endurability
Interoperability
Security
Priority Communications
Ubiquitous/Nationwide Coverage
Reliability/Resiliency
Public Safety Requirements
One-to-Many Communications
Dynamic Prioritization/ Quality of Service (QoS)
Dispatch
Direct Mode Communications

Because of these unique requirements, innovation cycles for NS/EP and public safety communications often lag commercial innovation cycles. The return on investments for innovation to support NS/EP and public safety communications is smaller because of a relatively smaller user community. Identifying and managing synergies and differences in NS/EP and public safety communications requirements will help to prevent incompatible solutions, ensure communications for both, and optimize the benefits of investments as advanced communications are deployed, both in commercial networks and the NPSBN.

3.3 Aligning to Enable Innovation

Numerous authoritative documents have highlighted the need to coordinate NS/EP and public safety users' requirements.[41] Until the NSTAC's examination, however, no formal effort had been undertaken

[40] Requirements are derived from DHS Functional Requirements documentation and briefing by Miller, T., *NSTAC Priority and QoS on the NPSBN*, Trent Miller (August 14, 2012).

[41] United States, Library of Congress, Congressional Research Service, *An Emergency Communications Safety Net: Integrating 911 and Other Services*, September 1, 2005. Available from https://opencrs.com/document/RL32939/2005-09-01/; United States, Library of Congress, Congressional Research Service, *Public Safety Communications and Spectrum Resources: Policy Issues for Congress*, July 23, 2010. Available from http://www.fas.org/sgp/crs/misc/R40859.pdf; George Washington University, Space and Advanced Communications Research Institute, *White Paper on Emergency Communications*, January 5, 2006. Available from http://spacejournal.ohio.edu/issue10/PDF/Final_Version_White_Paper.pdf; United States, Congress, House of Representatives, *Written Testimony of National Protection and Programs Directorate, Office of Cybersecurity and Communications, Deputy Assistant Secretary Roberta Stempfley before the House Committee on Homeland Security, Subcommittee on Emergency Preparedness, Response, and Communications Hearing Titled "Resilient Communications: Current Challenges and Future Advancements*," September 12, 2012. Available from http://www.dhs.gov/news/2012/09/12/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-0; Hallahan, R. and J.M. Peha, *Policies for Public Safety Use of Commercial Wireless Networks*, 38th

to examine how the current and evolving communications environment and the introduction of the NPSBN would affect NS/EP and public safety communications, nor how to more effectively manage the growing synergies in their needs. By coordinating requirements, incentives, and investments, NS/EP and public safety users can better leverage advanced communications to help fulfill their respective missions.

Coordinating Communications Capabilities and Requirements

NS/EP and public safety communications are transitioning to advanced broadband networks and, as noted in Section 3.2, their users have certain requirements; for example, security and reliability are higher than those for consumer, enterprise, and many other government users. In instances where NS/EP and public safety users coordinate and have similar requirements, they can achieve economies of scale, improve interoperability, security, and resiliency, and better leverage commercial innovation to more effectively and efficiently fulfill their missions. Without coordination, separate requirements may impede interoperable communications, or worse, may create conflicts and barriers. Moreover, the existence of competing and unprioritized requirements will not effectively guide private sector service providers and product vendors who must often decide the features to resource and in what order. Coordination to ensure end-to-end priority for NS/EP and public safety communications is of such importance, it will be discussed in detail in Section 4.0.

Even though NS/EP and public safety users have similar requirements, specific use cases may vary; users may differ in how those requirements are prioritized, as well as the technical approaches to fulfilling them. Coordination of requirements for NS/EP and public safety communications will help identify areas where requirements are complementary, distinct, or overlap.

Coordination on similar requirements will create mutual benefits, yet this is also true for coordination where there are differences in requirements. For example, the differences in the respective strategies in NS/EP and public safety with regards to transitioning voice, video, and data communications to NGN provides a clear example where coordination will be mutually beneficial. As previously noted, public safety organizations plan to transition video and data communications to the NPSBN while continuing to leverage LMR capabilities for mission critical voice. In contrast, NS/EP communications are focused on priority voice on LTE before video and data communications because of the increasing obsolescence of circuit-switched technologies upon which most NS/EP communications rely. Because NS/EP and public safety users have similar functional requirements and are leveraging the same LTE technologies but have different transition strategies, there is an opportunity to exchange lessons from their respective deployments to inform each other's subsequent efforts. Section 3.3.3 provides additional discussion on considerations to help manage differing priorities and challenges that may arise as officials seek to increase coordination among NS/EP and public safety users.

Fostering a vibrant marketplace to serve the needs of NS/EP and public safety users, especially considering the relatively smaller user base, requires thoughtful deliberation. Such an environment can

Telecommunications Policy Research Conference, October, 2010. Available from http://users.ece.cmu.edu/~peha/public_safety_priority_access.pdf; United States, Federal Communications Commission, *National Broadband Plan: Chapter 16: Public Safety*. March 2010. Available from http://www.broadband.gov/plan/16-public-safety/.

be promoted by establishing baseline requirements beyond those already required for interoperability, and by making those requirements broadly accessible to a wide range of entities—whether individuals, organizations, jurisdictions, or enterprises—that may want to develop and provide products and services in this market.[42] Establishing baseline requirements helps to ensure that NS/EP and public safety needs can be met, but that requirements are not so unwieldy as to constrain market entry, hinder deployment, and reduce the mutual benefits created by economies of scale. The resulting dynamic and organic environment will help foster collaboration that not only leverages, but also optimizes various jurisdictions' diverse capabilities for the benefit of the Nation. For example, following the Air Florida crash in 1982, jurisdictions within the National Capital Region collaborated to establish interoperable processes and technologies, which enhanced their collective ability to respond to incidents across the jurisdictions.[43, 44]

The publication of baseline requirements would create an environment where NS/EP and public safety users could not only take advantage of technological innovations, but also contribute to them. For example, the world is at the beginning of a massive innovation cycle in multimedia communications applications and many of these innovations could help provide NS/EP and public safety users with real-time access to key data or communication mechanisms.[45] Clearly NPSBN users will access applications on or through the NPSBN; however, it is too early to know which applications may be authorized and how they will be integrated. The establishment of publicly available baseline requirements would enable jurisdictions across all levels of government, commercial enterprises, and even motivated NS/EP and public safety users, to create applications that would satisfy identified needs and be interoperable outside of their jurisdictions. Additionally, such applications could be made available to all NS/EP and public safety users through a cloud-powered NPSBN application store that is run on a shared services model. As indicated in the *NSTAC Report to the President on Cloud Computing*, by leveraging shared infrastructure and software applications services, cloud computing allows an organization to build new information technology (IT) solutions and offer new services more quickly and cost-effectively than building those solutions and services themselves.[46]

> Considerable innovation is expected to be driven by public safety because of the larger number of users and their daily mission execution.

Close coordination on capabilities and requirements, and a focus on innovation, will be critical to understanding and managing today's complex communications

[42] United States, Federal Communications Commission, *Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network*, May 22, 2012. Available from http://apps.fcc.gov/ecfs/document/view?id=7021919873.

[43] United States, Library of Congress, Congressional Research Service, *Funding Emergency Communications: Technology and Policy Considerations*, December 14, 2011. Available from http://www.fas.org/sgp/crs/homesec/R41842.pdf.

[44] Reyes, E., Deputy Chief, City of Alexandria Police Department, Briefing for the National Security Telecommunications Advisory Committee on Emergency Communications Among State and Local Organizations, February 10, 2012.

[45] Rosenburg, J., General Manager Product Strategy and Research, Skype, Briefing for the National Security Telecommunications Advisory Committee on Skype, October 16, 2012.

[46] United States, DHS, National Security Telecommunications Advisory Committee, *Report to the President on Cloud Computing*, May 2012. Available from http://ncs.gov/nstac/reports/2012-05-15%20NSTAC%20Cloud%20Computing.pdf.

environment and the diversity across jurisdictions. This diversity includes how jurisdictions leverage varying communications technologies (e.g., LMR, commercial broadband) as well as the extent to which they adopt and use broadband capabilities to advance their missions. As technologies and skills become more diverse and resources become more constrained, NS/EP and public safety officials have emphasized the importance of collaborating across jurisdictions and developing services that can be shared across a larger user base to optimize limited resources and improve mission effectiveness.[47] Collaboration could extend to the FirstNet Board, making a variety of services available to jurisdictions via contract, providing them greater flexibility for building the NPSBN within their borders.[48]

Coordinating Standards, Research and Development, Pilot Programs, and Grants

NS/EP and public safety users can also benefit by coordinating efforts to develop standards, fund research and development (R&D), and initiate pilots to meet both similarities and differences in their communications requirements. Coordination will provide NS/EP and public safety users with greater awareness of existing Federal efforts and help identify gaps among them. Coordination and expansion of incentives and investments can also help promote innovation in the delta between commercial marketplace requirements and NS/EP and public safety requirements. Additionally, coordination will put NS/EP and public safety users in a better position to develop strategies to leverage existing efforts and funding in an increasingly resource-constrained environment.

The Federal Government already funds R&D, standards development, and pilot programs to help meet various unique requirements (e.g., priority communications, mission critical voice) for NS/EP and public safety communications. The Federal Government must continue these efforts as well as evaluate them for opportunities to help maximize the benefits to NS/EP and public safety communications, such as re-using or re-purposing outcomes to gain additional return on the investments. For example, the Defense Advanced Research Projects Agency (DARPA) transferred a communications technology, which has a specific feature related to priority service, to DHS' Science and Technology Directorate (S&T) so that DHS S&T could work with the private sector to commercialize it. Given that priority communications are a key requirement for NS/EP and public safety users, there may be opportunities to expand the purpose of the DARPA effort so that it also benefits NS/EP and public safety users.[49]

Some Federal R&D organizations reported having few opportunities to help define R&D priorities related to NS/EP and public safety users' unique communications requirements; these organizations also had not received requests to perform this research.[50] Coordinating R&D among NS/EP and public safety organizations and with other interested stakeholders will create greater awareness of R&D efforts, inform the development of priorities, and help optimize the value of these investments.

[47] Robinson, Chuck, City of Charlotte and Interoperability Board, North Carolina, Charlotte, *Challenges and Success Factors in Establishing a NPSBN.* Briefing for the National Association of Telecommunications Officers and Administrators, September 27, 2012. Available from http://www.natoa.org/events/Charlotte%20Presentation%20Robinson.pdf.

[48] Schrier, B., Chief Technology Officer, City of Seattle, Briefing for the National Security Telecommunications Advisory Committee on March 23, 2012.

[49] Maughan, D., Division Director, Homeland Security Advanced Research Projects, Science and Technology Directorate, U.S. DHS, Research and Development Discussion on March 23, 2013.

[50] Ibid.

Standardization is also essential to help support access, interoperability, security, reliability, and resiliency of NS/EP and public safety communications. Multiple organizations are already engaged in standardization efforts on technical requirements for infrastructure. They and other appropriate stakeholders also will need to facilitate development of future standards for applications and data to be used on or accessed through the infrastructure. These efforts will be necessary not only to meet Federal and State information compliance regimes across jurisdictions, but also to enable analysis of large and complex data sets (i.e., big data) for insights to drive improvements.

Standardization is particularly important when considering how to achieve nationwide scalability. Deployment and evolution of the NPSBN must account for jurisdictions' diverse capabilities and help ensure scalability to the national level. In addition to the connectivity discussed in Section 2.3.3, scalability also can be improved through standards-based open architecture that allows jurisdictions to deploy systems based on interoperable elements.

National policy can also help ensure scalability by enabling the coordination of R&D and standards to promote interoperability. For example, standards efforts in identity management, credentialing, authorization, or other security-related requirements will help to improve the interoperability and scalability of communications, as well as security and privacy, as described in the *NSTAC Report to the President on Identity Management Strategy*[51] and the *National Strategy for Trusted Identities in Cyberspace*.[52]

Coordination on pilot programs can also create mutual benefits. For example, the Department of Commerce has a Public Safety Communications Research (PCSR) Program that fosters nationwide communications interoperability through research, development, testing, and evaluation.[53] The PSCR Program has conducted successful pilot programs, including a project bridging LMR to broadband capabilities to test the integration of broadband technologies on two-way radios.[54] The insights gained through the PSCR Program may be applicable as NS/EP users manage technical challenges during the ongoing transition of commercial networks from existing circuit-based to more advanced IP-based technologies.

An applications store ("app store") serving both NS/EP and public safety users is another example where coordination could foster innovation in applications and services. This idea has received support from several organizations.[55] Such a store can enable greater interoperability and help reduce risk to the

[51] United States, DHS, National Security Telecommunications Advisory Committee, *Report to the President on Identity Management Strategy,* May 2009. Available from http://www.ncs.gov/nstac/reports/2009/NSTAC%20IDTF%20Report.pdf.

[52] United States, National Institute of Standards and Technology, *National Strategy for Trusted Identities in Cyberspace.* Available from http://www.nist.gov/nstic/.

[53] United States, Department of Commerce, Public Safety Communications Research Program Overview Home Page. Available from http://www.pscr.gov/about_pscr/pscr_about.php.

[54] United States, Department of Commerce, Public Safety Communications Research Program Projects Archive Home Page. Available from http://www.pscr.gov/projects/archive/broadband/broadband_archive.php.

[55] United States, Department of Commerce, National Telecommunications and Information Administration, FirstNet Board Meeting, September 25, 2012. Available from http://www.ntia.doc.gov/other-publication/2012/9252012-firstnet-meeting-transcript-and-archived-webcast.

NPSBN, and the devices and services running on it, by ensuring that users can access only authorized applications. There are several examples of app stores currently being developed within the Federal Government; the Department of Defense (DOD) is developing its own mobile application store, and law enforcement has developed apps, such as the Federal Bureau of Investigation's Child Abduction Response Management App Pilot. These early efforts have already generated some lessons learned, such as the importance of securing the application at the device and operating system layers, rather than merely securing the application itself.

It should be noted that very few pilot programs within DHS focus on NS/EP or public safety communications, as priorities compete for limited resources. The private sector, however, is moving forward with pilot programs to serve their customers' needs. Many of the private sector initiated pilot programs have only limited Government involvement, which could result in incompatible or proprietary approaches. NS/EP and public safety communications would benefit from a more active Government role and funding for DHS to sponsor or participate in pilot programs intended to address unique requirements that cannot be fulfilled by commercial offerings.

Providing Education and Training

All NS/EP and public safety users need to be able to use technology securely in order to execute their missions in a digital world. Standardization, ease of use, and training are important for NS/EP and public safety users in order to ensure that they understand and are able to work with existing and new communications capabilities. For example, current LMR capabilities used by public safety organizations would have little value without proper training on radio protocols.[56] Awareness, education, and training efforts targeted at raising levels of awareness of new technologies will increase understanding and help acclimate users to the benefits and risks associated with advanced communications in support of their missions. These activities should also cover requirements regarding privacy, civil rights, and civil liberties protections to ensure appropriate sharing and protection of personally identifiable information.

3.3.1 Organizing to Enable Coordination

The NSTAC examined the responsibilities and functions of various NS/EP or public safety communications organizations, met with representatives from some of these organizations, and engaged in several public safety–focused events. The NSTAC's examination of organizations with NS/EP and public safety communications responsibilities was not exhaustive, but did reveal that various Federal, State, and local groups representing a range of jurisdictions and capabilities are examining NS/EP and public safety communications, most often separately or with only informal touch points. This results in limited awareness of or coordination on common interests. There is a need to better organize and incent coordination to bolster current, nascent efforts to work together, catalyze more collaboration, and institutionalize a framework that enables NS/EP and public safety communications to take advantage of synergies and optimize the benefits realized through NGN investments across levels of government.

[56] Reyes, E., Deputy Chief, City of Alexandria Police Department, Briefing for the National Security Telecommunications Advisory Committee on Emergency Communications Among State and Local Organizations, February 10, 2012.

Current Landscape

NS/EP and public safety users have historically had distinct forums for collaboration and for developing and prioritizing requirements. Just as there is wide diversity among Federal NS/EP and Federal public safety communications users, there is, and will continue to be, wide diversity among organizations that represent their respective communications and policy interests. Even within counties, public safety users cross multiple jurisdictions, and numerous public safety entities exist statewide; as previously noted, some may organize based on geography and others based on discipline. The situation is similar across tribal and territorial areas. At the same time, NS/EP users and stakeholders are from a variety of organizations, and even within the private sector, users come from multiple sectors.

The NSTAC examined representative organizations with some NS/EP or public safety communications responsibilities, functions, and expertise, listed below. The list does not represent a complete inventory of all relevant organizations, but is provided to show the breadth of stakeholders and organizations with similar, but not yet well-coordinated, interests in NS/EP or public safety communications. This list also begins to reveal the complexity of working with such a broad stakeholder community to establish effective communications policy.

Federal Organizations and Representatives

- NS/EP Communications ExCom: The ExCom makes recommendations to the President on NS/EP communications to enhance the survivability, resilience, and future architecture of NS/EP communications, including what should constitute NS/EP communications requirements.[57] ExCom membership includes the Departments of State, Defense, Justice, Commerce, and Homeland Security, the Office of the Director of National Intelligence, the General Services Administration (GSA), and the FCC. Representatives from DOD and DHS serve as the ExCom's co-chairs.
- Emergency Communications Preparedness Center (ECPC): The ECPC is the Federal interagency focal point for interoperable and operable emergency communications coordination. Housed in the DHS, the ECPC members represent the Federal Government's broad role in emergency communications, with responsibilities that include regulation, policy, operations, grants, and technical assistance.[58] ECPC membership includes the Departments of State, Treasury, Defense, Justice, Interior, Agriculture, Commerce, Labor, Health and Human Services, Transportation, Energy, Homeland Security, the GSA, and the FCC.
- Federal law enforcement organizations with public safety roles: These organizations include the Federal Bureau of Investigation, U.S. Coast Guard, U.S. Marshals Service, Immigration and Customs Enforcement, and Customs and Border Protection.

[57] United States, White House, Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Function,* July 2012. Available from http://www.gpo.gov/fdsys/pkg/FR-2012-07-11/pdf/2012-17022.pdf.

[58] United States, DHS, Emergency Communications Preparedness Center Home Page. Available from http://www.dhs.gov/emergency-communications-preparedness-center.

- Federal defense organizations with public safety responsibilities: These consist of the U.S. Armed Forces, including the National Guard.[59]

State and Local Government and Public Safety Organizations and Representatives

- State and local government agencies and officials, including, for example, Governors, Lieutenant Governors, County leadership, mayors, police and fire leadership at all levels, Emergency Medical Services leadership, and many others.
- Influential State and local government organizations: These include the National Governors Association, National Association of Counties, National Conference of State Legislatures, National League of Cities, U.S. Conference of Mayors, International City/County Management Association, and Council of State Governments, among others.
- Key public safety associations organized at the national level: These include the Association of Public-Safety Communications Officials International (APCO), National Public Safety Telecommunications Council (NPSTC), SAFECOM, International Association of Chiefs of Police, National Sheriffs Association, National Emergency Number Association, International Association of Fire Chiefs, and others.[60, 61]
- Public Safety Advisory Committee (PSAC): P.L. 112-96 establishes the PSAC to assist the FirstNet Board in carrying out its duties. The PSAC is composed of 40 representatives from various public safety and State/local government organizations, including each of the organizations identified above within this category.

The passage of P.L. 112-96 was significant in part because it was the first time that the diverse community of public safety users at the national and local levels came together for a common goal (i.e., to support public safety communications legislation). NSTAC briefers noted the strong support for the legislation from public safety officials and organizations across multiple disciplines and their associations working together.

