March 1, 2017

WORKING GROUP 8
Priority Services

Final Report

Table of Contents

1 Executive Summary / Results in Brief

The evolution to packet-based networks, combined with the rapid innovation in communications technology to which priority services users have grown accustomed over the past decade, creates both challenges and opportunities with respect to the long term provision and planning of priority services. At the same time, the Department of Homeland Security (DHS) / Office of Emergency Communications (OEC) reports that growth in national security and emergency preparedness (NS/EP) priority services users have grown consistently at 3-5% per year since 2010; however a number of factors, including future changes in policy, expansion of the programs to incorporate non-human / proxy devices, or the occurrence of a major event / disaster which expands the need for extended priority communications, could augur a significant and transformative increase in both users and priority traffic.

The OEC is currently executing a Next Generation Networks Priority Services acquisition program, to evolve priority communications features and capabilities from circuit-switched networks to IP-based packet-switched networks. In addition, the Middle Class Tax Relief and Job Creation Act of 2012 contains provisions to create an interoperable NPSBN for Public Safety Entities. The Act created the First Responder Network Authority (FirstNet), an independent authority within the National Telecommunications and Information Administration, and outlined a governing framework for the deployment and operation of the National Public Safety Broadband Network (NPSBN) based on a single nationwide network architecture.

This report seeks to outline a framework to permit the evolution of priority services policy in light of changing user needs, market trends, and networking capabilities. Following introduction, history and background, the report's findings and recommendations are divided into three sections:

- Findings related to ongoing stewardship of the priority services user community, including keeping pace with usability expectations and continued outreach and education **(Section 5.2)**

- Findings related to the evolving applications necessary for future priority communications beyond traditional voice, including Short Message Service (SMS), video, and Internet of Things (IoT) applications **(Section 5.3)**

- Findings related to network capabilities, including quality-of-service, authentication, security, and anti-spoofing measures **(Section 5.4)**

Finally, **Section 6** of the report lists several questions for further review specific to the roll-out of FirstNet. The Working Group recommends that policy-makers and future advisory groups consider these questions as that program proceeds.

The following represents a summary of findings and recommendations emerging from Working Group 8's research.

- While there are no obvious dysfunctions in the current operations and provision of priority service, and the existing programs have a long history of managing change without disruption, policy-makers and suppliers should continue to seek opportunities to prepare for increased volume and scale – particularly as relates to automated ordering / provisioning

- Policy-makers should consider the potential impacts of provisions which reduce priority access of certain priority services users under particularly heavy congestion.

- Policy-makers should reaffirm existing guidance with respect to user classifications (e.g., FCC R&O 00-242), and clear guidelines should be given as to priority assigned to different roles in the face of limited capacity and events that invoke a high density of priority users. Similarly, policy-makers should provide clarification going forward related to pre-emption of communications for non-priority and lower-priority users (on a per application basis), in a congested environment. Relative priority classification of 911 and priority services communications in light of technical capabilities (i.e., LTE) should continue to be assessed.

- Policy-makers and suppliers should continue working with application, social media, and content providers relative to priority access to critical information.

- As evolution of non-domestic priority services increases, policy-makers should seek opportunities to support commonality in priority assignment and QoS for communications which cross national borders.

- The priority service user community (e.g., national security, emergency preparedness, emergency responder communities) should work closely with the networking industry to create and refine the set of application classes that may be needed for priority services treatment, including consideration given to IoT devices.

2 Introduction

2.1 CSRIC Structure

Communications Security, Reliability, and Interoperability Council (CSRIC) V CSRIC Steering Committee - Working Group Structure										
Susan Sherwood	Francisco Sanchez	Steven Johnson	Kent Bressie	Jennifer Manner	Rod Rasmussen	Brian Scarpelli	Bill Boni	William Reidway.	Brian Daly	John Kimmins
Jeff Cohen	Farrokh Khatibi	Kelly Williams	Catherine Creese		Chris Boyer	Joel Molinoff	Drew Morin	Thomas Anderson		Danny McPherson
Working Group 1: Evolving 911 Services	**Working Group 2**: Emergency Alerting Platforms	**Working Group 3**: Emergency Alert System	**Working Group 4**: Communications Infrastructure Resiliency	**Working Group 4**: Communications Infrastructure Resiliency	**Working Group 5**: Cybersecurity Information Sharing	**Working Group 6**: Secure Hardware and Software – Security-by-Design	**Working Group 7**: Cybersecurity Workforce	**Working Group 8**: Priority Services	**Working Group 9**: WiFi Security	**Working Group 10**: Legacy Systems and Risk Reduction
			Sub-Group A: Submarine Cable Resiliency	**Sub-Group B**: Network Timing Single Source Risk Reduction						

Table 1 – CSRIC V Working Group Structure

2.2 Working Group 8 Team Members

Working Group 8 consists of the members listed below.

Name	Company
Thomas Anderson - Co-chair	Cisco
Bill Reidway - Co-chair	Neustar
Greg Schumacher	Sprint
Natalie Baker	Intrado
Chris Oberg	Verizon
Calvin Blankenship	Verizon
Zachary Johnson	DHS
Jason Weil	TWC
John Brzozowski	Comcast
Lynette Van Someren	Comcast
Martin Dolly	AT&T / ATIS
Keylor Eng	AT&T
Bill Mertka	Motorola / ATIS
Stacy Hartman	CenturyLink
Kathryn Condello	CenturyLink
Matt Tooley	NCTA
Kevin Beaudry	Charter
Ingrid Caples	HHS

Joanne Sechrest	DHS
Rob Dew	DHS
Howard Brown	TDS
Tim Perrier	FCC
Ken Burnley	FCC

Table 1 - List of Working Group Members

3 Objective, Scope, and Methodology

3.1 Objective

The following set of objectives was given to Working Group 8 as part of the CSRIC V charter:

> Priority communications over commercial networks during a national emergency remains as essential today to responders and national security personnel as in decades past. However, commercial communications networks are increasingly relying on packet-based technology and retiring Time Division Multiplexing (TDM) technology. The Federal government is at risk of losing priority capabilities throughout this transition, as voice priority services rely on wireline TDM, which will eventually be replaced by IP-based infrastructure. Lack of priority communications services on packet-based systems could jeopardize national security or domestic incident response.
>
> – How a next-gen Priority Services framework will address authentication, authorization, privacy, eligibility and security.
> – Evaluation of barriers, both administrative and technical (e.g., How to authenticate and what is the appropriate access control mechanism?).
> – Definition of capabilities for national and overseas access and termination.
> – Description of potential ordering, billing and provisioning options for the next generation priority service.
> – Outline of network management best practices needed to enable priority services for NS/EP personnel.

3.2 Scope

The next generation priority services framework must address the needs of a priority services user with an authorized role and associated level of priority, that originates or terminates one or more communication applications over a variety of network contexts where one or more of these networks is experiencing significant congestion.

Following the objectives laid out above, and in recognition of the ongoing work across the communications industry and the Federal Government executive branch to maintain and evolve the services which enable priority communications, this report will seek to create a framework for definition of future policy requirements for application classification, user expectations, and network standards in light of the flexibility offered by packet-based networks. In particular, the working group has focused on how a priority service framework can address scenarios where a given user's priority status can change dynamically in response to the evolving needs during a crisis event:

- As the applicable emergency event unfolds, the role assigned to a user may change dynamically. For example, users that have been confined in the emergency area (e.g., they are trapped or are being held hostage), could be dynamically assigned a role with a priority higher than they might otherwise warrant. In this specific case, SMS and/or voice priority can be useful to help ensure effective communication with the confined party.
- As the event unfolds, the importance and as such the relative priority of an assigned role may need to change dynamically.
- A user involved in this event may play multiple or changing roles throughout the life of the event.
- For a given role, the assigned priority may be application class dependent. For example, a specific role might be defined that provides high priority voice and/or SMS service but not high priority data service, e.g., Internet access.