Recent alignment within the DHS Office of Cybersecurity and Communications and the assignment of public safety communications responsibilities to the NTIA similarly demonstrate efforts to improve

[59] DOD doctrine allows commanders to provide resources and assistance to civil authorities without or prior to a declaration under the *Stafford Act* when a disaster overwhelms the capabilities of local authorities and necessitates immediate action "to prevent human suffering, save lives, or mitigate great property damage." Source: Elsea, J. K., and Mason, R. C. "The Use of Federal Troops for Disaster Assistance: Legal Issues." Congressional Research Service, November 28, 2008.

[60] NPSTC is composed of 15 member organizations, including American Association of State Highway Transportation Officials; American Radio Relay League; Association of Fish & Wildlife Agencies; Association of Public-Safety Communications Officials International; Forestry Conservation Communications Association; International Association of Chiefs of Police; International Association of Emergency Managers; International Association of Fire Chiefs; International Municipal Signal Association; National Association of State Chief Information Officers; National Association of State Emergency Medical Services Officials; National Association of State Foresters; National Association of State Technology Directors; National Emergency Number Association; and National Sheriffs' Association.

[61] United States, DHS, SAFECOM Program Home Page. Available from http://www.safecomprogram.gov/default.aspx. SAFECOM has been instrumental in the creation of key documents such as the NECP to assist emergency responders nationwide in improving communications and interoperability.

coordination and alignment within the Federal Government. These are positive indicators, but are only two points in a larger NS/EP and public safety communications landscape. To date, coordination has focused within Departments and Agencies and on specific roles and responsibilities; there has not yet been a review that looked across relevant Departments and Agencies to determine the degree to which greater alignment will be mutually beneficial, and if structural changes may be necessary to serve the interests of the Nation.

More Cohesive Future

Since NS/EP and public safety users will leverage similar networks and technologies, public policy leaders should ensure their combined interests are addressed moving forward. The NSTAC's review of relevant policies, composition, responsibilities, and functions of these groups found that no single organization represents the communications interests of the large and diverse group of public safety users, much less the larger set of both NS/EP and public safety communications interests.

From a policy perspective, a key priority should be to facilitate relationship-building and coordination among NS/EP and public safety users and stakeholders, with the goal of driving innovation that can benefit users across functions. By creating bridges between communities, policy will enable innovation where it occurs most often: between individuals who seek to solve shared problems or satisfy unmet needs.

> There is a need to "expand the partnerships upon which the homeland security enterprise depends, develop technologies that support the achievement of homeland security mission goals and objectives, and institutionalize processes that will support effective and informed decision making and unity of effort within the enterprise."
>
> *Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland*. February 2010.

Users and their missions will likely benefit from traditional top-down and/or centralized models, such as the NSTAC and NPSTC, as well as more socially-driven models that foster more open and dynamic collaboration. From a top-down perspective, executive leadership has an opportunity to functionally align and streamline Government efforts underway for Federal NS/EP and Federal public safety NGN communications requirements. This alignment should be broadly focused across the Federal Government, but exclude independent authorities such as the FCC and the FirstNet Board.

Functional alignment within the Federal Government is not intended to drive consolidation, but rather is intended to provide an enabling structure to institutionalize coordination among a diverse and varied community of stakeholders. For example, a review of the specific responsibilities of the ExCom and ECPC reveals that the organizations have several similar responsibilities. The ExCom is responsible for coordinating the planning and provisioning of NS/EP communications for the Federal Government under all hazards and the survivability of NS/EP communications under all circumstances.[62] At the same time, the ECPC is responsible for ensuring that emergency response providers and relevant Government officials have the ability to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters.[63] If the ECPC and ExCom formally coordinated, or their responsibilities were

[62] E.O. 13618.

[63] P.L. 109-295.

rationalized, Federal Government officials would be able to identify shared interests and better serve both NS/EP and public safety users.

During the NSTAC's examination, DHS officials recommended immediately developing a plan and an approach for institutionalizing coordination between the ExCom, the ECPC, and related stakeholder organizations as appropriate. The NSTAC recognizes DHS' progress to align and improve coordination; yet it is only one organization among many that need to institutionalize coordination. Senior officials should establish clear, agreed upon understanding of roles, missions, and responsibilities among all parties, and inform the development of coordinated communications policies, resourcing, and operations.

Improved coordination within the Federal Government will not only help avoid falling into separate, incompatible solutions as already noted, but will also better position the Federal Government to partner with State and local officials as well as with the private sector. The need for this broad diversity of stakeholders was identified in the 2012 *Desirable Properties of a Nationwide Public Safety Communication System*, which called for "a wide range of actors, including traditional emergency responders, national homeland security elements, military, state militia, municipal, private-sector public safety organizations and research agencies and institutions."[64] Fostering coordination among diverse Federal, State, local, territorial, and tribal representatives, and public safety organizations, service providers, product vendors, and others with relevant expertise and knowledge will be effective only if the appropriate forums are structured, roles and responsibilities are clearly defined, and incentives and disincentives to coordination are identified and addressed.

In addition to aligning efforts within the Federal Government and ensuring the participation of the diverse set of stakeholders, the Federal Government should review relevant advisory boards to ensure that industry advice on advanced communications considers the evolving needs of both NS/EP and public safety. For example, E.O. 13618 requires that the executive branch be able to communicate within itself and with the other branches of the Federal Government, State, local, territorial, and tribal governments, and private sector entities at all times and under all circumstances.[65] The NSTAC membership and functions should represent the full range of industry NS/EP and public safety communications knowledge and expertise. This representation will best position the NSTAC to provide the President with advice to assure communications at all times and under all circumstances.

3.3.2 Positioning for the Future Communications Environment

The NSTAC's examination considered the near-term implications of the NPSBN, as well as how the rapidly evolving communications environment and increased synergies in communications needs and technologies may affect NS/EP's and public safety's communications and missions moving forward. This approach was intended to help ensure mission critical results today, and help government and industry forge a path to execute their missions successfully in the future. As government and industry consider the longer-term implications of the communications environment, it is essential that efforts to develop

[64] National Institute of Standards and Technology, Visiting Committee on Advanced Technology, "*Desirable Properties of a Nationwide Public Safety Communication System*," January 24, 2012. Available from http://www.nist.gov/director/vcat/upload/Desirable_Properties_of_a_National_PSN.pdf.

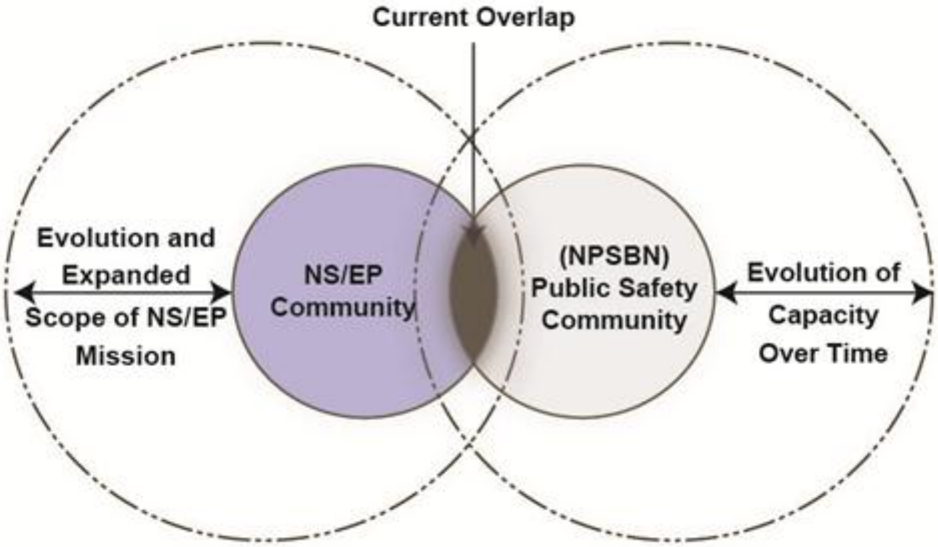
[65] E.O. 13618.

and deploy the NPSBN must not be delayed; public safety users urgently need the advanced communications that the NPSBN will enable.

While the NPSBN is still nascent and the technologies upon which it will be built are some of the most advanced today, history and experience show that technology will continue to evolve rapidly. Whether specific to NS/EP and public safety communications or in the broader commercial marketplace, technological innovation will continue to enable new scenarios and capabilities, drive development of more advanced infrastructure and devices, and prompt greater convergence among networks and users.

This rapidly evolving and diverse communications environment is changing the degree of intersection between the NS/EP and public safety missions. As illustrated in Figure 7, the degree of intersection is increasing over time because of the convergence being driven by technology as well as the expansion of the range of NS/EP events. The extent or rate at which that intersection is growing is not the NSTAC's to determine, but certain facts must be noted. Specifically, numerous diverse entities are engaged in multi-jurisdictional responses to NS/EP and public safety events and some responders are in both communities. Additionally, NS/EP and public safety users are, at least in part, dependent upon the same or very similar technologies, networks, applications, and services. While coordinating requirements, standards, and R&D is necessary and will benefit both NS/EP and public safety communications, coordination alone may not be sufficient in the future.

Figure 7: Intersection between NS/EP and Public Safety Missions


Current Overlap
Evolution and Expanded Scope of NS/EP Mission
NS/EP Community
(NPSBN) Public Safety Community
Evolution of Capacity Over Time

Furthermore, technological innovation occurs at a significantly faster pace than the evolution of communications policy. It is inadequate to consider only the characteristics of today's communications environment when formulating nationwide policies; by the time decisions are finalized, the communications environment will have changed. Policy development for NS/EP and public safety communications has been distinct for each set of users and was based on only limited understanding or appreciation for the capabilities and requirements of their counterparts. Moving forward, policy development must better account for tomorrow's communications environment. Policies need to more appropriately plan for a cohesive future in which NS/EP and public safety communications increasingly co-exist and intermingle with each other and with commercial services in converged networks, and share specialized services to fulfill their unique requirements. Policies regarding missions and communications should be thoughtfully structured to ensure that the Nation's interests are best served in light of these trends.

The functional alignment and broad stakeholder engagement recommended above can provide an institutional forum for NS/EP and public safety stakeholders to consider these trends. This forum would also allow NS/EP and public safety stakeholders to make recommendations to update the definitions and policy frameworks for NS/EP and public safety communications to better reflect their increasing intersection.

One area of focus should be updating overarching Federal NS/EP policies. Although E.O. 13618 codifies the importance of NS/EP communications, NS/EP policies remain outdated, focusing primarily on circuit-switched, voice communications. The 2012 *NSTAC Report to the President on Cloud Computing* studied the definition of NS/EP telecommunications in the 2010 Code of Federal Regulations (CFR), 47 CFR § 201.2(g), and determined that it should be updated to reflect the current technology landscape.[66] The NSTAC believes that while the 2010 definition is authoritative, it did not account for newer technology and information services like cloud computing.

The ExCom developed a definition for NS/EP communications that was released to Federal departments and agencies in September 2012. The NSTAC found the new definition to be ambiguous, and supports a re-examination of the definition as technical and operational changes require.

Ambiguity in the definition of NS/EP itself makes coordinating NS/EP and public safety missions difficult.[67] Each mission has unique aspects (e.g., Continuity of Operations and Continuity of Government for NS/EP and daily operational activities for public safety), but updating and aligning overreaching policy to clarify how and the extent to which NS/EP and public safety missions intersect, and ensuring that those missions are complementary, will enable more effective and efficient coordination across all levels of government and jurisdictions.

Many Federal public safety communications policies were updated and codified by P.L. 112-96. Senior officials should review these policies for completeness and to consider intersections with NS/EP policies. For example, as discussed in Section 2.3.2, while the NSTAC found an authoritative definition for "public safety services" in P.L. 112-96, Section 6001 (27), and also located authoritative definitions for "public

[66] United States, DHS, National Security Telecommunications Advisory Committee, *Report to the President on Cloud Computing,* May 2011. Available from http://ncs.gov/nstac/reports/2012-05-15%20NSTAC%20Cloud%20Computing.pdf.

[67] Although there is no definition for NS/EP, there is a definition for NS/EP Communications found in 47 C.F.R § 201.2(g): "[NS/EP] telecommunications services, or NS/EP services, means those telecommunication services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States." In addition, the ExCom developed a definition of NS/EP communications, which can be found in Section 2.1 of this report.

safety officers" and "emergency response providers," it was unable to locate an authoritative definition for "public safety" itself.

3.3.3 Managing Change

The growing synergies in communications requirements, as described in Section 3.2, lead to an increasing need to coordinate communications policies, requirements, and standards across diverse missions and interests. However, that coordination may prove difficult as organizations reasonably focus on individual responsibilities, missions, and budgets. Managing coordination and alignment of these requirements, missions, and interests will require leadership and vision, appropriate representation of all stakeholders, and agility, prioritization, and mechanisms to identify and address impediments.

Leadership and Vision

Fostering change will require the leadership and personal involvement of senior officials with the vision and authority to overcome bureaucratic and cultural challenges. Public safety officials noted that the large and diverse set of public safety stakeholders, each focused on jurisdictional responsibilities, organizational missions, and budgets, naturally creates cultural and technical challenges that hinder coordination, especially for nationwide initiatives. This is also true for Federal departments and agencies working across their own organizational boundaries. Without senior leadership and vision, these constraints—institutional, cultural, financial, technical—have little chance of being addressed to serve the Nation's interest.

Representation and Agility

This report notes that managing equities across this complex communications environment requires engaging and working with a broad and diverse stakeholder community that includes experts from Federal, State, local, territorial, and tribal governments, service providers, product vendors, and others with relevant NS/EP and/or public safety communications expertise and knowledge. Yet, the concept of representative participation will be particularly important and balancing inclusivity and agility will be essential. Organizations and decisions involving large numbers of stakeholders often find it challenging to make progress, which is further complicated when considering the rapidly evolving communications environment.

Prioritization

Various communications scenarios, capabilities, and requirements will be developed for NS/EP, public safety, and commercial purposes, and, even if synergistic, these items may not be identical; instead, they may have different technical requirements. Stakeholders will have to prioritize such requirements and their implementation carefully, recognizing that different users may have different priorities or believe that technical requirements are best met in different ways. Vendors too may have specific views on the best ways to meet NS/EP and public safety requirements.

Optimally, both the NS/EP and public safety users will recognize, appraise, and seek to act in partnership on communications concerns within the domain of their shared interests, such as network security, including credentialing and user identity management; access and prioritization; and mobile device interfaces and displays of information. Special attention must be paid in this shared-interest domain, lest small disagreements stall progress in larger and more important nationwide benefits.

Accountability and Oversight

Coordination among such a large and diverse community of stakeholders with some shared and competing interests will be difficult. The NSTAC seeks to facilitate that coordination by creating a process that documents key milestones and initiatives and identifies impediments so that they can be addressed. Reporting helps drive progress by ensuring that key stakeholders are aware of and have opportunities to inform implementation of the NSTAC's recommendations.

E.O. 13618 already requires the ExCom to develop a strategic agenda and quarterly reports related to its efforts to enhance the survivability, resilience, and future architecture of NS/EP communications. These documents serve two purposes. First, they make the ExCom accountable to the White House for progress made against the responsibilities assigned to it in E.O. 13618. Second, they offer the EOP an opportunity to oversee the ExCom's activities and provide the ExCom with recommendations to help it execute its responsibilities. The strategic agenda and quarterly reports can be augmented with information regarding implementation of the recommendations in this report.

3.4 Summary of Mutual Benefits

By identifying synergies among capabilities and requirements, NS/EP and public safety users will be able to reap many potential benefits. For example, they will:

- Achieve lower costs for acquisition. Service providers and product vendors will have fewer sets of requirements to meet, minimizing or eliminating costly special exceptions and increasing the market base for specialty devices and services.
- Attain greater interoperability of advanced communications among jurisdictions and levels of government, making collaboration more effective, especially in large, maximum stress events.
- Enable collaboration to help address issues related to a diversity of capabilities across jurisdictions.
- Build on the best practices developed in daily use by public safety and NS/EP users.

Coordinating requirements can also help to minimize areas of concern for NS/EP and public safety users. Some of those areas of concern include:

- Capacity of the NPSBN and commercial networks in times of congestion or disruption.
- Priority communications, including voice, video, and data for users, devices, and applications across networks.
- Security, when measures require considerable effort or expertise it is not often implemented, especially during crisis situations.
- Scalability, which is of increasing concern as incidents involve a greater number and diversity of potential NS/EP and public safety users leveraging advanced communications that require more bandwidth.

- Usability, since some technologies and systems seem overly complex and may require work-arounds or training to use properly.
- Accessibility, as NGN broadband communications requirements and systems must support authorized NPSBN and NS/EP users with disabilities who rely on alternative methods for communication (e.g., video relay, TTY) or who are not proficient in English.[68]

Coordination, particularly during this timely opportunity as both groups define requirements, will also enable both NS/EP and public safety users to share their respective expertise on issues such as interfaces, training, capital expenditures, and liability. For example, for years, NS/EP communications have been required to function nationwide, as explained in Section 3.3; NS/EP communications stakeholders may have insights to share with public safety on how to achieve this nationwide scalability. Similarly, public safety users are performing their mission day-to-day, so they may have insights and innovations to share with NS/EP stakeholders.

The ubiquitous availability of broadband infrastructure, including the NPSBN once deployed, the exponential increase in devices to access that infrastructure, and the growth in cloud-based services present the opportunity to improve effectiveness and efficiency across NS/EP and public safety communications. However, availing ourselves of this opportunity is not guaranteed. Success will depend, in part, upon bringing the NS/EP and public safety stakeholders together and encouraging them to collaborate on areas of shared interests. If NS/EP and public safety stakeholders do not take advantage of this timely opportunity, achieving mutual benefits will be difficult and there will be an inevitable negative impact on NS/EP and public safety users' abilities to fulfill their respective missions in the long-term.

4.0 PRIORITY COMMUNICATIONS

NS/EP and public safety users require continuous communications to fulfill their respective missions; priority services help to ensure that these users have communications when networks are congested or degraded. While this critical requirement has historically focused on voice communications, prioritization of data, image, video, and various other multimedia applications is increasingly important as those types of communications become integrated into day-to-day operations. Coordination of priority communications requirements is necessary to ensure that the diverse community of all users—both NS/EP and public safety—have the reliable, prioritized communications they need as their services traverse various networks.

4.1 Communications Resiliency

Communications resiliency is a fundamental tenant of the NS/EP mission as well as a statutory requirement of the NPSBN.[69] Ensuring resilient voice communications will continue to be imperative, but reliable, resilient, and prioritized data, video, and other communications will become increasingly important. The NSTAC highlighted the importance of communications resiliency and made associated recommendations in its 2011 *NSTAC Report to the President on Communications Resiliency*.[70] In that

[68] P.L. 93-112 § 504-508.

[69] E.O. 13618 (b)(2)(A).

[70] United States, DHS, National Security Telecommunications Advisory Committee, *Report to the President on Communications Resiliency*, April 2011. Available from

report, the NSTAC noted that communications resiliency must be assured even as technologies, networks, and services evolve.

Communications resiliency must be ensured under adverse conditions, including network equipment failures, operational faults, natural disasters, and cyber attacks. It can be improved in a variety of ways, including through the use of hardened facilities, redundant network equipment, diverse routing of communications traffic, use of deployable communications capabilities, and access to alternative communications networks. Each of these mitigations comes at some cost, and compromises often must be made to balance the costs with the expected benefits. For example, while providing access to numerous alternative communications networks (e.g., through multiband devices) would improve resiliency, the significant costs and technical challenges associated with incorporating numerous frequency bands into devices prohibits service providers, product vendors, and users from pursuing that approach.

Resilience is critical to all NS/EP and public safety communications.

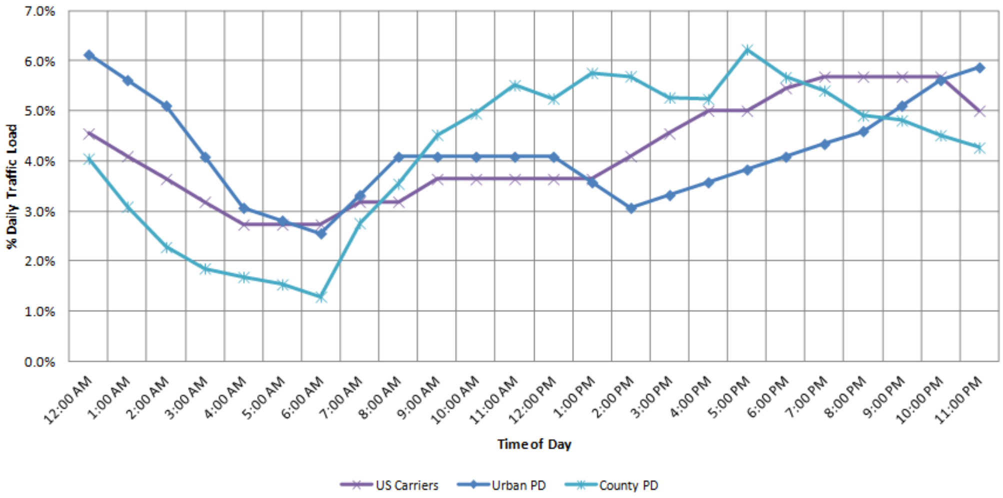
- **E.O. 13618:** Requires NS/EP communications to be available "at all times and under all circumstances."
- **P.L. 112-96:** Requires NPSBN to be built with resiliency that will ensure effective public safety communication.

Communications resiliency can also be improved by providing priority communications to NS/EP and public safety users. Priority communications allow service providers to treat authorized communications with a higher level of priority than that of other traffic (e.g., commercial traffic) and may also allow some types of communications to be treated with a higher level of priority over another. The ability for both NS/EP and public safety users to effectively perform their missions, especially during significant events, could be severely curtailed if their communications are not treated with an appropriate level of priority on the networks they utilize.

Under normal operating conditions, broadband networks have sufficient capacity to satisfy NS/EP, public safety, and commercial requirements without the need for priority. However, when these networks are heavily loaded, priority communications become critical, as multiple users and applications compete for finite network resources. Experience has shown that demand for communications is often geographically concentrated around an incident or problem area. During an incident, public safety communications traffic increases as numerous public safety organizations and users respond; similarly, commercial communications traffic increases as the general public call or text family members, attempt to contact emergency services, or attempt to use social networks. Traffic trends for public safety and commercial communications are closely correlated; when incidents occur, all networks may become congested. Figure 8 illustrates the typical traffic load for a day and shows a close correlation between wireless service providers and public safety network loading.

http://www.ncs.gov/nstac/reports/NSTAC%20Report%20to%20the%20President%20on%20Communications%20Resiliency%20(2011-04-19)(Final)(pdf).pdf.

Figure 8: Wireless Service Providers and Public Safety Traffic Trends[71]



4.2 Priority Communications for NS/EP

The Federal Government has long recognized the importance of NS/EP communications, and priority for those communications during times of crisis. Authority to establish priority services was provided at the inception of the NCS and is an integral part of DHS' mission to coordinate the planning and provision of NS/EP communications for the Federal Government.[72] DHS' strategy to fulfill this part of their mission is designed to achieve cost-effective priority communications by leveraging commercial networks and the associated capabilities of the communications sector. In support of that strategy, DHS initially developed two programs to facilitate priority access to commercial networks: GETS and WPS.

GETS provides emergency access and priority processing in the local and long distance segments of the public switched telephone network (PSTN) via a calling card mechanism. It is intended to be used in an emergency or crisis situation when the PSTN is congested and the probability of completing a call over normal or other alternate telecommunication means has significantly decreased. GETS supports Federal, State, local, and tribal government, industry, and NGO personnel in performing their NS/EP and public safety missions.

WPS is a priority calling capability that greatly increases the probability of call completion while using cellular phones during emergencies. WPS provides priority for emergency calls through a combination of special cellular network features and the same high probability of completion features used by GETS. Key Federal, State, local, and tribal government, and critical infrastructure personnel are eligible for WPS; public safety users may qualify for WPS, as well.[73]

[71] DeRango, M., Vice President, Advanced System Architecture, Chief Technology Office, Motorola Solutions, *Response to the NSTAC NPSBN Subcommittee Questions on Wireless Broadband Technology Demonstrator Broad Agency Announcement - BAA 12-10*. September 20, 2012.

[72] E.O. 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*. Rescinded July 2013.

[73] United States, DHS, Wireless Priority Service, *Program Information Home Page*. Available from https://www.dhs.gov/wireless-priority-service-wps. As part of the online WPS Service Request, participating

Capabilities needed to provide priority communications for NS/EP users in the NGN have not been adequately resourced; current priority service capabilities are quickly becoming obsolete as commercial networks transition to IP-based broadband communications.

GETS and WPS are designed for use on legacy circuit-switched commercial networks. Both are limited to voice and voice-band data communications; neither supports priority for data, video, or other non-voice applications. As a result, GETS and WPS are quickly becoming obsolete as commercial network providers rapidly deploy IP-based broadband networks. This trend is complicated by spectrum utilization in wireless networks. Cellular spectrum is a limited resource that carriers carefully and judiciously manage. WPS uses second-generation (2G) wireless technology, which is being phased out in favor of third- and fourth-generation technologies.[74] For example, one wireless service provider plans to sunset its 2G network in 2016, and a second will sunset its 2G network in 2021.[75] Given this trend, priority capabilities will be unable to fulfill the NS/EP mission in the near future and must evolve to operate over the NGN.

IP-based networks provide significant advantages to service providers, products vendors, and consumers, but providing priority communications over these networks is more complex than over circuit-switched networks. All packets for IP-based communications that traverse multiple networks must have an assigned priority to ensure proper priority treatment. Appropriate QoS levels must be maintained at the end points and across networks in order for service to function as expected. In order to achieve this, networks have rules regarding the treatment of different types of communications and what, if any, priority may be authorized. These rules address what packets must be processed immediately and what packets can be buffered for later processing. Depending on the applications or services involved, the acceptable sensitivity for message transmission can be milliseconds, seconds, or up to days of delay if necessary for some machine-to-machine communications (e.g., smart meter data). Voice and video applications are generally more sensitive to packet delays or lost packets, resulting in distorted sound or lost pixels/frames for users.

DHS has been working with commercial service providers and product vendors to develop NGN priority voice, video, and data services to support NS/EP users.[76] NGN priority service is designed as the successor to GETS and WPS, providing authorization for and transport of NS/EP communications across NGNs. The long-term objective of NGN priority service is to facilitate priority for all IP-based

organizations qualify eligibility of each WPS user based upon five categories of WPS NS/EP criteria established by the NCS: (1) executive leadership and policy makers; (2) disaster response/military command and control; (3) public health, safety, and law enforcement command; (4) public service/utilities and public welfare; and (5) disaster recovery.

[74] Welsh, S., *The 2G Sunset has Begun,* SDM Magazine, March 2013. Available from http://www.sdmmag.com/articles/the-2g-sunset-has-begun.

[75] Svensson, P., *AT&T Sets Deadline for 2G sunset in 4 Years,* Associated Press, August 3, 2012. Available from http://www.washingtontimes.com/news/2012/aug/3/att-sets-deadline-for-2g-sunset-in-4-years/
Kim, G., *PSTN Transition Will Happen; Only Issue is How,* TMCnet.com, January 30, 2013. Available from http://www.tmcnet.com/topics/articles/2013/01/30/324996-pstn-transition-will-happen-only-issue-how.htm.

[76] NGN priority services are envisioned to enable priority by providing temporary pre-defined priorities for NS/EP users among all commercial users. Users receive static (constant) priority when activated and end-user triggered priority based on the NGN priority services model. When activated, NGN priority services would allow priority for users' pre-defined set of applications, but are not non-preemptive in nature.

communications, including voice, data, and video. The initial phase of the NGN priority service will address voice priority via voice over IP, while later phases will address priority for data and video applications.

DHS has worked with service providers and product vendors to specify how priority NS/EP voice, video, and data communications would be implemented in NGNs.[77] DHS is also currently developing and deploying IP-based priority features in the core portion of commercial networks to extend the service life of GETS and WPS. Development of a functional NGN priority service capability and extension of GETS and WPS, however, has been hindered by lack of resources and appropriate funding prioritization considering the decline of operational capabilities to support mission requirements. As commercial service providers, product vendors, and application developers rapidly deploy advanced communications capabilities and technologies, the ubiquity and effectiveness of GETS and WPS for priority voice, and NS/EP communications in general, will continue to decline. The lack of operational capabilities to meet NS/EP requirements for priority voice in the NGN places the NS/EP mission at significant risk.

Immediate actions, including those to implement NGN priority service, are required to ensure that priority communications are sufficiently resourced to support mission requirements in the NGN. This recommendation was previously made by the FCC's Communications Security, Reliability, and Interoperability Council and was reiterated by the NSTAC in its 2011 *NSTAC Report to the President on Communications Resiliency*.[78, 79]

4.3 Priority Communications for Public Safety

Public safety operations require effective command, control, coordination, communication, and information sharing to support first responders, including police, firefighters, emergency medical technicians, and other public safety users. Personnel at all levels of government and across multiple disciplines must be able to communicate as authorized and when needed, regardless of circumstances. During an emergency, not all public safety users have the same needs; by nature, public safety operations are situational. Priority requirements must provide for elevated treatment, depending on various factors such as role, location, and communications type, for users, devices, and applications. Importantly, public safety users expect to have not only priority, but also preemption, when necessary.[80]

[77] For example, DHS and industry coordination has resulted in the creation of two relevant Government-Industry Requirements (GIR) documents: the *IMS* (IP Multimedia Subsystem) *GIR for NS/EP NGN Priority Services* and the *LTE Access Network GIR for NS/EP NGN Priority Services*. A number of key mechanisms to enable traffic prioritization have been presented to industry forums for standardization.

[78] United States, Federal Communications Commission, Communications Security, Reliability and Interoperability Council, Working Group 7: Pandemic Planning: Priority Service Requirements, *Final Report: Planning for NS/EP Next Generation Network Priority Services During Pandemic Events*. December 2010, p. 3. Available from http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG7_Final_Report_NGN_Priority_20101216.pdf.

[79] United States, DHS, National Security Telecommunications Advisory Committee *Report to the President on Communications Resiliency,* April 2011. Available from http://ncs.gov/nstac/reports/NSTAC%20Report%20to%20the%20President%20on%20Communications%20Resiliency%20(2011-04-19)(Final)(pdf).pdf.

[80] Preemption indicates instant access to resources for a user, at times disconnecting other users, while a priority user may not receive instantaneous access.

Public safety users expect to have dynamic, incident-based priority based on responders' situations. This dynamic priority could be activated by the responder, an incident commander, or a dispatcher and could preempt other traffic as authorized and needed to ensure resilient, prioritized communications for public safety users. These users also expect to have the ability to immediately invoke changes in priority, such as at times of imminent peril, to meet a sudden and urgent request for aid. This functionality must be as simple as pressing an emergency button that would elevate their communications to the highest level of priority. Priority is just as important for public safety communications as it is for NS/EP communications.

The NPSTC Broadband Working Group's Priority and QoS Task Group published a report in April 2012 on priority and QoS on the NPSBN.[81] It outlined public safety priority and QoS needs and use cases for the 700MHz NPSBN. The report noted that the needs of various public safety organizations are unique and can vary over both the short- and long-term, requiring flexibility be built into any policies, plans, and schemas for priority and QoS. It also noted that priority and QoS requirements will have to be modified as the NPSBN and advanced communications technologies, applications, and services evolve.

4.4 Providing End-to-End Priority to Assure Critical Missions

All levels of government require seamless voice, video, and data broadband communications across networks to accomplish their missions and respond in times of crisis. These communications must be capable of being prioritized across multiple networks, devices, applications, and services.

Given the potential for numerous levels of responders to be involved in any event, especially during response to NS/EP events, and the interconnected and changing network environment through which communications move, providing priority communications will require existing and emerging priority schemas continue to be advanced. These circumstances also create a strategic opportunity to develop more cohesive priority policies and schemas moving forward. By leveraging current capabilities and developing more efficient and effective capabilities for the future, priority communications can be available to ensure both NS/EP and public safety missions and interaction between and among their users not only on commercial networks, but also as users and their services move among networks that continue to evolve over time.

NPSTC is developing a technical schema for priority communications on the NPSBN, but the overarching policy framework for priority on the NPSBN is still to be developed by the FirstNet Board.

Three high-level use cases must be considered to ensure priority communications for NS/EP communications; the same three scenarios apply when seeking to ensure priority for public safety communications. These use cases are:

- **Priority on the NPSBN**: Priority for communications on the NPSBN will be determined by the FirstNet Board. This determination includes the level of priority for all authorized NPSBN users, including public safety, who are statutorily defined as primary users of the NPSBN, and any

[81] National Public Safety Telecommunications Council, Broadband Working Group Priority and QoS Task Group, *Priority and QoS in the Nationwide Public Safety Broadband Network*, April 17, 2012. Available from http://www.npstc.org/download.jsp?tableId=37&column=217&id=2304&file=PriorityAndQoSDefinition_v1_0_clean.pdf.

other users authorized by the FirstNet Board. P.L. 112-96 authorizes the FirstNet Board to include priority communications in its network design and requires the FirstNet Board to consult with State and local government representatives in assigning priority access to public safety users.[82]

Public safety users expect that their communications on the NPSBN will come with a default priority, based on normal, daily roles and responsibilities, and include preemption when needed. Priority is expected to be implemented and functioning at all times on the NPSBN rather than on a per-session basis, though priority can change based on situational needs.

NS/EP users may not be afforded the same level of priority on the NPSBN as they have on commercial networks through GETS and WPS. As a private network, the NPSBN is likely not subject to common carrier regulations under Title II of the *Communications Act of 1934*.

- **Priority on commercial networks:** Access to commercial networks for public safety users is important because it may provide them with communications wherever or whenever the NPSBN is not available, such as during build-out or when the NPSBN becomes congested.

  P.L. 112-96 authorizes the FirstNet Board to negotiate arrangements with commercial service providers for access to and priority on their networks; the type of arrangement it establishes will affect the ability of public safety communications to receive priority access and routing on those networks. In briefings, the NSTAC heard that public safety users may want to be granted priority treatment for their communications on commercial networks in a manner that is as close as possible to what they are afforded on the NPSBN; whether they will be able to achieve that goal remains to be seen. According to P.L. 112-96, the FCC "may adopt rules, if necessary, in the public interest, to improve the ability of public safety networks to roam onto commercial networks and to gain priority access to commercial networks in an emergency if such access does not preempt or otherwise terminate or degrade all existing voice conversations or data sessions."[83]

  Priority communications for NS/EP users on commercial networks are expected to be fulfilled by the existing GETS and WPS priority services, and eventually by the NGN priority services that DHS is developing. These priority communications capabilities may be available to public safety users that otherwise qualify as NS/EP users.

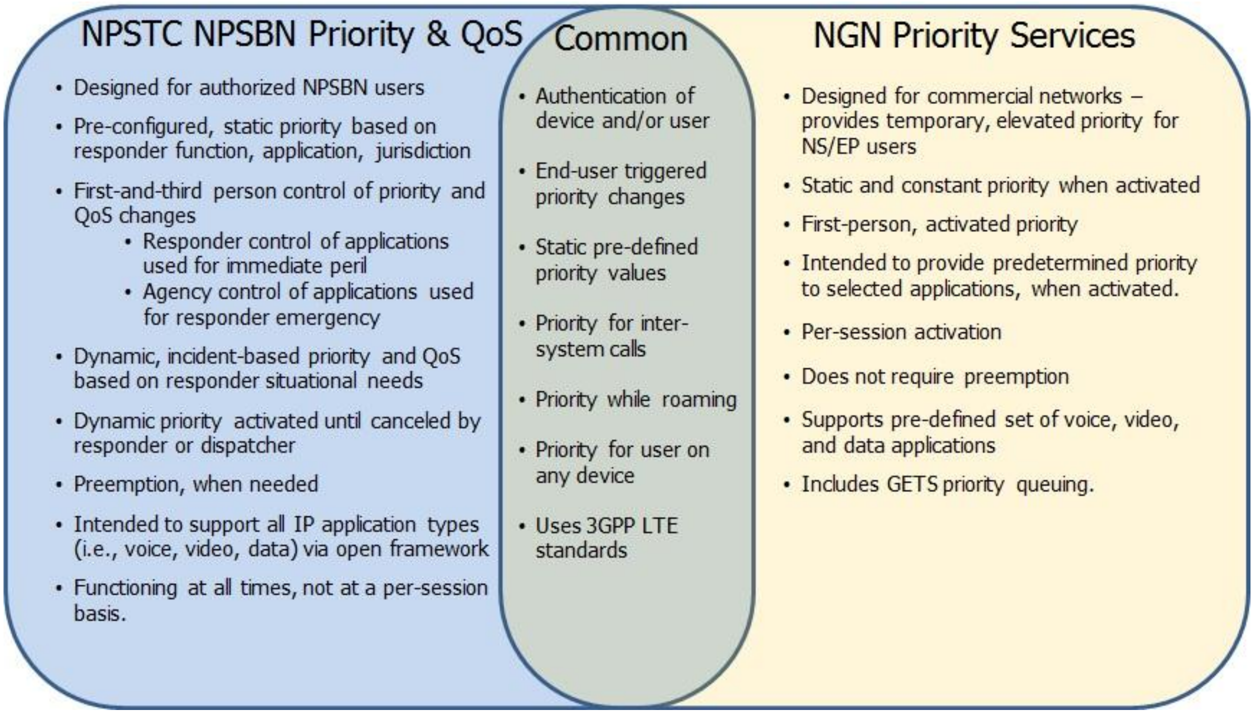
- **Priority among networks**: The likelihood that public safety communications will frequently move between the NPSBN and commercial networks, and the possibility that some NS/EP communications may be authorized on the NPSBN by FirstNet and, therefore, also moving between commercial and private networks, gives rise to several additional use cases for priority communications. The use cases include public safety communications that originate or terminate on either the NPSBN or on a commercial network, as well as NS/EP communications that traverse these different networks, and multiple data types.

  Appendix J, *Scenarios*, identifies eight scenarios that can be expected when NS/EP and public safety users originate, receive, and traverse between the NPSBN and commercial networks. It also addresses the inter-system priority considerations that arise with each.

[82] P.L. 112-96 § 6206(c)(2)(A)(v).
[83] Ibid. § 6211(3).

As noted, fulfilling the priority communications needs for NS/EP and public safety users will require the existing NS/EP priority services (i.e., GETS and WPS) and the emerging priority schema for the NPSBN being developed by NPSTC to coexist in the immediate future. Technically, priority is provided in different ways on the variety of networks (e.g., LMR, circuit-switched voice, private IP-based network, commercial IP-based networks) currently being used by NS/EP and public safety users. Both schemas can be used simultaneously as the underlying technical mechanisms utilize Third Generation Partnership Project (3GPP) LTE standards. Figure 9 provides a comparison of the NPSTC priority and QoS framework applicable to communications on the NPSBN and the NGN priority services framework applicable to NS/EP communications on commercial networks. From a technical perspective, additional levels of priority may be assigned to traffic on NPSBN than can be granted on commercial networks, and a translation function will be required for traffic to move between networks and receive priority. Users should understand that their priority experiences will differ on different networks.