In addition, a new priority services framework must account for the needs of a new set of constituents, including connected devices under the umbrella of the Internet-of-Things, which opens opportunities to prioritize devices which monitor and support critical infrastructure during a crisis event. Finally, the framework must accommodate the need for priority services users to access, with priority, information provided by general Internet servers and social media sites.

NOTE: This draft report of June 30, 2016 seeks to define key aspects of the priority services framework, and establish a baseline for recommendations to be finalized by the end of 2016. The final report will be also augmented by additional analysis in key areas still under review by the working group (notably the framework's alignment with FirstNet deployment and user onboarding).

3.3 Methodology

Working Group 8 includes experts in the current provision of priority services, as well as representatives from service providers, network and Operational Support System (OSS) suppliers, standards bodies, and government agencies. Since its charter in November 2015, the members have established bi-weekly meetings to define scope, propose research areas, and develop recommendations. The group conducted two face-to-face meetings in Washington DC in 2016.

To inform its recommendations, the working group has participated in working sessions and user group events with the FCC's Public Safety and Homeland Security Bureau and Technical Advisory Committee, as well as the Office of Emergency Communications.

4 Background

4.1 Existing Priority Services Programs (GETS, WPS, NGN-PS, TSP)

The Department of Homeland Security (DHS) provides and manages priority telecommunications services programs to support national security and emergency preparedness

(NS/EP) communications for government officials, emergency responders, and critical infrastructure owners and operators. The establishment of priority telecommunications services was directed by the White House in national policy and requirements over 30 years ago. Two of these priority services: Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS) are maintained in a constant state of readiness for use in an emergency or crisis situation when the public telephone networks are congested and the probability of completing a normal call is reduced. GETS improves call completion over public wireline networks and WPS improves call completion over public wireless networks. The current GETS and WPS services are based on legacy, circuit-switched networking technology which is being retired by industry. Accordingly, for the past ten years DHS has implemented a Next Generation Networks (NGN) Priority Services Program in key national service providers' networks to evolve priority services to the modern Internet Protocol (IP)-based, packet-switched networking technologies. The Telecommunications Service Priority (TSP) program enables telecommunications carriers to prioritize the restoration, recovery, and installation of critical circuits and voice capabilities.

4.1.1 History

In the late 1970s and early 1980s commercial long distance service providers under contract to the Federal Government performed studies of the Public Switched Telephone Network (PSTN) to determine the potential advantages of priority services for critical government stakeholders. Using the results of these studies, the Government established a national-level program, termed the Nationwide Emergency Telecommunications Service (NETS), to provide priority telecommunications for NS/EP users. The NETS architecture leveraged multi-service provider communications capabilities augmented with substantial Government investment in unique equipment and procedures. In March 1991, the White House recommended a Panel of Experts review the NETS program to examine alternate technologies that might result in cost savings. The Panel of Experts' review reaffirmed the need for an NS/EP priority telecommunications program; however, the panel recommended an alternate, PSTN-based solution that would enhance service robustness under severe network damage, maintain technical currency, and reduce costs. Following the panel's recommendations, the NETS program was restructured, and a revised service architecture was adopted. The new architecture, coupled with a different acquisition strategy, became the GETS program. The GETS program was approved by the White House in December 1991.

GETS capability reached initial operational capability in 1995 and achieved full deployment status on September 30, 2001. This was fortuitous as GETS was used extensively during and in the aftermath of the attacks on the World Trade Center towers and the Pentagon in September 2001. GETS includes priority enhancements in U.S. long distance and local service provider networks nationwide. In more than 20 years of service, GETS has provided vital communications capabilities during numerous hurricanes, earthquakes, floods, and wildfires, the Oklahoma City Bombing and the 9-11 attacks.

On October 19, 1995, a petition for rulemaking was submitted to the Federal Communications Commission (FCC) regarding NS/EP priority services for wireless networks. In response, on July 13, 2000 the FCC released a Second Report and Order (R&O) on wireless Priority Access

Service (PAS). This R&O authorizes service providers to offer priority wireless service to NS/EP users with liability protections. Following the 9-11 attacks, the National Security Council met in October 2001 to discuss the effectiveness of NS/EP telecommunications. The meeting resulted in tasking to immediately implement a priority cellular telephony service solution in Washington, D.C., and to recommend other metropolitan areas for implementation. The tasking also required the development of a plan to provide a nationwide priority cellular telephony service, targeted for operation within one year. Beginning in 2001, development and deployment was initiated for a nationwide, end-to-end, Wireless Priority Service (WPS). Both GETS and WPS were structured by the FCC to not be pre-emptive of public traffic.

The WPS capability reached full deployment status on the predominant U.S. wireless technologies, Global System for Mobile Communications (GSM), Integrated Digital Enhanced Network (iDEN), and Code Division Multiple Access (CDMA), in 2006, 2006, and 2009, respectively. Beginning in July 2008, development of a WPS Enhanced Overload Performance (EOP) capability was undertaken with the major wireless infrastructure vendors for implementation in the WPS CDMA service provider networks. During times of extreme congestion, the WPS EOP capability addresses handset-to-tower signaling overload, tower-to-handset paging overload, and real-time network processing overload conditions. Full deployment for WPS EOP was achieved in April 2015. A priority signaling capability similar to WPS EOP was also developed and deployed in 2015 for select third generation (3G) Universal Mobile Telecommunications System (UMTS) wireless networks. In its nearly 15 years of operation, WPS has supported NS/EP operations during hurricanes, tornados and floods, and provided critical communications capabilities during the Boston Marathon Bombing.
In the mid-2000s, DHS initiated planning and studies on the steps and developments needed to transition priority services to IP-based networking technologies. Initial activities included enhancing the gateways located at network-to-network interfaces to translate the priority signaling between circuit-switched and packet-switched formats. In 2010 approval was granted for the NGN Priority Services Acquisition Program—a Category 1, multi-phase, multi-increment effort to evolve GETS and WPS to IP technologies and to expand priority services to include data, video and information services capabilities.

4.1.2 Policy and Requirements

Several executive policies and directives support the existence and use of NS/EP priority telecommunication services. Foremost among these is Executive Order 13618, *Assignment of National Security and Emergency Preparedness Communications Functions*, signed by President Obama on July 6, 2012, and its predecessor Executive Orders. Additionally, the Federal Communications Commission's Second Report and Order, FCC 00-242, *Establishment of Rules and Requirements For Priority Access Service*, adopted on July 3, 2000, was instrumental in providing NS/EP personnel access to priority wireless telecommunications systems.

Requirements for NS/EP priority telecommunications services are identified in Government directives, orders and memoranda, and evolve from recommendations from Presidential advisory committees and working groups. Primary priority telecommunications services requirements include the following:

- Voice-band Service: The service must provide voice-band service in support of Presidential communications.
- Interoperability: The service must interoperate with and use the resources of selected other Government or private-sector facilities, systems, and networks through the application of standards.
- Survivability/Endurability: The service must provide for the interconnection of surviving users under a broad range of circumstances from widespread damage from natural or manmade disasters up to and including nuclear war.
- International Interface: The service must provide access to and egress from international locations.
- Nationwide Coverage: The service must provide readily available nationwide coverage to support the national security leadership and inter/intra-agency emergency operations.
- Intra/Inter-agency Emergency Operations: Common user services must provide NS/EP traffic with priority service.