Figure 9: Comparison of NPSTC Priority and QoS Schema with DHS NGN Priority Services Schema[84]



NPSTC NPSBN Priority & QoS

- Designed for authorized NPSBN users
- Pre-configured, static priority based on responder function, application, jurisdiction
- First-and-third person control of priority and QoS changes
  - Responder control of applications used for immediate peril
  - Agency control of applications used for responder emergency
- Dynamic, incident-based priority and QoS based on responder situational needs
- Dynamic priority activated until canceled by responder or dispatcher
- Preemption, when needed
- Intended to support all IP application types (i.e., voice, video, data) via open framework
- Functioning at all times, not at a per-session basis.

Common

- Authentication of device and/or user
- End-user triggered priority changes
- Static pre-defined priority values
- Priority for inter-system calls
- Priority while roaming
- Priority for user on any device
- Uses 3GPP LTE standards

NGN Priority Services

- Designed for commercial networks – provides temporary, elevated priority for NS/EP users
- Static and constant priority when activated
- First-person, activated priority
- Intended to provide predetermined priority to selected applications, when activated.
- Per-session activation
- Does not require preemption
- Supports pre-defined set of voice, video, and data applications
- Includes GETS priority queuing.

4.5 Convergence of Priority Policy

With the increasing convergence of the NS/EP and public safety missions and the coexistence and possible intermingling of their communications on both the NPSBN and on commercial networks, coordination by key stakeholders of the priority communications policy frameworks and associated technical schemas to support the NS/EP and public safety missions is necessary. Well-coordinated frameworks and schemas will enable users to have a more seamless experience, will enhance mission effectiveness, and will reduce costs for capital investments as well as those costs associated with skilled workers to manage increasingly diverse technologies. Importantly, the decision to utilize commercial

[84] Derived from Miller, T., Chief Technology Office, Motorola Solutions *NSTAC Priority and QoS on the NPSBN*, August 14, 2012.

standards and technologies (i.e., LTE) for the NPSBN makes reconciliation of NS/EP and NPSTC priority schemas technically feasible.

As highlighted in the scenarios in Section 4.4 and use cases in Appendix H, *Lessons Learned from GETS/WPS*, providing end-to-end priority for NS/EP and public safety communications is a complex task in today's diverse communications environment. Priority considerations must be applied to users, devices, and applications across numerous interfaces, including initial network access, requests to establish communications paths in the network, processing of packets using QoS, router functionality, and network gateways. End-to-end priority therefore requires careful engineering of the diverse components and interfaces that cross multiple access and core networks (which could include NPSBN, commercial LTE networks, satellite networks, deployable systems, etc.), and external service networks that connect various users, devices, applications, and services.

While engineering is complicated by the diversity of networks, as shown in Figure 9, the NPSBN priority schema and NGN priority services have many similar technical requirements, including authentication of users and devices. Reconciling the priority policies and schemas will help achieve comparable functionalities for the users across these priority service platforms, reduce costs through standardization and economies of scale, enable service providers and product vendors to rationalize provisioning strategies, simplify engineering of these services, move toward a seamless user experience, and support rapid innovation.[85] These synergies are important to realize moving forward, particularly as budgets continue to become more constrained; governments will have limited resources available to develop or fund the necessary solutions to continue to address the broad diversity of priority communications scenarios.

The intent of coordinating these policy frameworks is to ensure end-to-end priority communications for a diverse user base of NS/EP public safety users and for various types of communications (i.e., voice, video, and data). Fulfilling end-to-end priority communications requirements for these diverse users, and their devices, applications, and services across a mesh of interconnected networks will require significant coordination, as well as a common understanding of similarities and differences in technical requirements and concerns for both NS/EP and public safety users.

5.0 FINDINGS, CONCLUSIONS, AND RECOMMENDATIONS

A diverse set of industry and government stakeholders and SMEs participated in and contributed to the NSTAC's examination of the NS/EP implications of the NPSBN. The findings and conclusions presented in Section 5.1 represent the combined expertise and insights from this set of stakeholders and SMEs, who engaged actively to help all responders have the most advanced communications capabilities to fulfill their missions. The findings and conclusions also directly support the recommendations listed in Section 5.3.

[85] For example, existing communications prioritization efforts, such as the DHS IMS and LTE GIRs that have already addressed such common technical requirements, can be beneficial in expediting the development of an effective and efficient uniform approach.

5.1 Findings

The Communications Environment and the NPSBN

1. **NGN Adoption.** IP-based broadband networks will enable NS/EP and public safety users to take advantage of current and emerging technologies and capabilities to better fulfill their missions. To date, adoption of NGN technologies for Government-sponsored communications has been limited for a variety of reasons, such as funding and reliability concerns.
2. **NPSBN.** The NPSBN is the first effort at a nationwide, standardized network to provide public safety users with access to advanced, broadband communications. P.L. 112-96 identifies public safety users as primary users of the NPSBN.
3. **NS/EP Access to the NPSBN**. P.L. 112-96 authorizes FirstNet to determine, in consultation with Federal, State, tribal, and local public safety entities, the Director of NIST, the FCC, and the PSAC, how to manage NPSBN access and usage for both public safety and non-public safety users, as well as the levels of priority afforded to each. The FirstNet Board is also authorized to determine what levels of access, usage, and priority will be provided to NS/EP users on the NPSBN.

Alignment

1. **Complementary Missions.** NS/EP and public safety missions are related in various ways. Most NS/EP events, though led by Federal officials and responders, start as local events and therefore require and depend on the integrated contributions of responders across all levels of government throughout response and recovery stages.
2. **Maximizing Limited Resources to Perform the Mission**. As technologies become more diverse, the skills required to manage them become more advanced, and resources become more constrained, NS/EP and public safety officials have indicated a need to collaborate across jurisdictions and develop services that can be shared to optimize limited resources and improve mission effectiveness.
3. **Synergistic Capabilities and Requirements**. NS/EP and public safety representatives described leveraging similar communications capabilities (e.g., information management, cross-agency coordination, resource management, and situational awareness) to fulfill their missions. Both are defining requirements for future capabilities as part of their respective transitions to advanced broadband networks. Coordination will enable both NS/EP and public safety users to identify similarities and differences among communications requirements to achieve and maximize the benefits of a larger user base.
4. **National and Homeland Security Needs.** Coordination of requirements will help to ensure that service providers and product vendors can develop interoperable and scalable solutions to meet NS/EP and public safety users' unique homeland and national security needs.
5. **Scalability and Resiliency**. NS/EP and public safety communications can also benefit by coordinating efforts to develop standards, fund R&D, initiate pilots, and allocate grants to address similarities and differences in their communications requirements. Coordinating standards not only will promote interoperability, but also will improve scalability and resiliency. Policies that enable NS/EP and public safety communications to easily move between private and commercial networks will also improve scalability and enhance communications resiliency.

6. **Accessibility**. NGN broadband communications requirements and the resulting systems need to support authorized NPSBN and NS/EP users with disabilities who rely on alternative methods for communication (e.g., video relay, TTY) or who are not proficient in English.
7. **Innovation.** Current commercial networks and end user devices provide important capabilities, but are not designed or engineered to meet all NS/EP and public safety scenarios. Incentives and investments are needed to promote innovation in the delta between commercial marketplace requirements and NS/EP and public safety requirements. Once the NPSBN is implemented, public safety users are likely to drive more innovation, given their relatively larger user base and daily activities in support of their mission.
8. **Sharing Lessons Learned.** NS/EP and public safety communications will benefit from users sharing technical, operational, and policy lessons learned from their respective experiences exploring, acquiring, and using advanced communications technologies.
9. **Diverse Stakeholders.** Various Federal, State, and local groups, representing a range of jurisdictions and capabilities, are examining NS/EP and public safety communications separately. No single organization represents the communications interests of the large and diverse group of public safety users. Further, the NSTAC's review of relevant policies, composition, responsibilities, and functions of these groups found that none are representative of both NS/EP and public safety communications interests.
10. **Mutual Benefits**. Coordinating policies, requirements, and standards will help achieve economies of scale, reduced costs, improved interoperability, greater cross-jurisdictional cooperation, operational efficiencies, shared infrastructure for both steady state and response activities, and improved security, reliability, resiliency, and mission performance for all stakeholders.
11. **Near-Term Imperative.** The passage of P.L. 112-96 and the release of E.O. 13618 create a timely opportunity for coordination of public safety and NS/EP communications to achieve mutual benefits. If NS/EP and public safety leaders do not take advantage of this opportunity in the near-term, achieving mutual benefits will be difficult, and there will be an inevitable negative impact on NS/EP and public safety users' ability to fulfill their respective missions in the long term.
12. **Culture**. Disparate organizations are developing communications policies and requirements, and are prioritizing and funding standards, R&D, pilot programs, and grants for NS/EP and public safety communications separately. Their distinct roles and responsibilities do not require, and likely impede, integrated coordination across stakeholders. Senior leadership from NS/EP and public safety will be required to mitigate inherent tensions that may hinder coordination as organizations naturally focus on their individual responsibilities, missions, and budgets.

Cohesive Definitions

1. **NS/EP Events**. The full range of events requiring NS/EP communications has evolved over time. The NS/EP mission was originally focused on national security emergencies; however, as the number and type of threats of concern to the Federal Government has expanded, so has the NS/EP mission. As it has grown, so has the involvement of public safety users during NS/EP events.
2. **Out-of-Date and Ambiguous Definitions**. Essential NS/EP definitions, including an authoritative definition of NS/EP itself and NS/EP communications, are out-of-date or do not exist. The

NSTAC found ambiguity among the mission, composition, roles, and responsibilities of the NS/EP and public safety users and how they relate to each other.

3. **Clarity in a Complex Environment.** Given the multijurisdictional nature of response, the dependence on similar or shared technologies, networks, and applications, as well as the rapid rate of change in the communications environment, there is a clear need to update the definitions and policy frameworks for NS/EP and public safety communications to be intentionally complementary and account for technological innovation.

Priority

1. **NPSBN Capacity.** Until the NPSBN is fully deployed, commercial services will be used to augment existing public safety voice capabilities with advanced data communications. Even after the NPSBN is deployed, it may become congested. During the initial build-out or during congestion, NPSBN users, services, and applications will coexist, and possibly intermingle, with commercial users, services, and applications on carrier networks.
2. **Voice, Video, Data.** NS/EP and public safety voice, video, image, and data communications will traverse multiple networks. Ensuring priority for these communications will be critical at every network segment and interface in the end-to-end path, from access to routing.
3. **NS/EP Priority Programs.** On today's circuit-switched commercial networks, NS/EP voice communications have the highest priority for user traffic. The Federal Government has specified the technical requirements for moving NS/EP priority communications to NGN technology, but, to date, has not adequately resourced efforts to provide priority broadband communications in support of the NS/EP mission.
4. **Mission Critical Voice.** Public safety users described only limited use of the priority communications capabilities provided by DHS' NS/EP priority programs. They have and will continue to use LMR for mission critical voice until there is greater certainty that the NPSBN's LTE technology can fulfill reliability and functionality requirements.
5. **Priority on the NPSBN.** The FirstNet Board will determine priority on the NPSBN, including priority for NS/EP users.
6. **Priority on Commercial Networks**. How the FirstNet Board chooses to have public safety communications traverse commercial networks, whether via roaming, service-level agreement, or another contractual arrangement, will affect the ability of public safety communications to receive priority access and routing on those networks. Fulfilling the priority access needs of NS/EP and public safety communications will require current schemas to coexist in the near future while public safety communications utilize LMR, NPSBN, and commercial services.
7. **Priority among Networks**. The decision to utilize commercial standards and technologies (i.e., LTE) on the NPSBN makes reconciling NS/EP and NPSTC priority schemas technically feasible. Reconciliation of priority policies and schemas will help achieve comparable functionalities for users across platforms; reduce costs through standardization, streamlined engineering, and economies of scale; and enable providers and vendors to rationalize provisioning strategies and innovate more rapidly.

5.2 Conclusions

The NSTAC offers the following conclusions:

- NS/EP and public safety communications must meet functional requirements for interoperability, end-to-end priority, security, reliability, and scalability under all circumstances and at all times.
- Federal, State, and local NS/EP and public safety policy makers and stakeholders need to act now to coordinate communications requirements as part of their respective transitions to advanced broadband-enabled capabilities. Coordination of requirements will help both user groups realize mutual benefits and avoid separate solutions that are incompatible or exist within silos.
- NS/EP and public safety users should leverage scarce resources by coordinating incentives and investments to promote innovation in the delta between commercial marketplace requirements and NS/EP and public safety requirements.
- Policy frameworks need to be updated by a broad set of stakeholders to ensure mission effectiveness now and in the future. Senior leadership from all levels of government is needed to facilitate implementation of NSTAC recommendations. From a Federal Government perspective, it will be important to track progress and identify challenges.
- DHS' priority services program(s) should be adequately resourced to ensure priority communications on commercial networks in the NGN environment.

5.3 Recommendations

The NSTAC recommends that the President advance recommendations that rationalize NS/EP and public safety **organizations and functions**, update and align **policies**, direct **technical initiatives**, require **reporting** to facilitate implementation, and address **funding** gaps. Specifically, the President should focus on the following areas and actions:

1. **Organizational Roles, Responsibilities, and Relationships.** Direct the NSS to evaluate and, as needed, recommend statutory or other policy improvements to functionally align and streamline Federal NS/EP and Federal public safety NGN communications organizations, and their responsibilities and functions. This alignment should be broadly focused across the Federal Government, but exclude independent authorities such as the Federal Communications Commission (FCC) and the First Responder Network Authority (FirstNet) Board. The evaluation and recommendations are intended to institutionalize coordination, improve mission effectiveness, and optimize the use of scarce resources for both NS/EP and public safety communications. The NSS should:
    a. Be informed by stakeholders through outreach and partnerships.
    b. Ensure that stakeholders include representatives from Federal, State, local, territorial, and tribal public safety organizations, service providers, product vendors, and other entities with relevant NS/EP and/or public safety communications expertise and knowledge.
    c. Establish a process enabling stakeholders to participate in or advise, as appropriate, the resulting functionally aligned and streamlined organization(s) so that NS/EP and State, local,

territorial, and tribal public safety communications can complement each other as circumstances evolve.

d. Examine and make recommendations to ensure that the NSTAC membership and functions represent the full range of industry knowledge and expertise of NS/EP and public safety communications to provide the President with advice to ensure communications at all times and under all circumstances.

2. **Policy Changes.** Direct the organization(s) with the appropriate responsibilities and functions identified as a result of Recommendation 1 to lead a cross-governmental, public-private, integrated effort to: (1) update NS/EP policies; and (2) align Federal NS/EP and Federal public safety communications policies, requirements, and standards to ensure that the interests of the Nation are best served. The alignment must support the ability of all stakeholders to coordinate and execute their NS/EP and public safety missions consistent with the National Incident Management System. To further this goal, direct the new organization(s), including stakeholders listed in Recommendation 1, to propose updates to overarching NS/EP policies, including the definition of NS/EP communications, the definition of NS/EP, and the mission and composition of NS/EP relative to public safety. As appropriate, make associated legislative and regulatory recommendations to:

   a. Reconcile priority communications policies and regulations (e.g., *FCC Second Report and Order providing Establishment of Rules and Requirements for Priority Access Service*) to account for and enable priority on all data types (e.g., voice, video, data) for NS/EP and public safety communications on commercial networks.

   b. Update national strategies (such as the *National Response Framework* and the *National Emergency Communications Plan*) and initiatives to account for advanced NGN communications capabilities, such as the NPSBN, and to reflect the evolving communications environment.

3. **Technology Initiatives.** Direct the organization(s) with the appropriate responsibilities and functions identified as a result of Recommendation 1 to lead a cross-governmental, public-private, integrated effort to:

   a. Identify similarities and differences in NS/EP and public safety NGN communications requirements, including those needed to meet "unique homeland security or national security needs" as required by Section 6206 (b)(2)(D) of P.L. 112-96 and in accordance with Section 3.3(a) of E.O. 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*.

   b. Review and recommend updates to priority schemas to account for and enable priority on all forms of NGN communications (e.g., voice, video, data) for NS/EP and public safety communications on commercial networks.

   c. Identify and recommend standards to meet requirements resulting from Recommendations 2 and 3(a).

   d. Identify and recommend opportunities for coordination and collaboration of research and development activities, grants, funding, pilots, and new standards that promote innovation to close the gap between commercial marketplace requirements and NS/EP and public safety requirements.

4. **Reporting Requirements.** Direct the NS/EP Communications Executive Committee, established by E.O. 13618, or its successor, to provide a status of the implementation of Recommendations 1, 2, and 3 above as part of the reporting requirements created in E.O. 13618, Section 3.3.
    a. Within six months, identify additional required tasks and develop and document a plan with milestones for addressing these tasks. Report these tasks and progress against milestones as part of the quarterly updates.
    b. Document tasks, milestones, and funding as part of the annual NS/EP communications strategic agenda.
    c. Distribute the quarterly updates and annual strategic agenda to the NSTAC chair to inform the NSTAC's ability to meet the functions defined in E.O. 12382, *President's National Security Advisory Committee.*
5. **Funding.** Request that Congress fully fund DHS' NGN priority service program(s) to ensure that advanced broadband communications priority services are fully developed, implemented, and operational before legacy priority systems are unable to support mission requirements.