4.1.3 Priority Services Users

The NS/EP community spans the Federal, State, local, tribal and territorial governments, critical infrastructure sectors in industry, and non-profit organizations. Typical priority services users are responsible for the command and control functions critical to management of, and response to, national security and emergency situations, particularly during the first 24 to 72 hours following an event. Figure 1 provides a summary of current priority services users, their organizational affiliation and distribution, and an indication of the growth in the number of priority services users over the past 6 years. The annual growth rate in the number of priority services users has typically been 3-5%. A large growth rate in the number of users is not expected without a major event, a change in policy, or a new capability such as priority for data to support emerging needs such as Internet of Things (IoT).

	2010		2016	
	GETS	WPS	GETS	WPS
Federal Government	116,942	74,034	121,028	74,456
State and Tribal Government	29,330	5,544	37,734	9,987
Local Government	57,172	10,584	79,397	19,758
National Security/Emergency Preparedness Industry & Non-Government Organizations	60,466	15,408	102,899	35,814
Total Users	263,910	105,570	341,058	140,015

Figure 1. Priority Services User Statistics

The potential magnitude of the NS/EP priority services user base is estimated to range between 2 million and 15 million, dependent largely on which NS/EP roles and responsibilities are included in the base. In 2008, the Office of the Manager, National Communications System (OMNCS) conducted a study to determine the potential NS/EP user population. A resulting paper published in November 2008 indicated a potential NS/EP user population of about 2 million. This user population consists only of members of the traditional NS/EP community, e.g., officials of various governments, first responders, and industry and community leaders.

In December 2010, the Federal Communications Commission's Communications Security, Reliability and Interoperability Council (CSRIC) published a study on the use of Next Generation Network NS/EP priority services during pandemic events. In estimating the magnitude of priority communications services users during a pandemic, the CSRIC report referenced a January 2007 report prepared by the President's National Security Telecommunications Advisory Committee (NSTAC) which identifies a potential NS/EP priority communications services user base of 8 – 10 million users. This NS/EP user base includes first responders, national response and federal response plan users, National Incident Management System (NIMS) users, NS/EP users, Critical Infrastructure (CI) owners, operators and decision makers, key municipal leadership and decision makers, public health systems, and cyber security and public warning stakeholders. Additionally, the CSRIC study cited a 2009 Partnership for Critical Infrastructure Security (PCIS) report that identifies the number of "mission-critical" Tier 1 and Tier 2 users expected during a pandemic as 15 million. The difference cited by CSRIC between the 10 million users identified in the NSTAC report and the 15 million users identified in the PCIS report is PCIS' inclusion of key personnel, including accounting and payroll personnel, necessary to keep organizations running during a pandemic. Based on these sources, CSRIC estimated that up to 15 million mission-critical personnel may require priority communications during a pandemic. These mission-critical personnel would represent approximately 5 percent of the population of the U.S.

4.2 Existing NS/EP Priority Services

4.2.1 Government Emergency Telecommunication Service (GETS)

GETS improves the probability of call completion over public wireline telephone networks during emergencies when congestion may arise due to increased call volumes and/or damage to communications infrastructure. GETS priority features have been implemented on both local and long distance wireline networks, and these features are maintained in a constant state of readiness. GETS is an easy-to-use calling card service that is accessible nationwide and from most international locations. To access GETS, users dial a universal access number (710-NCS-GETS) using common telephone equipment and enter a personal identification number (PIN). Once authenticated, calls placed through GETS receive priority over normal calls. However, GETS calls do not preempt calls in progress or prevent the general public's use of the telephone network.

4.2.2 Wireless Priority Service (WPS)

The WPS service provides priority calling for authorized personnel when the cellular networks are congested and the probability of completing a call is reduced. WPS priority features have been implemented on all nationwide and several regional cellular service provider networks, and these features are maintained in a constant state of readiness. WPS is an easy-to-use, add-on feature to cellular telephone subscriptions. In the event of wireless network congestion, an NS/EP user invokes the WPS service on a WPS-enabled phone by dialing *272 prior to dialing the desired destination number. The WPS call receives priority over public calls; however, WPS calls do not preempt calls in progress or deny the general public's use of the radio spectrum.

4.2.3 Next Generation Networks (NGN) Priority Services Program

The NGN Priority Services Program is a DHS initiative to evolve priority communications features and capabilities from circuit-switched networks to IP-based packet-switched networks. Initial NGN activities in the mid-2000s included planning, studies and enhancement of network gateways interfacing circuit-switched and packet-switched networks. Later in the decade, approval was granted for the Category 1 NGN Priority Services Acquisition Program. This DHS program is a multi-phase, multi-increment effort as depicted by the Acquisition Plan shown pictorially in Figure 2.

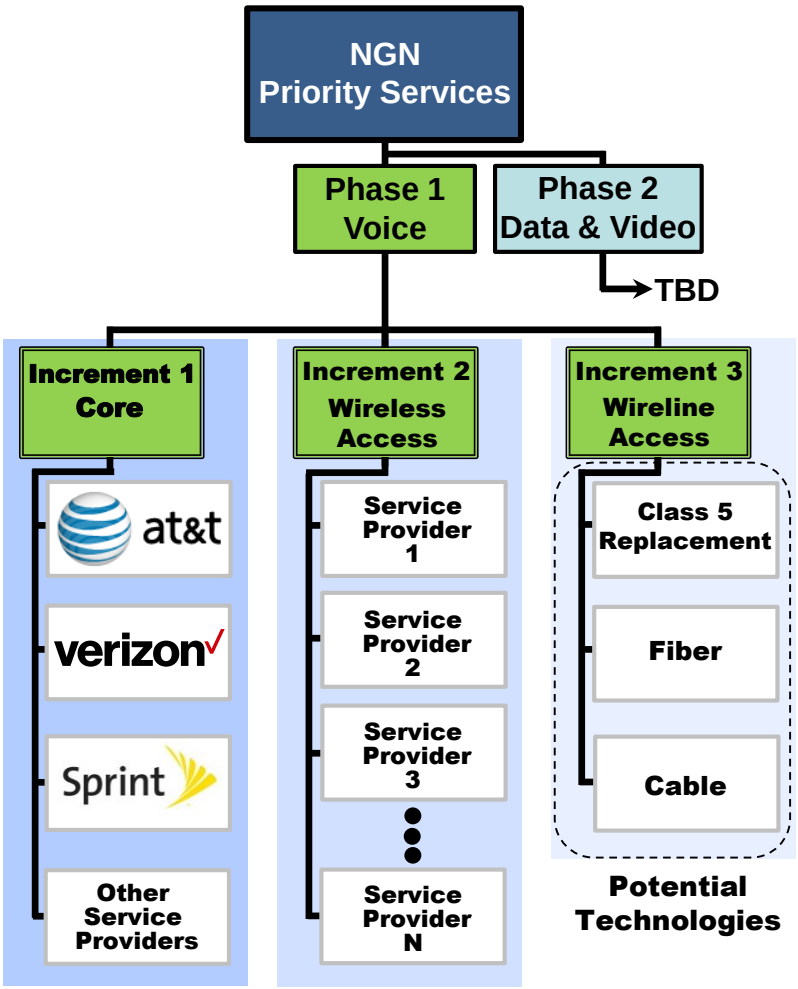


Figure 2. DHS Next Generation Network Priority Services Acquisition Plan

During Phase 1 (Voice), the NGN Priority Services Program is acquiring priority voice capabilities on IP networks comparable to legacy GETS and WPS. Beginning in 2010 with Increment 1 (Core), GETS priority features are being developed and implemented in the Core IP networks of the three GETS long distance service providers. The priority features being acquired include, among others, priority treatment, alternate routing, route diversity, exemption from network management controls, user authentication, and quality of service. To ensure continuity of GETS service, the service provider NGN core networks will interface with legacy,

circuit-switched, local networks, and IP-based access networks. The NGN GETS capability had a service introduction in the Core IP networks in 2013. Full deployment status for NGN GETS in Core IP networks is slated for 2019.

In 2015, planning and development was initiated to acquire priority WPS features in wireless service provider fourth generation (4G), Long Term Evolution (LTE) networks. The resulting Voice over LTE (VoLTE) solutions are expected to incorporate advanced features and capabilities of LTE networks such as Access Class Barring (ACB), High Priority Access (HPA), Allocation and Retention Priority (ARP), and Quality Class Identifier (QCI). DHS has been active in the Standards Development Organizations to establish associated standards for priority services for these LTE features. Late in 2015 DHS started related technology demonstrations and development efforts with a few nationwide wireless service providers. Initial service introduction for WPS on VoLTE is planned for 2018; full deployment status is anticipated in 2020.

Under Phase 2 (Data and Video) the NGN Priority Services Program will acquire priority data, video and information services capabilities on the service providers' wireline and wireless IP telecommunications networks. Priority data services are anticipated to include services such as email, SMS, enterprise access, Web access/browsing, and other currently used data services. Early in 2016 DHS initiated Phase 2 acquisition planning. Comprehensive acquisition activities will commence following formal approvals for an NGN Phase 2.

4.2.4 Telecommunications Priority Services (TSP)

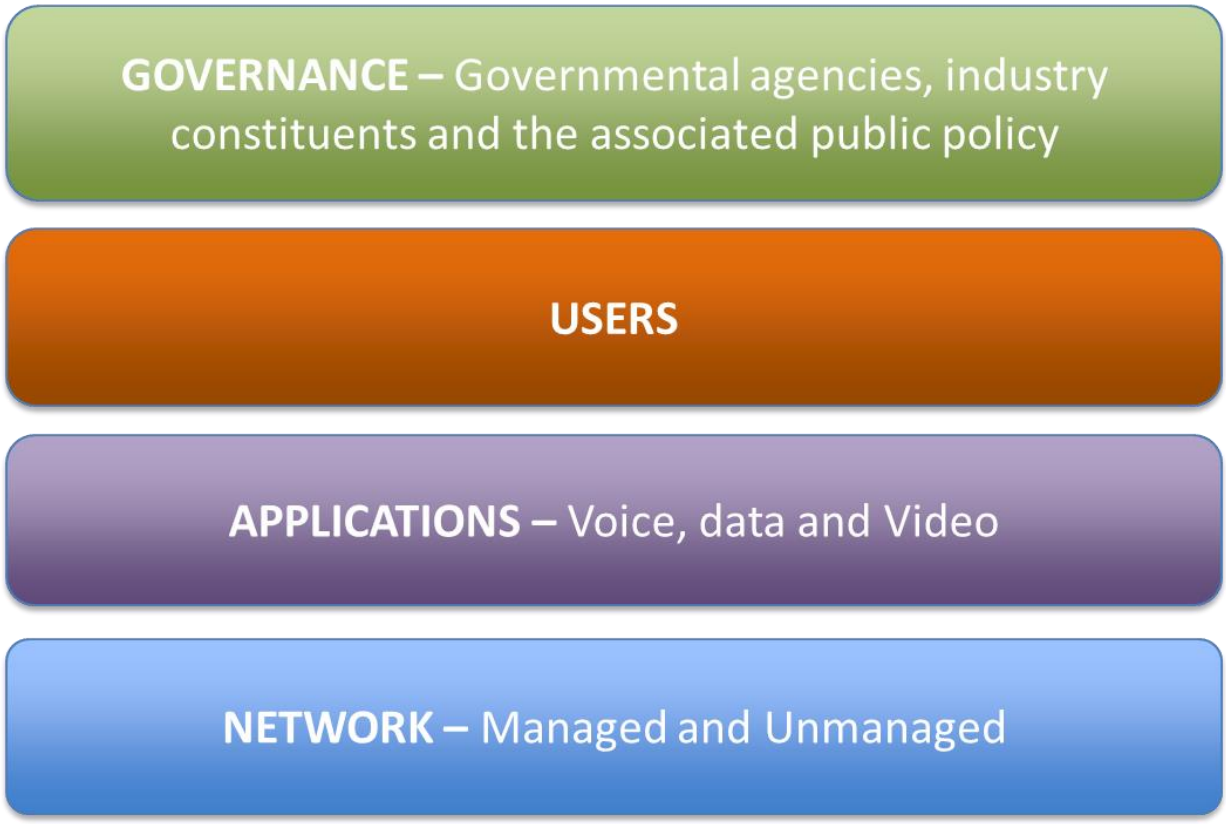
Telecommunications Priority Service (TSP) is a government program that authorizes NS/EP organizations to receive priority restoration and installation of vital voice and data circuits or other telecommunications services that may be damaged as a result of a natural or man-made disaster. TSP enables telecommunications carriers to prioritize the restoration, recovery, and installation of critical circuits and voice capabilities. TSP contributes to rapid NS/EP communications recovery, but recent technology changes will not have an impact on the program. For this reason, TSP will not be a focus of this report.

4.3 FirstNet and Next Generation-911

In February 2012, Congress enacted the Middle Class Tax Relief and Job Creation Act of 2012 (the Act), containing provisions to create an interoperable NPSBN for Public Safety Entities (PSEs). A PSE is defined in Section 6001(26) of the Act as an "entity that provides public safety services" 47.U.S.C. § 1401(26). The Act created FirstNet, an independent authority within the National Telecommunications and Information Administration, and outlined a governing framework for the deployment and operation of the NPSBN based on a single nationwide network architecture. FirstNet and its funding represents an opportunity to shape regulation to support the priority communications landscape.

5 Analysis, Findings and Recommendations

This section of the document describes a priority services framework which can address a wide range of voice, data and video applications to support national security and emergency preparedness communications for government officials, emergency responders, critical infrastructure owners and operators, and vital industry members. The framework consists of four major components:



- Governance – Governmental agencies, industry constituents and the associated public policy considerations.
- Users – identified priority users to support national security and emergency preparedness communications
- Applications – the broad application space of voice, data and video applications that will be needed by priority users in support of national security and emergency preparedness communications
- Networks – the complex web of managed and unmanaged networks which fundamentally must support the priority needs of users and their associated applications.

5.1.1 Summary of Recommendations

The following represents a summary of findings and recommendations emerging from Working Group 8's research. Detail supporting the recommendations below can be found in the remainder of this section 5.

- While there are no obvious dysfunctions in the current operations and provision of priority service, policy-makers and suppliers should continue to seek opportunities to prepare for increased volume and scale – particularly as relates to automated ordering / provisioning and measures to addressed increased likelihood of unauthorized access.

- Policy-makers should consider the impact of recommendations which limit the number of users that qualify for priority services, or which create provisions for reducing priority access of certain users under heavy congestion.

- Policy-makers should reaffirm existing guidance with respect to user classifications (e.g. FCC R&O 00-242), and clear guidelines should be given as to priority assigned to different roles in the face of limited capacity and events that invoke a high density of priority users. Similarly, policy-makers should provide clarification going forward related to pre-emption of communications for non-priority and lower-priority users (on a per application basis), in an over constrained environment. Relative classification of 911 and priority communications in light of technical capabilities (i.e. LTE) should continue to be assessed.