LIST OF APPENDICES

The following appendices provide references to the data the subcommittee considered in creating this report:

APPENDIX A: MEMBERSHIP

NSTAC SUBCOMMITTEE MEMBERS

Computer Sciences Corporation (CSC)	Mr. Michael Laphen, Co-Chair Mr. Guy Copeland, Co-Leader
Microsoft Corporation	Mr. Scott Charney, Co-Chair Ms. Angela McKay, Co-Leader
AT&T, Incorporated	Mr. Brooks Fitzsimmons Ms. Elizabeth Gunn
Avaya, Incorporated	Mr. Mark Fletcher, ENP
CenturyLink, Incorporated	Ms. Kathryn Condello
Ciena Corporation	Mr. Robert Kimball
Communications Technologies, Incorporated	Mr. Milan Vlajnic
Department of Agriculture	Ms. Jessica Zufolo
Department of Commerce	Ms. Regina Harrison
Department of Homeland Security	Mr. Mark Becker Mr. Pat Amodio Ms. Nicole Sanchez
Ericsson, S.A.	Ms. Louise Tucker
Frontier Communications Corporation	Mr. Andy Robinson Mr. Michael Saperstein
Harris Corporation	Mr. Dennis Martinez
Intelsat General	Mr. Richard DalBello
Iridium Communications, Incorporated	Ms. Donna Bethea-Murphy
Juniper Networks, Incorporated	Mr. Robert Dix
Level 3 Communications, Incorporated	Mr. Denmark Litwinchuk
Lockheed Martin Corporation	Mr. Macy Summers
Motorola Solutions	Mr. Michael Alagna
Neustar, Incorporated	Mr. Richard Fruchterman
Palo Alto Networks, Incorporated	Mr. William Gravell

Raytheon Company	Mr. T.J. Kennedy Mr. William Russ
Rockwell Collins, Incorporated	Mr. Ken Kato
Sprint Nextel Corporation	Mr. Tony Wageman
Terremark Federal Group, Incorporated	Mr. Thomas Cannady
Vonage Holdings Corporation	Mr. Rohan Dwarkha

SUBJECT MATTER EXPERTS

AT&T, Incorporated	Mr. Stacey Black Mr. Martin Dolly Ms. Rosemary Leffler
CenturyLink, Incorporated	Ms. Stacy Hartman Ms. Susan Mohr Mr. Robert Morrill
Computer Sciences Corporation (CSC)	Mr. Richard Kaczmarek
Department of Agriculture	Mr. Christopher McLean
Department of Homeland Security	Ms. Rosalind Allen Mr. Rick Bourdon Mr. Peter Kim Mr. Ronald Hewitt Mr. Gabriel Martinez Mr. Douglas Maughan Mr. David Nolan Mr. Robert Rhoads Mr. Frank Suraci Ms. Carol-lyn Taylor
Ericsson, S.A.	Mr. Arun Hunda
Juniper Networks, Incorporated	Mr. James Bean
Microsoft Corporation	Mr. Paul Garnett Mr. Aaron Kleiner
Motorola Solutions	Mr. Mario DeRango Mr. Trent Miller Ms. Jane Wargo

Sprint Nextel Corporation	Mr. Richard Engelman Ms. Allison Growney Mr. Robert Kingsley Mr. Lawrence Krevor Mr. Nick Mangiardi
Terremark Federal Group	Mr. Don Hewatt Mr. Donald Tighe
Verizon Communications, Incorporated	Mr. Donald Brittingham Mr. Marcus Sachs

OTHER PARTICIPANTS

Akamai Technologies, Incorporated	Mr. Patrick Gilmore
AT&T, Incorporated	Mr. Jim Bugel
Avaya, Incorporated	Mr. Michael Stolker Mr. Daniel Wilson
Department of Homeland Security	Mr. Toby Lux
Level 3 Communications, Incorporated	Mr. Jack Water
McAfee, Incorporated	Mr. Ed White
Microsoft Corporation	Mr. David Bills
TE Connectivity, Ltd.	Mr. Philip Gilchrist

MANAGEMENT SUPPORT

Alternate NSTAC Designated Federal Officers	Mr. Allen Woodhouse Mr. Michael Echols
Department of Homeland Security	Ms. Suzanne Daage Mr. Julian Humble Ms. Deborah E. B. Keller
Booz Allen Hamilton	Mr. Mahesh Balagangadhar Ms. Megan Doscher Ms. Laura Karnas Ms. Katharine Willers

APPENDIX B: ACRONYMS

4G	4th Generation
5G	5th Generation
APCO	Association of Public Safety Communications Officials International
ASPR	Agreements, Standards, Policies, and Regulations
CDMA	Code Division Multiple Access
COP	Common Operational Picture
DARPA	Defense Advanced Research Projects Agency
DHS	Department of Homeland Security
DOC	Department of Commerce
DOD	Department of Defense
ECPC	Emergency Communications Preparedness Center
E.O.	Executive Order
EOP	Executive Office of the President
ExCom	NS/EP Communications Executive Committee
FCC	Federal Communications Commission
FirstNet	First Responder Network Authority
FOC	Full Operational Capability
GETS	Government Emergency Telecommunications Service
HSPD	Homeland Security Presidential Directive
IC	Immediate Capability
IOC	Initial Operational Capability
IP	Internet Protocol
IT	Information Technology
LMR	Land Mobile Radio
LTE	Long Term Evolution
NCS	National Communications System
NECP	National Emergency Communications Plan
NGA	National Governors Association
NGN	Next Generation Network
NGO	Non-Governmental Organization
NIMS	National Incident Management System
NIST	National Institute of Standards and Technology
NPSBN	Nationwide Public Safety Broadband Network
NPSTC	National Public Safety Telecommunications Council
NS/EP	National Security and Emergency Preparedness
NSS	National Security Staff
NSTAC	National Security Telecommunications Advisory Committee
NTIA	National Telecommunications and Information Administration
OEC	Office of Emergency Communications
P.L.	Public Law
PSAC	Public Safety Advisory Committee

PSTN	Public Switched Telephone Network
QoS	Quality of Service
R&D	Research and Development
RAN	Radio Access Network
RPH	Resource Priority Header
S&T	Science and Technology
SCADA	Supervisory Control and Data Acquisition
SME	Subject Matter Expert
TCP	Transmission Control Protocol
U.S.C.	United States Code
VPN	Virtual Private Network
WPS	Wireless Priority Service

APPENDIX C: GLOSSARY

Accessible: Refers to a site, facility, work environment, service, or program that is easy to approach, enter, operate, participate in, and/or use safely and with dignity by a person with a disability. (Americans with Disabilities Act)

Advanced Communications: Internet protocol (IP)-based broadband wireline and wireless networks, technologies, applications, and services. According to the *Twenty-First Century Communications and Video Accessibility Act*, the term `advanced communications services' means--(A) interconnected Voice Over IP (VoIP) service; (B) non-interconnected VoIP service; (C) electronic messaging service; and (D) interoperable video conferencing service.

Capacity: The information carrying ability of a telecommunications facility. What the "facility" is determines the measurement (e.g., you might measure a data line's capacity in bits per second). (Newton's Telecom Dictionary)

Circuit-Switched Network: A network that establishes a physical circuit temporarily on demand (typically when telephone or other connected device goes off hook) and keeps that circuit reserved for the user until it receives a disconnect signal. (Newton's Telecom Dictionary)

Cloud Computing: A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models. (National Institute of Standards and Technology Special Publication 800-145)

Commercial Networks: Communications networks that are owned and operated by the private sector.

Commercial Standards: The technical standards followed by the commercial mobile service and commercial mobile data service industries for network, device, and IP connectivity. Commercial standards include standards developed by the Third Generation Partnership Project (3GPP), the Institute of Electrical and Electronics Engineers, the Alliance for Telecommunications Industry Solutions, the Internet Engineering Task Force, and the International Telecommunication Union. (Public Law [P.L.] 112-96, § 6001 *Definitions*)

Common Operational Picture: A single identical display of relevant information shared by more than one command that facilitates collaborative planning and assists all echelons to achieve situational awareness; also called COP. (DoD Joint Publication 3-0)

Core Network: A combination of high-capacity switches and transition facilities which form the backbone of a carrier network. Provides switching, transport, and enhanced services for traffic emanating from and directed to the cellular network's Radio Access Network (RAN). (Newton's Telecom Dictionary)

Direct Mode Communications: An ad hoc form of radio communications in which both the transmitter and the receiver operate without support from infrastructure. Users cannot talk and listen simultaneously, and only one user can talk at any one time, while multiple other users in the area listen. This mode is essential to public safety operations as it allows public safety users to communicate with each other outside the existing public safety communications network coverage area. (National Public Safety Telecommunications Council [NPSTC])

Dispatch: A radio communications technique where one communicates to many through short bursts of communication. Users of dispatch services include taxis, trucking companies, and service personnel. (Newton's Telecom Dictionary)

Dynamic Priority: Dynamic priority refers to the ability of an authorized responder or administrator to override the default priority assigned automatically by the public safety broadband network. Typically, human intervention is required to trigger a dynamic priority change, such as pressing the user equipment's emergency button or turning on vehicle lights and siren. (NPSTC Broadband Working Group, Priority and Quality of Service Task Group)

Emergency Response Providers: As defined in the *Homeland Security Act of 2002,* "includes Federal, State, and local emergency public safety, law enforcement, emergency response, emergency medical (including hospital emergency facilities), and related personnel, agencies, and authorities."

End-to-End: The inclusion of all requisite components necessary to deliver stated information exchange capability from the information producer's information appliance to the intended user information appliance(s).

Government Emergency Telecommunications Service (GETS): Provides National Security/Emergency Preparedness (NS/EP) personnel a high probability of completion for their phone calls when normal calling methods are unsuccessful. It is designed for periods of severe network congestion or disruption, and works through a series of enhancements to the Public Switched Telephone Network (PSTN). GETS is in a constant state of readiness. Users receive a GETS "calling card" to access the service. This card provides access phone numbers, Personal Identification Number (PIN), and simple dialing instructions. (NCS.gov)

Internet Protocol: Part of the TCP/IP family of protocols describing software that tracks the Internet address of nodes, routes outgoing messages, and recognizes incoming messages; used in gateways to connect networks at OSI network Level 3 and above. (Newton's Telecom Dictionary)

Interoperability: The ability of independent systems to exchange meaningful information and initiate actions from each other, in order to operate together for mutual benefit. In particular, it envisages the ability for loosely-coupled independent systems to be able to collaborate and communicate; the possibility for use in services outside the direct control of the issuing assigner. (International Organization for Standardization Technical Committee 46/Subcommittee 9)

Land Mobile Radio: A collection of portable and stationary radio units designed to communicate with each other over predefined frequencies. They are deployed whenever organizations need to have instant communication between geographically dispersed and mobile personnel. (Newton's Telecom Dictionary)

Long Term Evolution (LTE): The access part of the Evolved Packet System. The main requirements for the new access network are high spectral efficiency, high peak data rates, short round trip time and frequency flexibility. (3GPP.org) LTE is the standard created and adopted by 3GPP through its Release 8 regarding fourth generation (4G) cellular wireless telecommunications. 4G is based upon an all IP packet switched network that supports mobile broadband access as well as multi-media applications with high data rates and low latencies utilizing spectrum efficiency by smooth handoffs and seamless roaming across multiple networks. LTE has been accepted and adopted by national and international communities as the foundation for future mobile telecommunications. (http://transition.fcc.gov/pshs/docs/LTE_Info_Sheet_09082010.pdf)

Mission Critical Voice: Key elements for the definition of mission critical voice include: direct or talk around; push-to-talk; full duplex voice systems; group call; talker identification; emergency alerting; and audio quality. (NPSTC)

Next Generation Network: Uses packets to transmit VoIP, data, and video technology. (Modified from Newton's Telecom Dictionary)

NS/EP Communications: Primarily those technical capabilities supported by policies and programs that enable the Executive Branch to communicate at all times and under all circumstances to carry out its mission essential functions and to respond to any event or crisis (local, national, or international); to include communicating with itself; the Legislative and Judicial branches; State, territorial, tribal and local governments; private sector entities; as well as the public, allies, and other nations. NS/EP communications also include those systems and capabilities at all levels of government and the private sector that are necessary to ensure national security and to effectively manage incidents and emergencies. (NS/EP Communications Executive Committee definition based on Executive Order 13618)

One-to-Many Communications: In telecommunications, point-to-multipoint communication is communication which is accomplished via a distinct type of one-to-many connection, providing multiple paths from a single location to multiple locations. (M. Cover, Thomas and Joy A. Thomas (1991), Elements of Information Theory, Wiley-Interscience. International Standard Book Number 0-471-06259-6.)

Open Systems Interconnect: A Reference Model developed by the International Organization for Standardization and is the only internationally accepted framework of standards for communication between difference systems made by different vendors. The purpose of the OSI is to create an open systems networking environment where any vendor's computer system, connected to any network, can freely share data with any other computer system on that network or a linked network. (Newton's Telecom Dictionary)

Packet-Switched Network: A network designed to carry data in the form of packets. (Newton's Telecom Dictionary)

Personally Identifiable Information: Any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information. (Government Accountability Office Report 08-536)

Public Safety Services: According to the *Communications Act of 1934*, public safety services means "services the sole or principal purpose of which is to protect the safety of life, health, or property."[86] P.L. 112-96 noted this definition and expanded the range of possible Nationwide Public Safety Broadband Network users as discussed in Section 2.3.2.

Preemption: Preemption indicates instant access to resources for a user, at times disconnecting other users.

Priority: A ranking given to a task which determines when it will be processed. (Newton's Telecom Dictionary)

Quality of Service: The mechanism for accomplishing priority in IP-based networks. (Newton's Telecom Dictionary)

Radio Access Network: Cellular networks essentially consist of two parts: the RAN, which controls transmission and reception of radio signals; and the Core Network, which provides switching, transport, and enhanced services for traffic emanating from and directed to the cellular network's RAN. (Newton's Telecom Dictionary)

Reliability: A measure of how dependable a system is once you actually use it. (Newton's Telecom Dictionary)

Resilience: Presidential Policy Directive (PPD)-8: National Preparedness defines resilience as the ability to adapt to changing conditions and withstand and rapidly recover from disruption due to emergencies. (PPD-8: National Preparedness)

Roaming Agreements: An agreement between wireless carriers that allows their subscribers to use their phones on other wireless carriers. (Newton's Telecom Dictionary)

Scalability: Something that can be made larger or smaller relatively easily and painlessly. (Newton's Telecom Dictionary)

Schema: The set of definitions for the universe of objects that can be stored in a directory. For each object class, the schema defines which attributes an instance of the class must have, which additional attributes it can have, and which other object classes can be its parent object class. (Newton's Telecom Dictionary)

Security: A way of insuring data on a network is protected from unauthorized use. Network security measures can be software-based where passwords restrict users' access to certain data files or directories. This kind of security is usually implemented by the network operating system. Audit trails

[86] Communications Act of 1934 § 337(f) as codified in 48 Stat. 1064.

are another software-based security measure, where an ongoing journal of what users did what with what files is maintained. Security can also be hardware-based, using more traditional lock and key. (Newton's Telecom Dictionary)

Service Providers: In the broadest sense, a service provider is any company which provides service to anyone else. That means a service provider could be a phone company in the form of either a Local Exchange Carrier or IntereXchange Carrier; it could be an Application Service Provider; it could be an Internet Service Provider. A service provider is thus any company which doesn't itself consume all of the services it sells. (Newton's Telecom Dictionary)

Spectrum: A continuous range of frequencies, usually wide in extent within which waves have some specific common characteristics. (Newton's Telecom Dictionary)

Stakeholder: An individual with unique knowledge, experience, and operational skills, often has a role to play and responsibilities in implementing the mission requirement solutions.

Survivability: A property of a system, subsystem, equipment, process, or procedure, that provides a defined degree of assurance that the device or system will continue to work during and after a natural or man-made disturbance (e.g., nuclear attack). This term must be qualified by specifying the range of conditions over which the entity will service, the minimum acceptable level of post-disturbance functionality, and the maximum acceptable outage duration. (Newton's Telecom Dictionary)

Transmission Control Protocol: A specification for software that bundles outgoing data into packets (and bundles incoming data), manages the transmission of packets on a network, and checks for errors. TCP is the portion of the TCP/IP protocol suite that governs the exchange of sequential data. (Newton's Telecom Dictionary)

Usability: Refers to how well users can learn and use a product to achieve their goals. It also refers to how satisfied users are with that process. Usability measures the quality of a user's experience when interacting with a product or system, including: websites, software applications, mobile technologies, and any user-operated device. (Usability.gov)

Wireless Priority Service (WPS): A priority communications service for improving call completion capabilities for authorized NS/EP cell phone users. In the event of congestion in the wireless network, an emergency call using WPS can queue for the next available channel. All WPS (and GETS) calls will receive priority during access, transport, and egress to a wireless mobile on a WPS carrier, even if the terminating mobile is not subscribed to WPS. WPS calls do not preempt calls in progress or deny the general public's use of the radio spectrum. (GETS/WPS Program Management Office, NCS.gov)

APPENDIX D: OVERVIEW OF THE FIRSTNET BOARD

Public Law (P.L.) 112-96 created the First Responders Network Authority (FirstNet) Board as an independent authority within the National Telecommunications and Information Administration (NTIA). The FirstNet Board holds the public safety wireless license granted for the Nationwide Public Safety Broadband Network (NPSBN) and takes all actions necessary to ensure the building, deployment, and operation of the NPSBN, in consultation with Federal, State, local, and tribal public safety entities; the Director of the National Institute of Standards and Technology; the Federal Communications Commission (FCC); and a public safety advisory committee required by the Act. The FirstNet Board's authority for responsibilities detailed in P.L. 112-96 expires after 15 years.

What is the FirstNet Board?

The FirstNet Board is an independent authority within NTIA. Specifically, it:

- Is headed by a 15-member board, including the Secretary of Homeland Security, the U.S. Attorney General, the Director of the Office of Management and Budget, and 12 individuals appointed by the Secretary of Commerce;
- Holds the single public safety 700 Megahertz wireless broadband license; and
- Takes all actions necessary to ensure the design, construction, deployment, and operations of the NPSBN.

The FirstNet Board's authority expires after 15 years.

While the terms are often used synonymously, it is important to note that FirstNet is the governing board that manages the NPSBN, while the NPSBN is the actual network.

P.L. 112-96 includes provisions to fund and govern an NPSBN that provides a secure, reliable, and dedicated interoperable network for emergency responders to communicate during an emergency and to support FirstNet in meeting its responsibilities for the NPSBN. Some other key provisions of the Act include:

- Granting a 10-year renewable license for the D-Block spectrum to the FirstNet Board for use by the NPSBN;
- Allocating over $7 billion in funds for NPSBN-related capital expenditures;
- Creating the Public Safety Interoperability Board (Interoperability Board) within the FCC to develop and recommend technical requirements to ensure the NPSBN's nationwide interoperability;[87]
- Establishing a grant program to help State and local jurisdictions plan for and integrate their networks with the NPSBN; and
- Funding NPSBN research and development activities and facilitating the advancement of other NPSBN-related initiatives.[88]

[87] The Interoperability Board has completed its task and has been decommissioned.

[88] This funding is contingent on first funding a number of activities, including reducing the debt by $20 million, out of auction proceeds.

APPENDIX E: PREVIOUS NSTAC FINDINGS AND RECOMMENDATIONS

The following are recommendations from previous National Security Telecommunications Advisory Committee (NSTAC) reports that are relevant to national security and emergency preparedness (NS/EP) and advanced Internet protocol (IP)-based broadband networks (referred to as next generation networks in previous NSTAC reports). Provided within parenthesis in red below is a brief context for each recommendation as it applies to the scope of the current report.

NSTAC Report to the President on Emergency Communications and Interoperability

January 16, 2007
http://www.ncs.gov/nstac/reports/2007/NSTAC%20Report%20on%20Emergency%20Communications%20and%20Interoperability.pdf

RECOMMENDATION

- The President should modernize existing national security and emergency preparedness (NS/EP) policy guidance to clarify and consolidate Federal Government emergency communications roles and responsibilities. (Need for Federal level NS/EP related policy changes and organizational alignment)

NSTAC Report to the President on Communications Resiliency

April 19, 2011
http://www.ncs.gov/nstac/reports/NSTAC%20Report%20to%20the%20President%20on%20Communications%20Resiliency%20(2011-04-19)(Final)(pdf).pdf

RECOMMENDATIONS

The NSTAC recommends the President, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*:

- Request that Congress fund DHS' priority services efforts to continue industry and Government collaboration and to ensure that advanced NS/EP communication services are operational when needed. (Funding needs for advanced NS/EP services)
- Encourage DHS to petition the FCC to issue a declaratory ruling to confirm that network service providers may lawfully offer IP-based priority access services to NS/EP authorized users. (Legalizing transition to IP-based priority access for NS/EP services)
- Direct DHS and other appropriate departments and agencies to support collaboration between State and local government and industry to determine the most effective and appropriate mechanisms for restoring critical communications services. (Coordinating and aligning to improve effectiveness and achieve efficiencies in critical communications restoration)

Next Generation Networks Task Force Report
March 28, 2006
http://www.ncs.gov/nstac/reports/2006/NSTAC%20Next%20Generation%20Networks%20Task%20Force%20Report.pdf

RECOMMENDATIONS

- Coordination on Common Operational Criteria for NGN NS/EP end-to-end Services*:* The President should direct OSTP, with support from the collective NCS agencies, to establish a Common Operational Criteria development framework to meet NS/EP user requirements on the NGN. This would be a joint industry-Government initiative to ensure NS/EP communications capabilities in the NGN environment, and would include the creation of a regular NGN summit with annual reporting that would enable telecommunication/information technology industry sector and Government stakeholders to: (1) develop and coordinate common NGN planning activities; (2) measure progress of NGN-related efforts; and (3) recommend and monitor initiatives that would foster NS/EP capabilities within the NGN. (Outline for work involved in transition of NS/EP services to IP-based broadband networks)

- Research and Development***:*** In support of the prior recommendation, the President should direct OSTP, with support from other relevant agencies, especially the Science and Technology Directorate of DHS, NIST, and DOD to establish and prioritize within the Federal Government initiatives that will foster collaborative and coordinated R&D supporting the Common Operational Criteria, and accelerate demonstrations of critical NGN NS/EP-supporting capabilities or technology among NGN telecommunication/information technology and service providers. (Coordination efforts among related organizations to accelerate R&D activities for NS/EP services on IP-based broadband networks)

- Agreements, Standards, Policy, and Regulations*:* The President should direct DHS, the Department of State, and DOC (including NIST and NTIA) to engage actively with and coordinate among appropriate domestic and international entities to ensure that the relevant policy frameworks support NGN NS/EP capabilities. These policy frameworks are established through Agreements, Standards, Policies, and Regulations (ASPR). As part of the Common Operational Criteria development framework, these agencies should continuously monitor the entire lifecycle of ASPR associated with ensuring NS/EP capabilities to identify and act on opportunities to enhance ASPR, address their vulnerabilities, and eliminate potential impediments to providing NS/EP capabilities in a globally-distributed NGN environment. (Establishing policy frameworks)

- First Responders: The President should direct DHS and other appropriate Government agencies to assist first responders and public safety organizations in making the transition to the NGN, which will provide them with greater capabilities, but will also be a challenge to achieve given their limited resources and legacy systems. When mature, the NGN will provide first responder and public safety organizations with much greater capabilities, such as transmission of data real-time along with voice. The NGN will also aid interoperability in cases where "operability" of first responder and public safety networks and the NGN itself are present. The connection or bridging of disparate networks to the NGN will allow communication between them via the underlying protocols of the NGN. (Transition of public safety communications to IP-based broadband networks)

Report on National Security and Emergency Preparedness Internet Protocol-Based Traffic
November 6, 2008
http://www.ncs.gov/nstac/reports/2008/NSEP%20IP-Based%20Traffic%20Report.pdf

RECOMMENDATIONS

The NSTAC recommends, in accordance with responsibilities and existing mechanisms established by Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, that the President should:

- In the long term, require Federal departments and agencies to remain actively involved in standards development of priority services on IP-based networks by supporting efforts to: Provide adequate funding that will be used to develop timely solutions across all technology platforms; and Commit appropriate resources to actively participate in and lead the global standards bodies' efforts to address NS/EP IP-based priority services. (Funding and participation in NS/EP priority services related technology standards development)
- Petition the FCC for a declaratory ruling to confirm that network service providers may lawfully offer IP-based priority access services to NS/EP authorized users. (Legalizing transition to IP-based priority access for NS/EP services)

APPENDIX F: NS/EP POLICY MATRIX

Category I - Statutory/Regulatory/Presidential Directives/Executive Orders
47 United States Code (U.S.C.) § 153 (20) http://www.gpo.gov/fdsys/pkg/USCODE-2011-title47/html/USCODE-2011-title47-chap5-subchapI-sec153.htm Defines Information Service in the context of communications technology.
44 U.S.C. § 3502 (8) http://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/html/USCODE-2011-title44-chap35-subchapI-sec3502.htm Defines Information System for the purposes of Federal records management.
47 U.S.C. § 332(d)(3) http://www.gpo.gov/fdsys/pkg/USCODE-2009-title47/pdf/USCODE-2009-title47-chap5-subchapIII-partI-sec332.pdf Defines private mobile service.
44 U.S.C. §3536 http://www.gpo.gov/fdsys/pkg/USCODE-2011-title44/html/USCODE-2011-title44-chap35-subchapII-sec3536.htm Defines minimum requirements for National Security Systems for the purposes of Federal record-keeping.
47 C.F.R. § 201.2(g) http://www.gpo.gov/fdsys/pkg/CFR-2008-title47-vol5/xml/CFR-2008-title47-vol5-chapII.xml "National security and emergency preparedness (NS/EP) telecommunications services, or NS/EP services; means those telecommunication services which are used to maintain a state of readiness or to respond to and manage any event or crisis (local, national, or international) which causes or could cause injury or harm to the population, damage to or loss of property, or degrades or threatens the NS/EP posture of the United States."
National Security Presidential Directive (NSPD) 51/Homeland Security Presidential Directive (HSPD) 20 http://www.fas.org/irp/offdocs/nspd/nspd-51.htm Outlines systems relevant to continuity of operations and continuity of government, including National Essential Functions and Primary Mission Essential Functions.
Homeland Security Act of 2002, as amended, 6 U.S.C. § 571 *et. seq.* www.gpo.gov/fdsys/pkg/PLAW-107publ296/pdf/PLAW-107publ296.pdf Creates the U.S. Department of Homeland Security (DHS) and the new cabinet-level position of Secretary of Homeland Security.
Executive Order (E.O.) 13618 *(Revokes E.O. 12472)* **- Assignment of National Security and Emergency Preparedness Communications Functions** http://www.fas.org/irp/offdocs/eo/eo-13618.htm Outlines responsibilities for NS/EP communications policies, programs and capabilities. The updated NS/EP communications definition provided by the NS/EP Communications Executive Committee (ExCom) and based on language from this E.O. 13618 was approved by the Domestic Resilience Group on December 20, 2012. Applicable to the Nationwide Public Safety Broadband Network (NPSBN) to the extent (as anticipated) that Federal Government entities use the NPSBN for NS/EP communications. The new ExCom serves as a strategy and policy body. The ExCom cannot supplant the First Responder Network Authority (FirstNet) Board's statutory role to manage NPSBN operations. The ExCom is charged

with making recommendations about what should constitute NS/EP communications requirements.

HSPD 3: Homeland Security Advisory System
http://www.fas.org/irp/offdocs/nspd/hspd-3.htm
Provides a comprehensive and effective means to disseminate information regarding the risk of terrorist acts to Federal, State, and local authorities and to the American people. The National Terrorism Advisory System has replaced the color-coded Homeland Security Advisory System.

HSPD 5: Management of Domestic Incidents
http://www.fas.org/irp/offdocs/nspd/hspd-5.html
Establishes a single, comprehensive national incident management system to enhance the ability of the U.S. to manage domestic incidents.

HSPD 8: National Preparedness
http://www.dhs.gov/xabout/laws/gc_1215444247124.shtm
Establishes policies to strengthen the preparedness of the U.S. to prevent and respond to threats or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining actions to strengthen preparedness capabilities of Federal, State, and local entities.

Communications Act of 1934, as amended
47 U.S.C. § 151 et. seq. http://transition.fcc.gov/Reports/1934new.pdf
Combines and organized Federal regulation of telephone, telegraph, and radio communications, and created the Federal Communications Commission (FCC) to oversee and regulate these industries. FirstNet will become the FCC licensee of the NPSBN pursuant to the Communications Act.

FCC's Second Report and Order - Establishment of Rules and Requirements for Priority Access Service, WT Docket No. 96-86
http://wps.ncs.gov/documents/242.pdf
Establishes that the priority services offered to NS/EP authorized users were *prima facie* lawful under the Communications Act of 1934 as amended, and not an unreasonable preference or discrimination in contravention of Section 202(a) of the Communications Act.

Middle Class Tax Relief and Job Creation Act of 2012, P.L. 112-96, 126 Stat. 156 (2012), §§ 6204-6301.
http://www.gpo.gov/fdsys/pkg/BILLS-112hr3630enr/pdf/BILLS-112hr3630enr.pdf
Outlines the creation of the NPSBN and its governing authority, FirstNet.

Presidential Policy Directive (PPD) 1 – Organization of the National Security Council System
http://www.fas.org/irp/offdocs/ppd/ppd-1.pdf
Outlines the organization of the National Security Council System including its functions, membership, and responsibilities.

PPD 21 - Critical Infrastructure Security and Resilience
http://www.fas.org/irp/offdocs/ppd/ppd-21.pdf
Advances a national unity of effort to strengthen and maintain secure, functioning, and resilient critical infrastructure. Replaces HSPD 7: Critical Infrastructure Identification, Prioritization, and Protection.

E.O. 13636 - Improving Critical Infrastructure Cyber security
http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity
Focuses on improving cyber security for critical infrastructure, by improving information sharing, creating a framework to reduce cyber risk, and identifying critical infrastructure that is at greatest risk.

Rehabilitation Act of 1973, codified as 29 U.S.C. § 701, P.L. 93–112, 87 Stat. 355
http://www.gpo.gov/fdsys/pkg/USCODE-2010-title29/pdf/USCODE-2010-title29-chap4-sec31.pdf

Replaces the Vocational Rehabilitation Act and authorizes the grant programs for vocational rehabilitation, supported employment, independent living, and client assistance.
Category II – National Communications System (NCS) Directives
National Coordinating Center (NCC) Operating Charter http://www.ncs.gov/ncc/nccoc/nccoc_toc.html The mission of the NCC is to assist in the initiation, coordination, restoration, and reconstitution of NS/EP telecommunications services or facilities. The NCC will perform or contribute to the performance of the telecommunications functions enumerated in NCC functions.
NCS Directive 3-1: Telecommunications Operations **Telecommunications Service Priority (TSP) System for NS/EP** http://www.ncs.gov/library/issuances/NCSD%203-1.pdf Implements policy, explains legal and regulatory basis, assigns responsibilities, and prescribes procedures for the TSP system for NS/EP.
NCS Directive 3-4: Telecommunication Operations **National Telecommunications Management System (NTMS)** http://www.ncs.gov/library/issuances/NCSD%203-4.pdf Establishes the NTMS, describes its components, and broadly describes the administrative responsibilities of the NCS Manager and participating NCS member organizations. *This directive will need to be reviewed and revised to take into account the new paradigm for exercising Presidential authority under Section 706 of the Communications Act set forth in E.O. 13618.*
NCS Directive 3-8: Telecommunications Operations **Provisioning of Emergency Power in Support of NS/EP Telecommunications** http://www.ncs.gov/library/issuances/NCSD%203-8.pdf Establishes policies covering the provision of reliable electric power for telecommunication facilities in support of NS/EP.
NCS Directive 3-9: Telecommunications Operations **Communications Resource Information Sharing Initiative** http://www.ncs.gov/library/issuances/NCSD%203-9.pdf Establishes policies pertaining to administering and using the NCS Communications Resource Information Sharing Initiative. *It is unclear how this function will be carried out going forward in light of the NCS Committee of Principals being disbanded.*
NCS Directive 3-10: Minimum Requirements for Continuity Communications Establishes policy, explains legal and regulatory basis, assigns responsibilities, and prescribes minimum requirements for continuity communications capabilities.
NCS Directive 4-3: Technology and Standards **Interoperability of Telecommunications in Support of NS/EP** http://www.ncs.gov/library/issuances/NCSD%204-3.pdf Establishes the policy by which the NCS supports NS/EP objectives by seeking to ensure the interoperability of NS/EP telecommunications assets among Federal Government departments, agencies, or entities, and other affected Executive entities.
NS/EP Requirements for NETWORX contract http://ncs.gov/nstac/reports/2012-05-15%20NSTAC%20Cloud%20Computing.pdf Appendix G of the NSTAC Report to the President on Cloud Computing lists 14 functional requirements.
Category III – The Committee on National Security Systems Policies (CNSSP)
CNSSP-17: Policy on Wireless Communications Protecting National Security Information http://www.cnss.gov/Assets/pdf/CNSSP-17.pdf

Addresses the safeguarding responsibilities for wireless transmitting and/or storing National Security Information (NSI) in wireless devices. Can provide recommendations on technical security requirements and related operational procedures for NSI.
CNSSP-18: National Policy on Classified Information Spillage (IS) http://www.cnss.gov/Assets/pdf/CNSSP-18.pdf Framework for the consistent handling of spillage of classified information onto an unclassified IS, or higher-level classified information onto a lower level classified IS, to include non-government systems.
National Security Telecommunications and Information Systems Security Policy -101: National Policy on Securing Voice Communications http://www.cnss.gov/Assets/pdf/nstissp_101.pdf National policy to improve U.S. communications security, and specifically to reduce the vulnerability of governmental voice communications to exploitation.
Category IV– Current Cybersecurity/Critical Infrastructure Policies
NSPD 54/HSPD 23: Cyber Security and Monitoring Outlines security requirements for voice communications. Can provide considerations for the varying levels of security requirements across Federal, State, and local agencies.
Federal Information Security Management Act, 44 U.S.C. § 3541 *et. seq.* http://csrc.nist.gov/drivers/documents/FISMA-final.pdf Assigns specific responsibilities to Federal agencies, the National Institute of Standards and Technology, and the Office of Management and Budget in order to strengthen information system security.
E.O. 13231: Critical Infrastructure Protection in the Information Age http://www.fas.org/irp/offdocs/eo/eo-13231.htm Ensures protection of information systems for critical infrastructure, including emergency preparedness communications, and the physical assets that support these systems.
Defense Production Act, 50 U.S.C. App. § 2061 *et. seq.* http://www.fema.gov/library/viewRecord.do?id=3590 Authorizes the President to require businesses to sign contracts or fulfill orders deemed necessary for national defense, to establish mechanisms (such as regulations, orders or agencies) to allocate materials, services and facilities to promote national defense, to control the civilian economy so that scarce and/or critical materials necessary to the national defense effort are available for defense needs.
Computer Fraud and Abuse Act, 18 U.S.C. § 1030 http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/html/USCODE-2011-title18-partI-chap47.htm Intended to reduce cracking of computer systems and to address Federal computer-related offenses.
E.O. 12333: United States Intelligence Activities http://www.fas.org/irp/offdocs/eo/eo-12333-2008.pdf Intended to extend powers and responsibilities of U.S. intelligence agencies and direct the leaders of U.S. Federal agencies to co-operate fully with CIA requests for information.
Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. § 5121 *et. seq.* http://www.fas.org/sgp/crs/homesec/RL33053.pdf Authorizes the President to issue major disaster or emergency declarations in response to catastrophes in the U. S. that overwhelm State and local governments.
Electronic Communications Privacy Act, 18 U.S.C. §§ 2510-22 http://www.gpo.gov/fdsys/pkg/USCODE-2011-title18/pdf/USCODE-2011-title18-partI-chap119.pdf Extends government restrictions on wire taps from telephone calls to include transmissions of electronic data by computer.

Intelligence Authorization Act http://www.intelligence.senate.gov/pdfs112th/11287.pdf Codifies covert, clandestine operations and defines requirements for reporting such operations to Congress.
Intelligence Reform and Terrorism Prevention Act http://www.nctc.gov/docs/pl108_458.pdf Broadly affects the U.S. Federal terrorism laws. In juxtaposition with the single-subject rule, the Act is composed of several separate titles with varying subject issues.
National Emergencies Act, 50 U.S.C. Sections 1601-1651 http://uscode.house.gov/download/pls/50C34.txt Stops open-ended states of national emergency and formalizes the power of Congress to provide certain checks and balances on the emergency powers of the President.
Category V – DHS Homeland Security Policy Statements
National Strategy for Homeland Security www.hsdl.org/?view&did=479633 Serves as a guide to face the dual challenges of preventing terrorist attacks in the homeland and strengthening our Nation's preparedness for both natural and man-made disasters.
National Strategy for the Physical Protection of Critical Infrastructures and Key Assets http://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf Identifies a clear set of goals and objectives and outlines the guiding principles to secure the Nation's critical infrastructures and key assets.
National Strategy to Secure Cyberspace http://www.us-cert.gov/reading_room/cyberspace_strategy.pdf Provides a framework for protecting the Nation's cyberspace infrastructure.
National Emergency Communications Plan http://www.dhs.gov/xlibrary/assets/national_emergency_communications_plan.pdf Promotes the ability of emergency response providers and relevant government officials to continue to communicate in the event of natural disasters, acts of terrorism, and other man-made disasters, as well as to ensure, accelerate, and attain interoperable emergency communications nationwide.
National Incident Management System http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf Establishes NS/EP protocols for response, including communications leadership and interoperability.
National Response Plan National plan to respond to emergencies such as natural disasters or terrorist attacks. The Plan was superseded by the National Response Framework on March 22, 2008.
National Infrastructure Protection Plan http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf Aims to unify critical infrastructure and key resource protection efforts across the country.
Bottom Up Review Report http://www.dhs.gov/xlibrary/assets/bur_bottom_up_review.pdf Provides the results of a Department-wide assessment of DHS, begun in November 2009, to align the Department's programmatic activities and organizational structure with the mission sets and goals identified in the Quadrennial Homeland Security Review.

APPENDIX G: ADVANCED COMMUNICATIONS TECHNOLOGIES

Today's advanced communications technologies offer tremendous benefits for mission execution (e.g., big data, cloud processing).

- **Machine to Machine Communications:** The use of Internet protocol-based technologies to provide telemetry (automatic transmission and measurement of data from remote sources) and supervisory control and data acquisition capabilities for industrial, infrastructure, and facility processes.
- **Content and Context Aware Technologies:** Technology that offers feedback based on the meaning of a request (content) or the circumstances in which the request was made (context).
- **Collaboration and Social networking Technologies:** Collaboration technology is software, platforms, or services that enable people at different locations to communicate and work with each other in a secure, self-contained environment. May include capabilities for document management, application sharing, presentation development and delivery, whiteboarding, chat, and more (web.worldbank.org). Social networking technology is any network-based tool that allows for community creation and content sharing.
- **Cloud Computing:** A model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This cloud model promotes availability and is composed of five essential characteristics, three service models, and four deployment models (National Institute of Standards and Technology Special Publication 800-145).
- **Big Data:** A phenomenon defined by the rapid acceleration in the expanding volume of high velocity, complex, and diverse types of data. Big Data is often defined along three dimensions—volume, velocity, and variety.
(http://www.techamerica.org/Docs/fileManager.cfm?f=techamerica-bigdatareport-final.pdf)
- **Unified Communications (UC) Technologies:** UC is the integration of one or more of the following communications capabilities: telephony, unified messaging, desktop client, email, instant messaging, audio conferencing, video conferencing, web conferencing, converged conferencing, notification service, personal assistant, rich presence service, communications-enabled business processes, contact cent, mobile solutions, and collaboration. UC allows a message sent on one medium to be received on another medium.

APPENDIX H: LESSONS LEARNED FROM GETS/WPS

Stakeholders will require performance information on the networks supporting priority communications, whether national security and emergency preparedness (NS/EP) or public safety. The requests from stakeholders will likely include the following questions:

- In an event, did the network perform as designed? If not, why not?
- Why did a specific user not get the communications requested during an event?
- Can the network be tweaked to provide better performance to more users?
- Does the network need to be upgraded with new technology to support the user base? If so, when? How much will this cost?
- How do I know that the network is functioning properly and is available for priority communications?
- Why should I support priority communications? (Service Provider stakeholder question)

The Government Emergency Telecommunications Service (GETS) has been addressing these questions since its beginning in 1993, while the Wireless Priority Service (WPS) has been addressing these questions since its beginning in 2002.

Did the Network Perform as Designed?