- Policy-makers and suppliers should continue working with application providers, social media, and content providers relative to priority access to critical information

- As evolution of non-domestic priority services increases, policy-makers should seek opportunities to support commonality in priority assignment and QoS for communications which cross national borders.

- The priority service user community (e.g. national security, emergency preparedness, emergency responder communities) should seek to work closely with the networking industry to create and refine the set of application classes that may be needed for priority services treatment, including consideration given to IoT devices.

For the remainder of this section:

- User aspects will be covered in Section 5.2.
- Application aspects will be covered in Section 5.3.
- Finally, network and technology aspects of priority services are covered in Section 5.4.

5.2 User Framework

The need of priority users to authenticate and authorize their roles for access to one or more priority services are managed in a layer we'll call the "User Context". This layer exists to establish associated priorities for access to services over dedicated and/or shared

communications networks. Communications networks are, to varying degrees, constrained (technically (i.e., laws of physics), operationally, and geographically) to supporting a limited number of users at their planned busiest times. As an ever-increasing number of users seeks to use a network simultaneously, network capacity is ultimately exceeded and performance will degrade.

Communications networks can perform similarly to the streets and highways in many of nation's larger cities (which slow during high-volume traffic commute times) where users can similarly experience slow or blocked sessions when too many users can exceed a network's planned capacity or when equipment failures cause localized or route stoppages. During natural or man-made disasters (9/11, Hurricane Katrina and 2013 Boston Marathon bombing), communications service providers' networks performance, throughput and/or connectivity was degraded in those areas as the number of users wanting to contact family, friends or acquaintances exceeded their networks capacities.

Just as there are methods (using the example above) to provide priority for authorized users (i.e., HOV lanes for 2+ occupant or emergency vehicles, re-routing traffic off, and/or preventing traffic from getting on, etc.) during times of congestion, communications service providers could engineer and implement priority services mechanisms in their national networks.

For the last three decades, Federal-sponsored priority services development in the major US communications service providers' networks has created a proven and tested wireline and wireless priority service national network in GETS and WPS under the National Security / Emergency Preparedness (NS/EP) program. In NS/EP's establishment, the Federal government also created a framework for user authentication and authorization guidance for role-based priority and precedence for scarce communications resources in public networks during emergencies. In effect, a "user context layer" was created to accommodate any user at any level of government or industry to perform those essential roles in serving the public and vital to the smooth functioning of society.

This Federal "User Context Layer" for priority services is codified in regulation, but is being buffeted by three events: 1) Congressional legislation authorizing a second nationwide priority service (FirstNet) to provide state and local jurisdictions and emergency responders (police, fire, EMT) with emergency communications to replace their LMR systems. 2) The staggering transformation of people's use of technology worldwide in the last 10 years (since the introduction of the smartphone); 3) and demographic-driven user preferences to embrace newer, IP-based communications tools.

With astronomical volume growth in packet-based network traffic[1], US per capita market saturation of smartphones and the emergence of Internet of Things (IoT) sensors since 2007, all users at all levels of government (Federal, state, local, tribal), industry and consumers have become accustomed to rapid technological innovation, instant communications, and immediate access to web-based data repositories. As such, the majority of users look for applications and internet services to be intuitive, easy-to-use, and to allow them to communicate in ways (i.e., voice, messaging, video, applications) that they are accustomed to.

[1] AT&T network traffic growth of 150,000% (2007-2015)

In this changing environment, the challenges of emerging and possibly discordant "User Contexts" as defined by various jurisdictional (Federal, state, local, tribal) legal and regulatory guidance could delay the deployment of an interoperable and cost-effective next generation priority service that is usable by citizens with responsibilities for continuity of critical industry up to the nation's most senior leaders.

Any next generation priority services framework must address the needs of any priority user with an authorized role and associated level of priority, that originates or terminates using one or more communication applications over a variety of network contexts where one or more of these networks is experiencing significant congestion.

5.2.1 User Roles and Priority

We can expect going forward that definition of a priority user will include multiple criteria based on jurisdictional responsibilities. A user will be designated as a priority user with a specific role and an associated priority level, depending upon:

- Mission of the user (i.e. Continuity of Government, Continuity of Operations, etc.) to restore services and protect the public as determined by jurisdictional scope and responsibilities
- Which governmental agency establishes and authorizes a user as a priority user
- What role (i.e., prescribed function) is to be performed by the actor in relation to an event triggering the need for priority services.

Additional aspects of user management include dependencies on geography (the level of functional distribution), along with any back office support required in the management of authentication, authorization of roles and priority.

In the context of any given event, the priority access granted to a particular user may need to change dynamically. In particular:

- As the applicable emergency event unfolds, the role assigned to a user may change dynamically. For example, users that have been involuntarily confined in the emergency area (e.g. they are trapped or are being held hostage), could be dynamically assigned a role with a priority higher than they might otherwise receive. In this specific case, SMS and/or voice priority could be useful to help ensure effective communication with the confined party.
- As the event unfolds, the importance and as such the relative priority of an assigned role may need to change dynamically (i.e. personnel first-on-the-scene vs. those in command and control later in the event).

Currently, roles and priority levels are not defined for non-human or proxies for humans needing priority (i.e., IoT devices).

5.2.1.1 Federal Level

Different jurisdictions (Federal, state, local, tribal), organizational (police, fire, EMT, etc.), critical infrastructure industries (communications, transportation, banking, water, energy, etc.) and user hierarchies are defined by FCC R&O 00-242 and other applicable regulatory guidance. From government agencies charged with national security operations to first responders (i.e., local fire, police and paramedic personnel), to critical industry (i.e., energy, water, communications, healthcare, banking, etc.) staff providing needed services, their need for access to priority communications services to cut through emergency-induced congestion in the public network is vital to allow them to respond to crises in accordance with the National Response Framework at multiple operational levels.

NS/EP users are comprised of

- 1. Executive Leadership and Policy Makers
- 2. Disaster Response / Military Command and Control
- 3. Public Health, Safety and Law Enforcement Command
- 4. Public Services / Utilities and Public Welfare
- 5. Disaster Recovery.

For these users currently relying on public networks for priority communications, preemption of non-priority traffic is not present until and unless DHS, FCC, and White House agree it may be used in the public networks.

5.2.1.2 State, Local, Tribal, and Emergency Responder Levels

Users currently expect priority service to function effectively, but with precedence according to the hierarchy of their organization (i.e., a Police Chief would receive higher priority than a patrol officer). Local Control of network assets, operations, maintenance, and user administration will be a requirement in the future

It is similarly expected that roles and priority in one jurisdiction may not be applicable in an adjacent one (state, county, city, town, etc.), suggesting the need for a rationalization or user classifications across jurisdictions in the future.

5.2.1.3 Critical Infrastructure Industry Level

Similar to government personnel, priority users from critical infrastructure expect the priority service to function but with precedence according to the hierarchy of their organization (i.e., CEO is higher than incident staff performing service restoration).

When using GETS and WPS, critical infrastructure personnel are currently governed by the Federal "User Context".

5.2.1.4 General Public

Users in the general public will expect E911 and NG911 services to communicate with PSAPs for emergency responders. It is currently unknown if general public will be subjected to pre-emption by successively higher levels of priority users in the context of a crisis event; policy-makers should consider the implications of carving out allowances for pre-emption or service

degradation on a per-application basis.

5.2.1.5 Autonomous or Proxied Devices

An actor, in the context of this document, is a user or function (e.g., network or application) that plays a role in the usage or delivery of a priority service. Currently roles and priority levels are not defined for non-human or proxies for humans needing priority (i.e., IoT devices); this should be done for both terminating and originating scenarios.