This question is typically answered by a performance report. For example, the Office of Emergency Communications (OEC) provided the following performance data on GETS and WPS for Hurricane Sandy from October 29, 2012 to November 6, 2012:

- GETS valid call attempts: 18,347
- GETS calls that failed: 121
- GETS completed calls: 18,226
- GETS call completion rate: 99.34% for both user calls and test calls; 96.4% for user calls
- GETS activations: 47
- WPS activations: 267
- WPS call origination attempts: 23,123 (call attempts that reached the cell tower)
- WPS call attempts successfully assigned a radio channel: 22,815
- WPS origination success rate: 98.67%
- NS/EP (GETS or WPS) calls delivered to a WPS Mobile Switching Center for termination: 17,802
- NS/EP calls assigned a termination radio channel: 16,843
- WPS termination success rate: 94.61%
- Telecommunications Service Priority expedited provisioning: 196 supporting the Federal Emergency Management Agency, Red Cross, U.S. Coast Guard, U.S. Corps of Engineers, U.S. Forest Service, and the Insurance Industry

The statistics above show that GETS and WPS well exceeded the design goals of more than 90% call completion for GETS and 80% for WPS. The success rate for WPS terminations is generally lower than for originations because the destination may not be available for a number of reasons, such as busy on another call, or mobile device turned off, or out of range.

In addition to performance reports, testimonials from users may be provided to the Government. A sample of the testimonials received by OEC for GETS/WPS includes:

- Gary Vandegriff, Director, Highway Maintenance, Seymour District, Indiana Department of Transportation: The event was tornadoes in the mid-west on March 23, 2012. "A combination of infrastructure damage and congestion prevented standard calls from completing, but by following the instructions on the rear of the GETS card, I was able to complete a majority of my WPS/GETS calls."
- Dan Busse, Communication Specialist, Eureka Fire Protection District, St. Louis, Missouri: The event was adverse weather at the St. Louis Fair on July 7, 2012. "Adverse weather necessitated evacuation of 200,000 fair goers and closure of the fair. The local meteorologist needed to confer with the National Weather Service, and the landline and mobile telephone lines were congested. I made a successful WPS call for the meteorologist."
- Kyle Aumell, Point of Contact, Samaritan Medical Center, New York: The event was a fiber cable cut in Watertown, New York on August 2, 2012. "The fiber cable cut affected six counties. The only way to complete calls from the Medical Center was via GETS. I shared the GETS PIN to accommodate 37 calls."

Why Did a Specific User Not Get the Communications Requested During an Event?

To answer such a request, one needs information about the user's location and activity and network state at the time of the communications attempt. Operational measurements from network devices showing when priority was invoked, and call detail records showing the user's activity as seen by the network are critical to answering this request.

The unsatisfied call request can occur for one or more of the following reasons:

- The network operated as designed. For example, the call request did not have high enough priority to be completed.
- There is a network design deficiency based on evolving traffic and technology. For example, cellular signaling channels were not seen as a bottleneck by Industry in 2002; however, an increased user base and short message service capabilities caused signaling to be a bottleneck in the 2008 Los Angeles earthquake and the 2011 East Coast earthquake, blocking WPS users from accessing the cellular networks.
- There is a user error in accessing the network.

In the case of the network performing as designed, the stakeholder will typically ask if the network can be tweaked to support a need. This follow-up question is addressed in the next section.

The performance analyses of priority services by a Government Program Office after each major event, with a focus on service failures, should identify network design deficiencies. When the deficiencies are identified, alternatives to address the service failures are analyzed, and recommendations are made for enhancements to address these failures. For example, the signaling channel issue identified above is being corrected by OEC through an Enhanced Overload Performance effort in the CDMA networks.

User errors are typically addressed by training. For example, during an NS/EP event, users may have difficulty using the GETS and WPS services because:

- They are unable to locate their GETS card.
- They do not follow the procedures to make a GETS call (e.g., they do not enter their PIN after hearing a prompt).
- They assume they have WPS capabilities when they only have a GETS card (i.e., they try to enter the *272 WPS feature code on their mobile, and are blocked by the network).
- They attempt to use WPS on a non-WPS-registered mobile. This case can arise when the user changes/upgrades his/her mobile, service, or carrier, and has not notified OEC of these changes so that WPS can be placed on the new device.

User issues can be addressed before an event if the users test GETS and WPS services. Periodic testing (e.g., monthly) is recommend by OEC; however, less than five percent of the NS/EP user population performs periodic tests.

Can the Network Be Tweaked to Provide Better Performance to More Users?

The technology standards on which the networks are based are continually evolving; these standards may be incorporated in new software releases and hardware within the networks. These features may provide additional capabilities to the NS/EP and public safety community.

To take advantage of these new capabilities, the Government Program Office should perform periodic analyses of these capabilities, creating alternatives (including technical, cost, and schedule) to determine what enhancements, if any, should be recommended.

Does the Network Need to Be Upgraded with New Technology to Support the User Base? If so, When? How Much Will This Cost?

Networks based on "4G" technologies will be replaced by "5G" technologies within the coming decades. Effectively managing the migration from "4G" to "5G" will require the Government Program Office to perform periodic analyses of existing and emerging technologies, creating alternatives (including technical, cost, and schedule) to determine what migration, if any, should be recommended.

Migration to the new technologies will typically occur in phases. An Immediate Capability (IC) is based on the use of the technologies' existing capabilities. The costs associated with an IC are typically for provisioning, operating and maintaining the features found in the technologies. Since development of features is not required, the timeframe for implementation is relatively short.

An Initial Operational Capability (IOC) is based on the use of the technologies' existing capabilities with NS/EP and/or Nationwide Public Safety Broadband Network unique developments to provide end-to-end capabilities in a first nationwide service provider. A Full Operational Capability (FOC) has the same capabilities as an IOC but is implemented by all nationwide service providers. Available funding will typically constrain the functionality delivered and the implementation schedule for IOC and FOC.

How Do I Know that the Network Is Functioning Properly and Is Available for Priority Communications?

In any given component with priority features, these features may not be frequently exercised. Given network changes, priority features may be erroneously disabled or provisioned to non-optimal values. To address this issue, periodic manual and automated testing of the priority features should occur. Monthly testing, when combined with analysis of operational measurements and call detail records, may indicate issues with specific equipment. For example, monthly testing of GETS is completed from both domestic and international locations. Periodic fraud and abuse testing is also completed by the carriers for GETS and WPS.

It may be costly and timely to test all components on a monthly basis; however, to address availability concerns, carriers should be required to provide an annual "audit" of the priority features in their network. For GETS and WPS, this audit includes:

- A copy of the carrier's Methods of Procedures. These procedures identify how GETS and WPS are provisioned in the carrier's networks. These procedures are reviewed by the Government to ensure the procedures accurately reflect the GETS and WPS provisioning requirements.
- A copy of all GETS and WPS provisioning parameters for each network component (e.g., switches). This document is checked against the recommended provisioning parameters; the carrier is notified of discrepancies. A plan is created and implemented to correct identified problems.
- Testing of the GETS and WPS features in each network component type (e.g., each switch type) in the carrier's network. This testing ensures that new features added to a switch type have not impacted the functionality of the NS/EP features.

It is also important to periodically reconcile the priority user base with the carrier to ensure that only authorized users have access to the service. For example, GETS/WPS user reconciliation is performed with the carriers on a regular basis to ensure that the carriers' databases of GETS/WPS users agree with the Government's database.

Why Should I Support Priority Communications? (Service Provider Stakeholder Question)
To address this question, the Government must satisfy both the legal and business concerns of the carrier community.

Legal

GETS and WPS are provided by the carriers on a voluntary basis. Even if GETS and WPS agreements were mandated by the Government, carriers' lawyers would look for liability protection from the Government in providing these services. There are two aspects to this protection:

- **Protection from lawsuits from the public when GETS/WPS services are provided to the Government.** The concern expressed by the carriers' lawyers is that carriers could be sued by the public if it could be demonstrated that an NS/EP call prevented a critical public call from being completed. The protection against these lawsuits is Federal Communication Commission rules, which state that it is in the Government's best interest to provide priority services to the NS/EP user.

- **Protection from lawsuits from NS/EP users when the service is not available.** GETS/WPS services need to operate in "all hazards" situations. The concern expressed by the carriers' lawyers is that carriers could be sued by an NS/EP user whose call is not completed and the user can demonstrate that more could have been done to make the network more robust. The protection against these lawsuits is twofold:
    - Contracts/agreements with the carriers which identify that NS/EP should function over the carriers' surviving assets;
    - Specification and development of features to support priority in vendors' equipment. The Government makes these features available to the carriers, and the carriers are responsible for provisioning and maintaining these features in their networks.

Business

GETS and WPS are not significant money makers for the service providers, so the capabilities provided are constrained by Government funding in conjunction with the service providers' business case for supporting priority communications.

Initially, the Federal Government requested GETS carriers develop NS/EP features using their capital budgets. The NS/EP features were not developed because of budget constraints. In addition, the cost-benefit tradeoffs of the NS/EP features were minimal given other features required by the carriers to increase revenue. To address this business case, the former NCS funded the development of priority features with the vendors and provided a no-cost, right-to-use agreement with the carriers to ensure timely deployment of NS/EP features. This approach was found to satisfy the carriers' business case to support GETS and WPS.

APPENDIX I: NGN NS/EP TELECOMMUNICATIONS SERVICES FUNCTIONAL REQUIREMENTS

The 14 basic functional requirements for next generation network (NGN) national security and emergency preparedness (NS/EP) telecommunications and information technology services include the following:

- **Enhanced Priority Treatment:** Voice and data services supporting NS/EP missions should be provided preferential treatment over other traffic, with the ability to differentiate among classes of NS/EP users and applications.
- **Secure Networks:** Networks must have protection against corruption of, or unauthorized access to, traffic and control, including expanded encryption techniques and user authentication, as appropriate.
- **Non-Traceability:** Selected users must be able to use NS/EP services without risk of usage being traced (i.e., without risk of user or location being identified).
- **Restorability:** Should a service disruption occur, voice and data services must be capable of being re-provisioned, repaired, or restored to required service levels on a priority basis.
- **International Connectivity:** Voice and data services must provide access to and egress from international carriers.
- **Interoperability:** Voice and data services must interconnect and interoperate with other government or private facilities, systems, and networks.
- **Mobility:** The ability of voice and data infrastructure to support transportable, re-deployable, or fully mobile voice and data communications.
- **Nationwide Coverage:** Voice and data services must be readily available to support the national security leadership and inter- and intra- agency emergency operations, wherever they are located.
- **Survivability/Endurability:** Voice and data services must be robust to support surviving users under a broad range of circumstances, from the widespread damage of a natural or manmade disaster up to and including nuclear war.
- **Voice Band Service:** The service must provide voice band service in support of Presidential communications.
- **Broadband Service:** The service must provide broadband service in support of NS/EP missions (e.g., voice, video, imaging, Web access, and multimedia).
- **Scalable Bandwidth**: NS/EP users must be able to manage the capacity of the communications services to support variable bandwidth requirements.
- **Affordability:** The service must leverage network capabilities to minimize cost (e.g., use of existing infrastructure, commercial off-the-shelf (COTS) technologies, and services).
- **Reliability/Availability:** Services must perform consistently and precisely according to their design requirements and specifications (e.g., during network congestion), and must be usable with high confidence.

Reference: October 2011 NCS Committee of Principals Meeting

APPENDIX J: SCENARIOS

The likelihood of public safety users traversing between the Nationwide Public Safety Broadband Network (NPSBN) and commercial networks gives rise to various priority communications scenarios that must be addressed. This includes public safety communications that either originate or terminate on either the NPSBN or on a commercial network, as well as national security and emergency preparedness (NS/EP) communications that traverse these networks. The table below identifies various scenarios[89] that can be expected when NS/EP and public safety users originate, receive, and traverse between the NPSBN and commercial networks, and the inter-system priority issues that arise with each.

To address these issues, the following questions must be addressed:

- What are the markings/Quality of Service (QoS) levels used in the NPSBN?
- What are the markings/QoS levels used in the commercial networks?
- How are the NPSBN markings/QoS levels mapped into the commercial network markings/QoS levels?
- If the mapping is not one-to-one (e.g., two NPSBN QoS levels are mapped into one commercial network QoS level), how does an NPSBN gateway know which NPSBN value to use when it receives a packet from the commercial network?
- Are there NPSBN QoS levels that will be mapped into public (i.e., non-priority) QoS levels in the commercial networks? (If not, all NPSBN traffic will receive priority on commercial networks.)

Four NS/EP User Communication Scenarios

Scenario	**Description**	**Considerations for End-to-End Priority**
1 – NS/EP users have use of the NPSBN	A FirstNet-authorized NS/EP user with a Wireless Priority Service subscribed Long Term Evolution wireless device is able to originate and receive communications via the NPSBN	Scenario 1 assumes a FirstNet-authorized NS/EP user does not need to invoke priority to originate and receive communications.
1.a – Voice and Session-Oriented Video	The FirstNet-authorized NS/EP user originates a voice call or a video (teleconference) session	• What priority markings (e.g., Resource Priority Header [RPH]) are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the

[89] DHS' Office of Emergency Communications, developed eight scenarios and listed them in the *Expectations for the NPSTC Broadband Working Group Revised Statement of Requirements.* The presented tables augment the information provided in that report to identify considerations that must be addressed to provide priority end-to-end communications.

		media for the call on the NPSBN? • If the call is routed to a commercial network, what priority markings does the NPSBN gateway place on the signaling messages for the call? • If the call is routed to a commercial network, what QoS markings does the NPSBN gateway place on the signaling messages for the call? • If the call is routed to a commercial network, what QoS markings does the NPSBN gateway place on the media for the call?
1.b – Data	The FirstNet-authorized NS/EP user originates a data session	The data session may be with a server on the NPSBN or on the Internet. • If a data packet is routed to the Internet, what QoS markings does the NPSBN gateway place on packet? • If a data packet is received from the Internet, what QoS markings does the NPSBN gateway place on packet?
2 – NS/EP users can invoke / have priority when using NPSBN	A FirstNet-authorized NS/EP user, using the NPSBN, when unable to originate an official communication, can invoke and has priority on the NPSBN	Scenario 2 assumes a FirstNet-authorized NS/EP user invokes priority to originate and receive communications. • How do the priority markings on the NPSBN differ between Scenario 1 and Scenario 2? • Can the NPSBN gateway differentiate between normal and NS/EP calls to place the appropriate markings on traffic sent to commercial networks?
2.a – Voice and Session-Oriented Video	The FirstNet-authorized NS/EP user originates an NS/EP voice call or a video (teleconference) session	• What priority markings (e.g., RPH) are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the media for the call on the NPSBN? • If the call is routed to a commercial network, what priority markings does the NPSBN gateway place on the signaling messages for the call? • If the call is routed to a commercial network, what QoS markings does the NPSBN gateway place on the signaling

		messages for the call? - If the call is routed to a commercial network, what QoS markings does the NPSBN gateway place on the media for the call?
2.b – Data	The FirstNet-authorized NS/EP user originates a priority (NS/EP) data session	The data session may be with a server on the NPSBN, or on a server connected to an NS/EP Virtual Private Network (VPN) provided by the commercial service provider, or on the Internet. - How is the NPSBN gateway notified that an NS/EP data session has been invoked? - How does the NPSBN gateway determine whether to route the packet to the NPSBN core, NS/EP VPN, or Internet? - If a data packet is routed to the NS/EP VPN or Internet, what QoS markings does the NPSBN gateway place on the packet? - If a data packet is received from the NS/EP VPN or Internet, what QoS markings does the NPSBN gateway place on the packet?
3 – NS/EP users can originate and receive communications (voice, data and video) with NPSBN users	An NS/EP user using his/her subscribed commercial service can originate a communication to an NPSBN user, and can receive a communication from an NPSBN user	Scenario 3 assumes an NS/EP user does not need to invoke priority to originate a communication.
3.a – Voice and Session-Oriented Video	The NS/EP user originates a voice call or a video (teleconference) session to a user on the NPSBN	The NPSBN gateway is responsible for mapping the signaling and media packets from the commercial network into NPSBN appropriate values. - What priority markings (e.g., RPH) are given to the signaling messages for the call on the NPSBN? - What QoS markings are given to the signaling messages for the call on the NPSBN? - What QoS markings are given to the media for the call on the NPSBN? - What priority markings does the NPSBN gateway place on the signaling messages

		routed to the commercial network? - What QoS markings does the NPSBN gateway place on the signaling messages routed to the commercial network? - What QoS markings does the NPSBN gateway place on the media for the call routed to the commercial network?
3.b – Data	The NS/EP user originates a data session to a user or server on the NPSBN	- What QoS markings does the NPSBN gateway place on packets delivered to the NPSBN? - What QoS markings does the NPSBN gateway place on packets delivered to the NS/EP user?
4 – NS/EP users can invoke / have priority when originating communications to NPSBN users	An NS/EP user using his/her subscribed commercial service, when unable to originate an official communication to an NPSBN user, can invoke / has end-to-end priority	Scenario 4 assumes an NS/EP user invokes priority to originate and receive communications. - How do the priority markings on the NPSBN differ between Scenario 3 and Scenario 4? - Can the NPSBN gateway differentiate between normal and NS/EP calls to place the appropriate markings on traffic sent to commercial networks?
4.a – Voice and Session-Oriented Video	The NS/EP user originates an NS/EP voice call or a video (teleconference) session to a user on the NPSBN	The NPSBN gateway is responsible for mapping the signaling and media packets from the commercial network into NPSBN appropriate values. - What priority markings (e.g., RPH) are given to the signaling messages for the call on the NPSBN? - What QoS markings are given to the signaling messages for the call on the NPSBN? - What QoS markings are given to the media for the call on the NPSBN? - What priority markings does the NPSBN gateway place on the signaling messages routed to the commercial network? - What QoS markings does the NPSBN gateway place on the signaling messages routed to the commercial network? - What QoS markings does the NPSBN gateway place on the media for the call routed to the commercial network?
4.b – Data	The NS/EP user originates a priority (NS/EP) data session to a	- What QoS markings does the NPSBN gateway place on packets delivered to

	user or server on the NPSBN	the NPSBN? • What QoS markings does the NPSBN gateway place on packets delivered to the NS/EP user?