5.2.2 Current User Experience

5.2.2.1 User Knowledge

Priority Services users, supported by the Office of Emergency Communications, are aware that a limited set of communications service providers offer GETS and WPS. Individuals are authenticated and authorized by their organization as employees, and their information is forwarded to Federal-level agency coordinators who validate requests. These are forwarded to DHS/OEC and its contractors who issue WPS provisioning instructions to carriers and/or issue GETS calling card.

During the Eagle Horizon exercise in May 2016, over 97% WPS attempts were successful, along with over 99% of GETS attempts. As of this writing, investigation was still ongoing as to the source of the issues that were encountered. In any event, on-going testing and training for users will continue to be required under an updated framework, supported by OEC, the FCC, and the user community itself.

Users are also aware that the FirstNet deployment will create additional options for priority users; the FirstNet RFP award is scheduled for 1Q'17.

Prior analysis suggests that some users are not sufficiently trained and familiar with the current Federal NS/EP service and the associated keypad sequence to initiate calls. During an event, this could itself result in a number of incomplete or failed priority calls, regardless of platform and network availability, arguing for a continued focus on user outreach and education.

5.2.2.2 User Expectations

Users of priority services increasingly expect parity with commercially-available innovations in smartphone-based application interfaces, but must learn dialing sequences of up to 37 digits to make a priority phone call using NS/EP. The Office of Emergency Communications is in the process of launching a dialer application for a subset of smartphone operating systems.

Users expect the priority service to work irrespective of congestion by public. In addition to person-to-person communications using voice, messaging, or video, future priority users may also need to access, with priority, information provided by general Internet servers and social media sites.

Users expect priority communications to function on any User Equipment, including traditional- and smart-phones, tablets, laptops, and desktops. Applications covered under priority services should function regardless of operating system (Android, iOS, other), use commonly available

contact list features, and be capable of traversing multiple applications (phone, video) seamlessly and intuitively, requiring little to no training.

Within a particular priority services communication (voice / data / video), events could trigger updates to prioritization on a user-by-user level. Even within a distinct role, an assigned priority on the network may be changed based on use of an application. For example, a specific role might be defined that provides high priority voice and/or SMS service but not high priority internet access.

For all users and jurisdictions, authenticating to the service, session initiation, and application / update of priority must be intuitive and user-friendly, and require a minimum of training and education.

Currently, the only non-domestic requirement for priority services is the ability to make GETS calls to and from overseas. Priority service begins on an overseas GETS call when the call arrives at a U.S. trunk. WPS is not available overseas.

5.3 Application Framework

Previous priority services have focused on priority voice telephony. As we move into a world that is "content enabled" (which today heavily leverages the use of IP data packets), the set of priority services should expand to include a broader class of content oriented communications. We specifically include as "in scope for priority services" applications that utilize:

- **Hyper Real-Time** services such as Mission Critical Push-To-Talk (PTT) where both signaling and mission critical data require both low latency and low packet loss rates.
- **Conversational services** including voice and video telephony. Conversational services generally require the preservation of the time relation (variation) between information entities of the stream to the extent that allows both parties to naturally converse. Many conversational services can function quite sufficiently at relatively high packet loss rates (e.g. ~1% packet loss). This allows systems to trade off packet loss for lower latency.
- **Streaming services** which must also preserve the time relation between informational entities but with much greater tolerance for delay variation. Streaming services include video services where the user is observing a video clip of some length. Since buffering of the streamed data is typical, the delay variation can be much larger than for conversational services. However, streaming services tend to require much higher bandwidth and much lower packet loss rates in comparison to voice based conversational services.
- **Interactive services** require some level of non-real time interaction. Web based browsing is an example of an interactive service.
- **Background Services** which may include email and other "Store and Forward" services. Most background services do not require priority treatment. Selected store and forward services such as SMS are in scope for priority consideration given the existence of reasonable use cases utilizing SMS communication during priority services events. However, when some level of non-real time interaction is necessary, we may classify these services as Interactive services.

Alternatively, application classes can also be categorized by their separate network environments. For example, one might separate carrier grade managed voice/SMS services (being served by a dedicated network architecture), from Internet centric services.

From a priority services framework perspective, the primary interest is to define classes of applications where the applications within a class all have similar QoS attribute requirements. An example of an application could be viewing a video (at a specific resolution and format size). It is then possible to specify that a priority user should or should not have access to a specific class of applications with priority. The carrying network can then utilize the appropriate low level QoS framework to achieve the desired application behavior for a priority user.

To that end, we recommend that priority service user community (e.g. national security, emergency preparedness, emergency responder communities) work closely with the networking industry to create the set of application classes that may be needed for future priority services treatment.

5.3.1 The Internet of Things (IoT) and Priority Services

The Internet of Things (IoT) can be defined in many different ways and it encompasses many aspects of life—from connected homes and cities to connected cars and roads to devices that track an individual's behavior. In essence, the IoT involves the interconnection of devices and sensors to the global Internet and to IP-based networks of all kinds, all tasked with reporting useful information or performing automated tasks related to this information. The IoT will involve the eventual interconnection of billions of devices performing tasks that range from controlling "smart" homes, appliances and vehicles, to automatic monitoring of buildings, transportation systems and city environments.

The IoT has created already significant new opportunities for business and consumers which in turn has dramatically increased the volume of traffic transported over service providers' networks. In contrast, the IoT has also demonstrated its ability to overwhelm portions of the Internet and interrupt the traffic generated by people when billions of unsecure devices are hacked in cybersecurity exploits (i.e., 10/21/16 DDoS on DNS attack on Dyn).[2] As the IoT comes to predominate network traffic and grows in importance globally, the risks to priority communications services will increase if strong security measures for these devices are not put in place.

Governments, businesses and consumers are rapidly adopting some of the IoT's vast breadth of sensors and automated devices to complement their activities. For those key organizations and individuals with continuity of government (COG), continuity of operations (COOP), and public safety responsibilities, their adoption of the IoT will drive the need for priority services to expand beyond traditional voice to prioritize voice, video and/or data traffic.

This represents a paradigm shift in the way priority services have been supported in the nation's communications networks and the Working Group believes now is the time for standards bodies, platform and service providers, and Federal regulatory agencies to start addressing how the lack of security in, and the expanded use of the IoT will impact priority services.

5.3.1.1 The IoT's Scope

New approaches need to be considered to address the impact on priority services by IoT's security challenges and its rapid growth. These approaches must be adopted into existing policy, legal and technology frameworks that currently govern the provisioning of priority services.

As the Internet Society said in its report ***The Internet of Things: an Overview***:

> *"The Internet of Things is an emerging topic of technical, social, and economic significance. Consumer products, durable goods, cars and trucks, industrial and utility components, sensors, and other everyday objects are being combined with Internet connectivity and powerful data analytic capabilities that promise to transform the way we work, live, and play. Projections for the impact of IoT on*

[2] https://krebsonsecurity.com/2016/10/ddos-on-dyn-impacts-twitter-spotify-reddit/

> *the Internet and economy are impressive, with some anticipating as many as 100 billion connected IoT devices and a global economic impact of more than $11 trillion by 2025.*
>
> *At the same time, however, the Internet of Things raises significant challenges that could stand in the way of realizing its potential benefits. Attention-grabbing headlines about the hacking of Internet-connected devices, surveillance concerns, and privacy fears already have captured public attention. Technical challenges remain and new policy, legal and development challenges are emerging."*[3]

What this quote highlights about the IoT's scope and impact on society and the nation's communications networks also applies to key government and critical infrastructure leaders and staff's abilities to use priority services during cyber exploits as well as during emergencies.