Four NPSBN User Communication Scenarios

Scenario	Description	Considerations for End-to-End Priority
5 – NPSBN users can originate and receive communications with commercial users	An NPSBN user can originate communications to a commercial network user, and can receive communications from a commercial network user (corollary to Scenario 3)	Scenario 5 assumes an NPSBN user does not need to invoke priority to originate and receive communications.
5.a – Voice and Session-Oriented Video	The NPSBN user originates a voice call or a video (teleconference) session	• What priority markings (e.g., RPH) are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the media for the call on the NPSBN? • What priority markings does the NPSBN gateway place on the signaling messages routed to the commercial network? • What QoS markings does the NPSBN gateway place on the signaling messages routed to the commercial network? • What QoS markings does the NPSBN gateway place on the media for the call routed to the commercial network?
5.b – Data	The NPSBN user originates a data session	The data session may be with a server on the NPSBN or on the Internet. • If a data packet is routed to the Internet, what QoS markings does the NPSBN gateway place on the packet? • If a data packet is received from the Internet, what QoS markings does the NPSBN gateway place on the packet?
6 – NPSBN users can invoke /have priority when originating communications to commercial users	An NPSBN user, when unable to originate an official communication to a commercial network user, can invoke and has end-to-end priority (corollary to Scenario 4)	Scenario 6 assumes an NPSBN user invokes priority to originate and receive communications. • Are these priority markings the same or different from the NS/EP markings? • How do the priority markings on the NPSBN differ between Scenario 5 and

		Scenario 6? • Can the NPSBN gateway differentiate between normal and priority NPSBN calls to place the appropriate markings on traffic sent to commercial networks?
6.a – Voice and Session-Oriented Video	The NPSBN user originates a priority voice call or a video (teleconference) session	• What priority markings (e.g., RPH) are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the media for the call on the NPSBN? • What priority markings does the NPSBN gateway place on the signaling messages for the call routed to a commercial network? • What QoS markings does the NPSBN gateway place on the signaling messages for the call routed to a commercial network? • What QoS markings does the NPSBN gateway place on the media for the call routed to a commercial network?
6.b – Data	The NPSBN user originates a priority data session	The data session may be with a server on the NPSBN, or on a server connected to a priority VPN provided by the commercial service provider, or on the Internet. • How is the NPSBN gateway notified that a priority data session has been invoked? • How does the NPSBN gateway determine whether to route the packet to the NPSBN core, priority VPN, or Internet? • If a data packet is routed to the priority VPN or Internet, what QoS markings does the NPSBN gateway place on the packet? • If a data packet is received from the priority VPN or Internet, what QoS markings does the NPSBN gateway place on the packet?
7 – NPSBN devices can originate and receive	An NPSBN device, using a commercial network, can originate communications to	Scenario 7 assumes an NPSBN user traversing a commercial network does not need to “invoke” priority to originate and

communications on commercial networks	commercial network users and NPSBN users, and receive communications from a commercial network user and an NPSBN user (corollary to Scenario 1)	receive communications. However, all communications from the NPSBN device will have priority markings consistent with the Service Level Agreement between the carrier and the FirstNet Board.
7.a – Voice and Session-Oriented Video	The NPSBN user originates a voice call or a video (teleconference) session	The NPSBN gateway is responsible for mapping the signaling and media packets from the commercial network into NPSBN appropriate values. • What priority markings (e.g., RPH) are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the media for the call on the NPSBN? • What priority markings are placed on the signaling messages from the commercial network? • What QoS markings are placed on the signaling messages from the commercial network? • What QoS markings are placed on the media from the commercial network?
7.b – Data	The NPSBN user originates a data session	• What QoS markings does the commercial network place on packets? • What QoS markings does the NPSBN gateway place on packets delivered to the NPSBN?
8 – NPSBN user devices can invoke / have end-to-end priority	An NPSBN user, when unable to originate an official communication on a commercial network, can invoke / has end-to-end priority (corollary to Scenario 2)	Scenario 8 assumes an NPSBN user invokes a "higher" priority than his/her default priority to originate and receive communications. • How do the priority markings on the commercial network differ between Scenario 7 and Scenario 8? • How do the priority markings on the NPSBN differ between Scenario 7 and Scenario 8? • Can the NPSBN gateway differentiate between normal and priority calls to place the appropriate markings on traffic?

8.a – Voice and Session-Oriented Video	The NPSBN user originates a priority voice call or a video (teleconference) session	The NPSBN gateway is responsible for mapping the signaling and media packets from the commercial network into NPSBN appropriate values. • What priority markings (e.g., RPH) are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the signaling messages for the call on the NPSBN? • What QoS markings are given to the media for the call on the NPSBN? • What priority markings are placed on the signaling messages from the commercial network? • What QoS markings are placed on the signaling messages from the commercial network? • What QoS markings are placed on the media from the commercial network?
8.b – Data	The NPSBN user originates a priority data session to a user or server on the NPSBN	• What QoS markings does the NPSBN gateway place on packets delivered to the NPSBN? • What QoS markings does the commercial network place on packets delivered to the NPSBN user?

APPENDIX K: BIBLIOGRAPHY

18 U.S.C. § 1030, ch. 47.

44 U.S.C. § 35.

47 CFR § 64.402.

47 CFR § 90.

47 CFR § 201.2(g).

47 U.S.C. § 53, ch. 5.

47 U.S.C. § 151.

48 Stat. 1064.

E.O. 12382.

E.O. 13618.

E.O. 13636.

Cisco. *Cisco Visual Networking Index: Global Mile Data Traffic Forecast Update, 2012-2017*. White Paper. February 6, 2013. Available: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525/ns537/ns705/ns827/white_paper_c11-520862.pdf.

George Washington University. Space and Advanced Communications Research Institute. *White Paper on Emergency Communications*. January 5, 2006. Available: http://spacejournal.ohio.edu/issue10/PDF/Final_Version_White_Paper.pdf.

Homeland Security Studies and Analysis Institute. *An Analysis of the Primary Authorities Supporting and Governing the Efforts of the Department of Homeland Security to Secure the Cyberspace of the United States*: Final Report. May 24, 2011. Available: http://www.homelandsecurity.org/docs/reports/MHF-and-EG-Analysis-of-authorities-supporting-efforts-of-DHS-to-secure-cyberspace-2011.pdf.

Kim, Gary, *PSTN Transition Will Happen; Only Issue is How*, TMCnet.com, January 30, 2013. Available: http://www.tmcnet.com/topics/articles/2013/01/30/324996-pstn-transition-will-happen-only-issue-how.htm.

Maughan, Douglas, Division Director, Homeland Security Advanced Research Projects, Science and Technology Directorate, U.S. Department of Homeland Security, Research and Development Discussion on March 23, 2013.

National Public Safety Telecommunications Council, Broadband Working Group Priority and QoS Task Group, *Priority and QoS in the Nationwide Public Safety Broadband Network*, April 17, 2012. Available: http://www.npstc.org/download.jsp?tableId=37&column=217&id=2304&file=PriorityAndQoSDefinition_v1_0_clean.pdf.

P.L. 93-112. *The Rehabilitation Act of 1973.* September 26, 1973.

P.L. 112-96. *The Middle Class Tax Relief and Job Creation Act of 2012*. February 22, 2012.

Svensson, Peter, *AT&T Sets Deadline for 2G Sunset in 4* Years, Associated Press, August 3, 2012. Available: http://www.washingtontimes.com/news/2012/aug/3/att-sets-deadline-for-2g-sunset-in-4-years/.

United States. Committee on the National Security Systems. *CNSSP-17: Policy on Wireless Communications: Protecting National Security Information*. May, 2010. Available: http://www.cnss.gov/Assets/pdf/CNSSP-17.pdf.

CNSSP-18: National Policy on Classified Information Spillage. June, 2006. Available: http://www.cnss.gov/Assets/pdf/CNSSP-18.pdf.

United States. Congress. House of Representatives. *Written Testimony of National Protection and Programs Directorate, Office of Cybersecurity and Communications, Deputy Assistant Secretary Roberta Stempfley for a House Committee on Homeland Security, Committee on Emergency Preparedness, Response, and Communications Hearing Titled "Resilient Communications: Current Challenges and Future Advancements*." September 12, 2012. Available: http://www.dhs.gov/news/2012/09/12/written-testimony-nppd-house-homeland-security-subcommittee-cybersecurity-0.

United States. Department of Commerce. *Acting U.S. Commerce Secretary Rebecca Blank Announces Board of Directors for the First Responder Network Authority*. August 20, 2012. Available: http://www.commerce.gov/news/press-releases/2012/08/20/acting-us-commerce-secretary-rebecca-blank-announces-board-directors-.

Fact Sheet: Announcement of the FirstNet Board of Directors: Frequently Asked Questions. August 20, 2012. Available: http://www.commerce.gov/news/fact-sheets/2012/08/20/fact-sheet-announcement-firstnet-board-directors-frequently-asked-questi.

Public Safety Communications Research Program Overview Home Page. Available: http://www.pscr.gov/about_pscr/pscr_about.php.

United States. Department of Commerce. National Telecommunications and Information Administration. FirstNet Board Meeting. September 25, 2012. Available: http://www.ntia.doc.gov/other-publication/2012/9252012-firstnet-meeting-transcript-and-archived-webcast.

United States. Department of Homeland Security. *Blueprint for a Secure Cyber Future: The Cybersecurity Strategy for the Homeland Security Enterprise*. November, 2011. Available: http://www.dhs.gov/xlibrary/assets/nppd/blueprint-for-a-secure-cyber-future.pdf.

DHS Announces First National Preparedness Goal. October 7, 2011. Available: http://www.dhs.gov/news/2011/10/07/dhs-announces-first-national-preparedness-goal.

Emergency Communications Preparedness Center Home Page. Available: http://www.dhs.gov/emergency-communications-preparedness-center.

National Incident Management System. December, 2008. Available: http://www.fema.gov/pdf/emergency/nims/NIMS_core.pdf.

Quadrennial Homeland Security Review Report: A Strategic Framework for a Secure Homeland. February, 2010. Available: http://www.dhs.gov/xlibrary/assets/qhsr_report.pdf.

SAFECOM Program Home Page. Available: http://www.dhs.gov/safecom-program.

United States. Department of Homeland Security. National Security Telecommunications Advisory Committee. *Report to the President on Cloud Computing*. May, 2012. Available: http://ncs.gov/nstac/reports/2012-05-15%20NSTAC%20Cloud%20Computing.pdf.

Report to the President on Communications Resiliency. April, 2011. Available: http://www.ncs.gov/nstac/reports/NSTAC%20Report%20to%20the%20President%20on%20Communications%20Resiliency%20(2011-04-19)(Final)(pdf).pdf.

Report to the President on Emergency Communications and Interoperability. January, 2007. Available: http://www.ncs.gov/nstac/reports/2007/NSTAC%20Report%20on%20Emergency%20Communications%20and%20Interoperability.pdf.

Report on National Security and Emergency Preparedness Internet Protocol- Based Traffic. November, 2008. Available: http://www.ncs.gov/nstac/reports/2008/NSEP%20IP-Based%20Traffic%20Report.pdf.

Report to the President on Identity Management Strategy, May 2009. Available: http://www.ncs.gov/nstac/reports/2009/NSTAC%20IDTF%20Report.pdf.

United States. Department of Homeland Security. Wireless Priority Service. *Program Information Home Page*. Available: https://www.dhs.gov/wireless-priority-service-wps.

United States. Department of Justice. *National Forum on Public Safety Broadband Needs*. August 23, 2010. Available: http://www.cops.usdoj.gov/Publications/e021111338-broadband-forum.pdf.

United States. Executive Office of the President. National Security and Emergency Preparedness Executive Committee. Letter to Mr. Chuck Donnell and attached Memorandum signed by Mr. Michael W. Locatis and Ms. Teresa M. Takai. November 6, 2012.

United States. Federal Communications Commission. *700 MHz Public Safety Broadband Nationwide License: WQQE234: First Responder Network Authority*. November 15, 2012. Available: http://wireless2.fcc.gov/UlsApp/UlsSearch/searchLicense.jsp. Search by call sign WQQE234.

National Broadband Plan: Chapter 16: Public Safety. March 2010. Available: http://www.broadband.gov/plan/16-public-safety/.

Recommended Minimum Technical Requirements to Ensure Nationwide Interoperability for the Nationwide Public Safety Broadband Network. May 22, 2012. Available: http://apps.fcc.gov/ecfs/document/view?id=7021919873.

United States. Federal Communications Commission. Communications Security, Reliability and Interoperability Council. Working Group 7: Pandemic Planning: Priority Service Requirements. *Final Report: Planning for NS/EP Next Generation Network Priority Services During Pandemic Events*. December 2010. Available: http://transition.fcc.gov/pshs/docs/csric/CSRIC_WG7_Final_Report_NGN_Priority_20101216.pdf.

United States. Federal Communications Commission. National Telecommunications and Information Administration. *Comments Regarding Implementing a Nationwide Broadband , Interoperable Public Safety Network in the 700 MHz Band* . June 10, 2011. Available: http://www.ntia.doc.gov/fcc-filing/2011/ntia-comments-regarding-implementing-nationwide-broadband-interoperable-public-safet.

"Middle Class Tax Relief and Job Creation Act of 2012: Title VI – Public Safety Communications and Electromagnetic Spectrum Auctions." Presentation. Adapted from a presentation by Anna Gomez, Assistant Secretary, NTIA. March 15, 2012. Available: http://www.nfpa.org/assets/files/metro%20chiefs/2012conffirstnet.pptx.

United States. Federal Communications Commission. Office of the Chairman. *Letter to The Honorable Henry A. Waxman, Chairman, Committee on Energy and Commerce, U.S. House of Representatives from Julius Genachowski, Chairman of the Federal Communications Commission*. July 20, 2010. Available: http://democrats.energycommerce.house.gov/sites/default/files/documents/HAW-FCC-7-20-2010.pdf.

United States. Library of Congress. Congressional Research Service. *An Emergency Communications Safety Net: Integrating 911 and Other Services*. September 1, 2005. Available: https://opencrs.com/document/RL32939/2005-09-01/.

Funding Emergency Communications: Technology and Policy Considerations, December 14, 2011. Available: http://www.fas.org/sgp/crs/homesec/R41842.pdf.

Public Safety Communications and Spectrum Resources: Policy Issues for Congress. July 23, 2010. Available: https://opencrs.com/document/RL40859/2010-07-23/.

National Special Security Events. March 24, 2009. Available: http://www.fas.org/sgp/crs/natsec/RS22754.pdf.

The Use of Federal Troops for Disaster Assistance: Legal Issues. November 28, 2008. Available: https://opencrs.com/document/RS22266/.

United States. National Institute of Standards and Technology. Visiting Committee on Advanced Technology. *Desirable Properties of a Nationwide Public Safety Communication System*. January 24, 2012. Available: http://www.nist.gov/director/vcat/upload/Desirable_Properties_of_a_National_PSN.pdf.

National Strategy for Trusted Identities in Cyberspace. Available: http://www.nist.gov/nstic/.

United States. President. *Homeland Security Policy Directive/HSPD-5: Management of Domestic Incidents*. February 28. 2003. Available: http://www.gpo.gov/fdsys/pkg/PPP-2003-book1/pdf/PPP-2003-book1-doc-pg229.pdf.

United States. White House. *The Benefits of Transitioning to a Nationwide Wireless Broadband Network for Public Safety*. June, 2011. Available: http://www.whitehouse.gov/sites/default/files/uploads/publicsafetyreport.pdf.

National Security Action Memorandum 252: Establishment of the National Communications System. July 11, 1963. Available: http://www.jfklibrary.org/Asset-Viewer/mOsd6HP9gkG_mqGvJhY1qA.aspx.

Presidential Policy Directive 21: Critical Infrastructure Security and Resilience. February, 2013. Available: http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil.

Welsh, Shawn, *The 2G Sunset has Begun*, SDM Magazine, March 2013. Available: http://www.sdmmag.com/articles/the-2g-sunset-has-begun.

Briefings

Alagna, Mike. Motorola Solutions. "NSTAC NPSBN Primer: Long Term Evolution Panel." July 19, 2012.

Basham, Craig. Joint Wireless Program Management Office, DHS. "DHS Next Generation Broadband Tactical Communications Approach." September 13, 2012.

Black, Stacey, AT&T Public Safety Solutions. "Considerations for Deploying LTE for a Public Safety Broadband Network." July 19, 2012.

Bratcher, Jeff and Orr, Dereck. Public Safety Communications Research Program, U. S. Department of Commerce. "Public Safety LTE Technology and ay Forward." February 17, 2012.

DeRango, Mario. Vice President, Advanced Systems Architecture, Chief Technology Office, Motorola Solutions. "Response to the NSTAC NPSBN Subcommittee Questions on BAA 12-10."
September 20, 2012.

Dolly, Martin. Lead Member of Technical Staff, AT&T. "LTE Evolution – NS/EP Implications for the NSTAC NPSBN Tasking." September 20, 2012.

Einsig, Barry. Chair, The Joint Council of Transit Wireless Communications. "NSTAC: Nationwide Public Safety Broadband Network Subcommittee Meeting." August 30, 2012.

Filios, Paul. Defense Information Systems Agency, U.S Department of Defense. "Mobility." August 14, 2012.

Flaherty, Laurie. U.S. Department of Transportation. "Next Generation 911, Alerts and Warnings, and Intersections with the NPSBN." March 16, 2012.

Fontes, Brian. National Emergency Number Association. "Next Generation 911, Alerts and Warnings, and Intersections with the NPSBN." March 16, 2012.

Fontes, Brian and Tray Forgety. NENA. "Deployment of Broadband Networks to Support NG911 Big Data Analytics." September 25, 2012.

Harrison, Regina. National Telecommunications and Information Administration, U.S. Department of Commerce. "First Responder Network Authority Update." August 2, 2012.

Herckis, Mitchel. National League of Cities. "State and Local Public Safety Perspective." March 9, 2012.

Hewitt, Ronald, Director, Office of Emergency Communications, DHS. "NS/EP Communications Definition." October 2, 2012.

Hogsett, Heather. National Governors Association. "State and Local Public Safety Perspective." March 9, 2012.

Holgate, Rick. Assistant Director for Science and Technology/CIO, Bureau of Alcohol, Tobacco, Firearms, and Explosives. "FirstNet Security Policy Issues." September 25, 2012.

Kilbourne, Brett and Parks, Prudence. Utilities Telecom Council. "700 MHz National Public Safety Broadband Network. Implications for Access by Utility and Critical Infrastructure Industries." August 30, 2012.

King, Pamela. Office of Emergency Communications, DHS. "Emergency Communications Preparedness Center (ECPC)." January 10, 2013.

Lipford, Mark and Migaldi, Scott. Sprint Nextel. "3rd Generation Partnership Program (3GPP) A View of Release 12 and Beyond." September 20, 2012.

Martin, Jay. Science and Technology Directorate, DHS. "Wireless Broadband Technology Demonstrator." September 13, 2012.

Martinez, Dennis. Harris Corporation and Interoperability Board Member. "Technical Advisory Board for

First Responder Interoperability (Interoperability Board)." August 2, 2012.

Miller, Trent. Chief Technology Office, Motorola Solutions. "NSTAC Priority and QoS on the NPSBN." August 14, 2012.

McEwen, Harlin, (Chief, Retired). Public Safety Spectrum Trust. "Federal Communications Commission/700 MHz Spectrum Update." March 14, 2012.

Nolan, David. Office of Emergency Communications, DHS. "NS/EP Requirements for the NPSBN." February 24, 2012.

Patrick, Paul. Chair, Communications Technology Committee National Association of State EMS Officials. "21st Century EMS Communications Systems: 'Brick' to the Tricorder." August 30, 2012.

Phythyon, Dan. Office of Emergency Communications, DHS. "NPSBN Legislative Status." February 24, 2012.

Reyes, Eddie, Deputy Chief, City of Alexandria Police Department. "State and Local Organizations/Early Adopter." February 10, 2012.

Rosenberg, Jonathon. General Manager Product Strategy and Research, Skype. "Skype Briefing for the National Security Telecommunications Advisory Committee (NSTAC)." October 16, 2012.

Robinson, Chuck. City of Charlotte and Interoperability Board. "Challenges and Success Factors in Establishing an NPSBN." March 23, 2012.

Rush, Scott. Lockheed Martin. "Intelligence-Driven Defense." September 25, 2012.

Schrier, Bill. Chief Technology Officer, City of Seattle. "Birthing the Nationwide Public Safety Wireless Broadband Net." March 23, 2012.

Suraci, Frank. Office of Emergency Communications, DHS. "NSTAC Nationwide Public Safety Broadband Network Panel Discussion." August 14, 2012.

Surma, Tony. Senior Director and CTO Microsoft Disaster Response. "Microsoft Disaster Response Enabling Community Responses." October 4, 2012.

Toigo, Jennifer and Richard VonBostel. Department of Justice. "Broadband Use by DOJ's Law Enforcement Field Users." October 2, 2012.

Waxman, Laura. U.S. Council of Mayors. "State and Local Public Safety Perspective." March 9, 2012.