A number of companies and research organizations have offered a wide range of projections about the potential impact of the IoT on the Internet and global economy during the next five to ten years. Cisco Systems projects more than 24 billion Internet–connected objects by 2019; Morgan Stanley, however, projects 75 billion networked devices by 2020. Looking even out further and raising the stakes higher, Huawei Technologies forecasts 100 billion IoT connections by 2025. McKinsey Global Institute suggests that the financial impact of the IoT on the global economy may be as much as $3.9 to $11.1 trillion by 2025. While the variability in predictions makes any specific number questionable, collectively they paint a picture of significant growth and influence.[4]

From a broad perspective, the confluence of several technology and market trends is making it possible to interconnect more and smaller devices cheaply and easily:

- *Ubiquitous Connectivity*—Low–cost, high–speed, pervasive network connectivity, especially through licensed and unlicensed wireless services and technology, makes almost everything "connectable''
- *Widespread adoption of IP–based networking*— IP has become the dominant global standard for networking, providing a well–defined and widely implemented platform of software and tools that can be incorporated into a broad range of devices easily and inexpensively
- *Computing Economics*— Driven by industry investment in research, development, and manufacturing, Moore's law continues to deliver greater computing power at lower price points and lower power consumption
- *Miniaturization*— Manufacturing advances allow cutting-edge computing and communications technology to be incorporated into very small objects. Coupled with greater computing economics, this has fueled the advancement of small and inexpensive sensor devices, which drive many IoT applications.

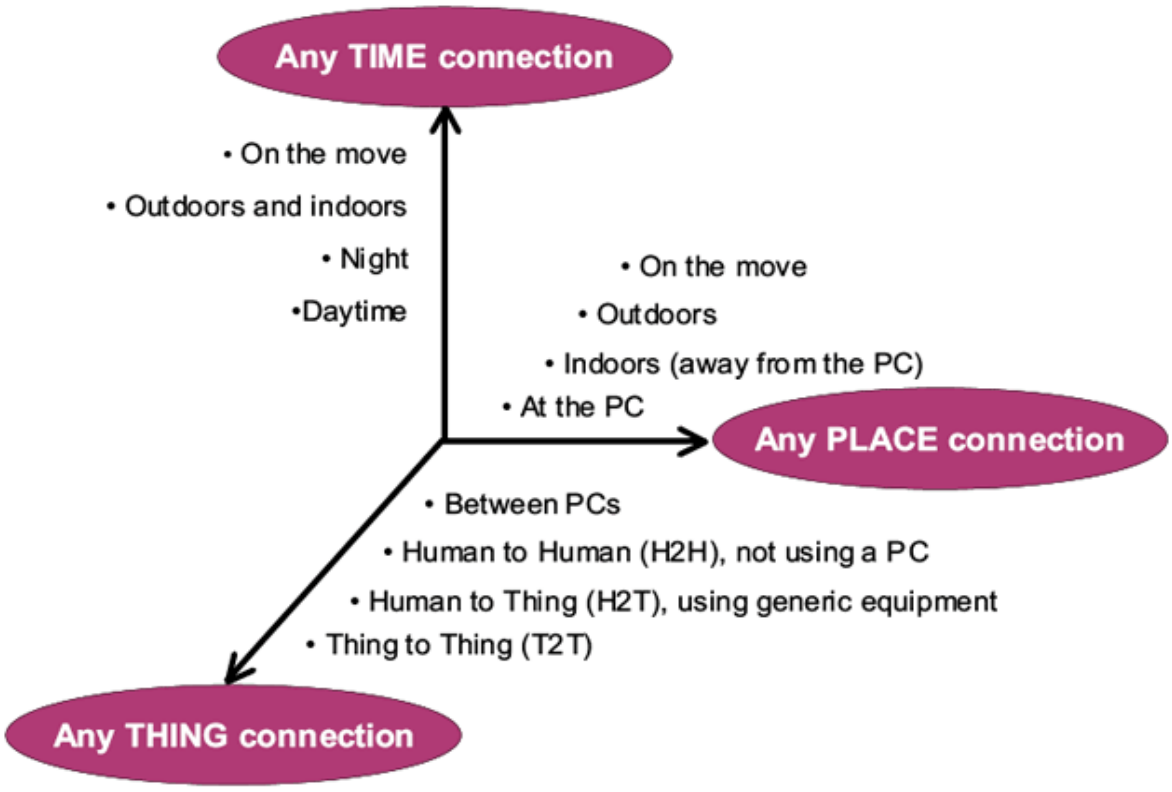
[3] *The Internet of Things: an Overview*, *The Internet Society*, November 2015, p. 1
[4] Ibid, p. 4

- *Advances in Data Analytics*— New algorithms and rapid increases in computing power, data storage, and cloud services enable the aggregation, correlation, and analysis of vast quantities of data; these large and dynamic datasets provide new opportunities for extracting information and knowledge.
- *Rise of Cloud Computing*– Cloud computing, which leverages remote, networked computing resources to process, manage, and store data, allows small and distributed devices to interact with powerful back-end analytic and control capabilities.[5]

5.3.1.2 The IoT's Growth and Telecommunications Considerations

The IoT's significant growth and potential disruptiveness of priority services is greatly increased as network service providers' communications infrastructures are migrated from TDM to IP.

Figure 1 below illustrates how the IoT offers technology users the ability to expand their organizational and individual activities away from traditional fixed locations (i.e., offices, homes) to a mobile anyplace, anytime environment. With the IoT's increasingly vast breadth of sensors and automated devices to complement any Federal, state, local, and tribal governments, businesses and consumers activities, the adoption of the IoT will drive the needs for greater security to protect service providers' networks for routine and priority voice, video and/or data traffic.



Source: ITU adapted from Nomura Research Institute

[5] This paragraph taken from *The Internet of Things: an Overview*, The Internet Society, November 2015, p. 8

Figure 1: Future Networks

Platform (i.e., major internet technology companies, etc.) and service providers (i.e., telecom, MSO, etc.) are rapidly expanding their commercial offerings to businesses and consumers using the IoT. From the edge devices such as passive sensors and handsets to autonomous devices that connect over licensed and/or unlicensed wireless spectrum to cloud-based computing resources, the IoT leverages the confluence of technology and mobility to perform functions that were previously too costly or impossible to do (i.e., real-time monitoring millions of cargo shipping containers worldwide, turning down the temperature in a home remotely, etc.)

To further grasp the impact the IoT will continue to have, consider Figure 2:

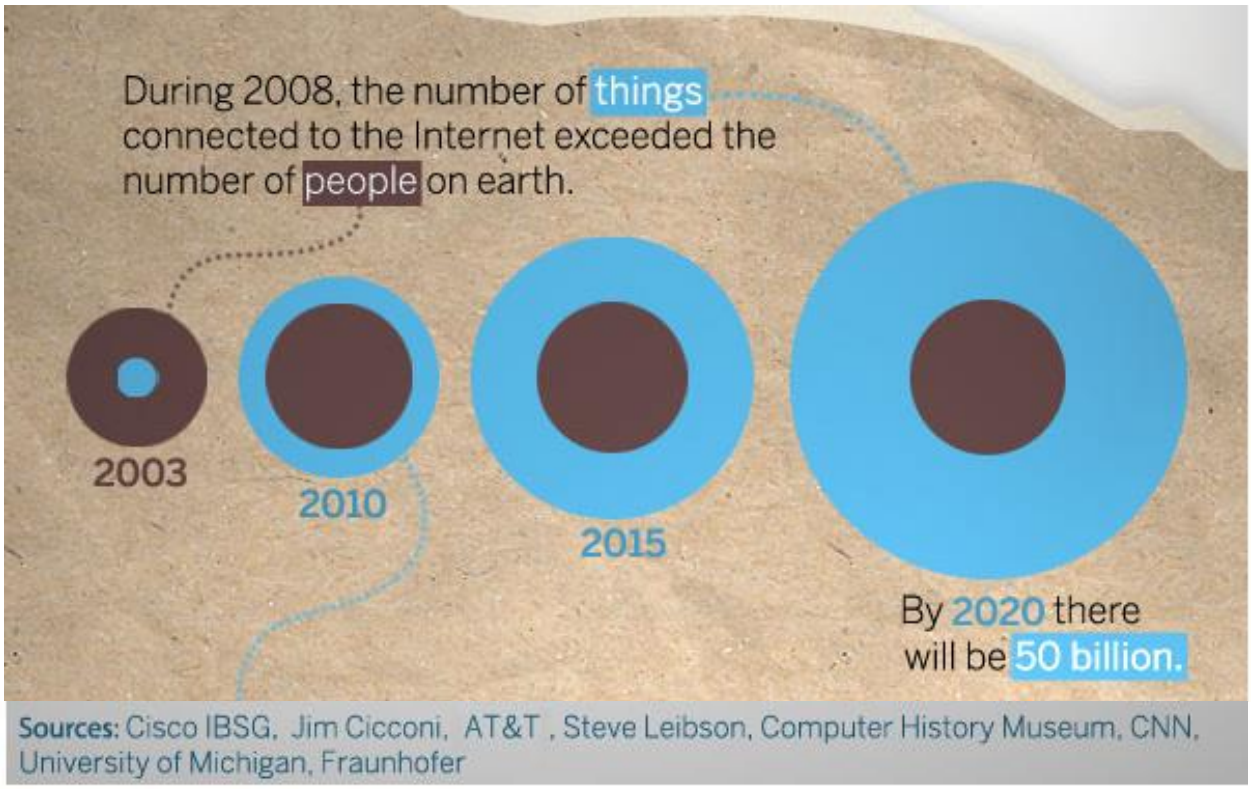


Image Courtesy: : CISCO

Figure 2: Devices Connected to the Internet vs. Global Population

The number of devices connected to the Internet has already far exceeded the global population. As interconnected devices and sensors are likely to continue to complement (and substitute for) users with COOP, COG or emergency services responsibilities (i.e., situational awareness, response and recovery coordination, etc.), to not accommodate access to priority services to the IoT could possibly limit the nation's senior leadership and crisis managers from having access to tools needed effectively managing a crisis.

5.3.1.3 Technological Evolution of the IoT and Industry Perspectives

As IoT devices have continued to become smaller, more capable and numerous, service providers correspondingly have upgraded their networks to support the increased traffic over their wireless and wireline infrastructures. Service providers have also worked closely with device manufacturers and platform providers (i.e., Internet technology companies) to characterize IoT devices' connectivity needs (i.e., bandwidth, latency) for their use in that nations' networks.

According to SRI, the evolution IoT technology illustrates how increasingly capable IoT devices have become. From RFID tags (past), to remote tele-operation and tele-presence (present) to capabilities by devices to interact in an "autonomous" fashion because of their connectivity to people or software agents.

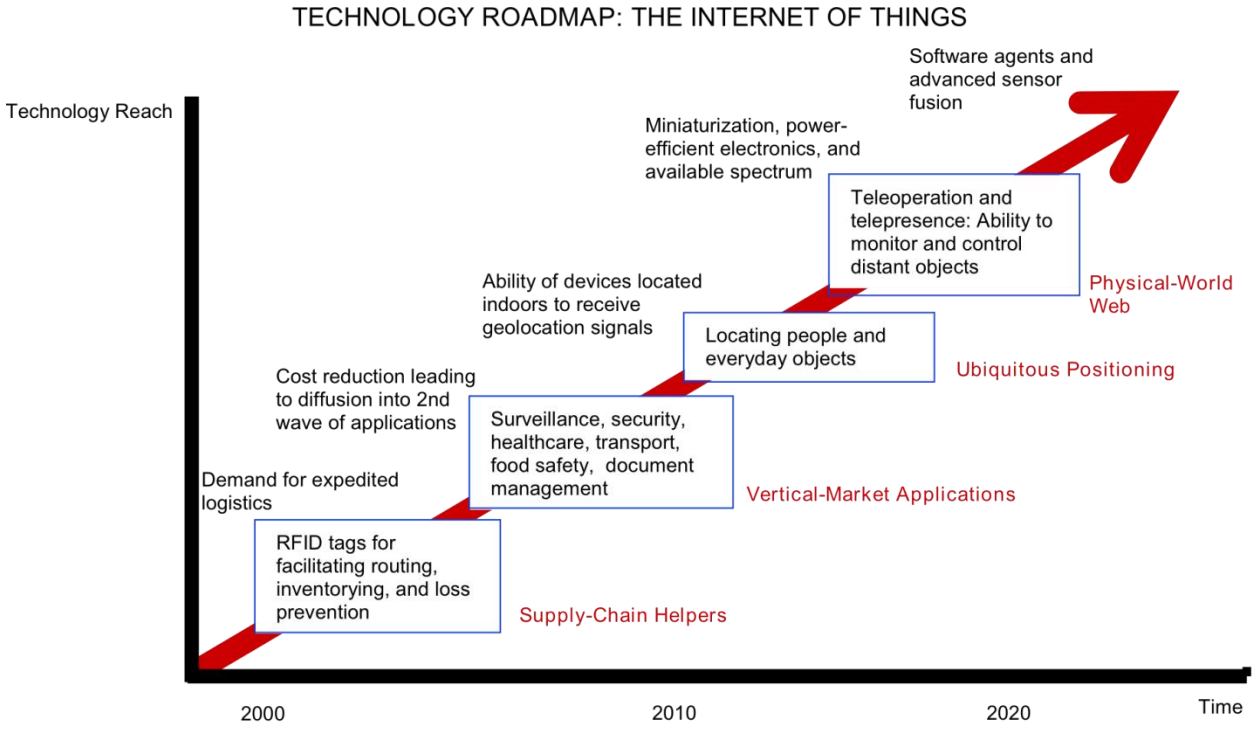


Figure 3: IoT Technology Trends

As further evidence of the impact of IoT technologies, McKinsey Global Institute in their report "Unlocking the Potential of the Internet of Things'' describes the broad range of potential applications in terms of environmental "settings" where IoT is expected to create value for industry and users as shown in Figure 4 below.

"Settings" for IoT Applications (Source: McKinsey Global Institute[26])		
Setting	**Description**	**Examples**
Human	Devices attached or inside the human body	Devices (wearables and ingestibles) to monitor and maintain human health and wellness; disease management, increased fitness, higher productivity
Home	Buildings where people live	Home controllers and security systems
Retail Environments	Spaces where consumers engage in commerce	Stores, banks, restaurants, arenas – anywhere consumers consider and buy; self-checkout, in-store offers, inventory optimization
Offices	Spaces where knowledge workers work	Energy management and security in office buildings; improved productivity, including for mobile employees
Factories	Standardized production environments	Places with repetitive work routines, including hospitals and farms; operating efficiencies, optimizing equipment use and inventory
Worksites	Custom production environments	Mining, oil and gas, construction; operating efficiencies, predictive maintenance, health and safety
Vehicles	Systems inside moving vehicles	Vehicles including cars, trucks, ships, aircraft, and trains; condition-based maintenance, usage-based design, pre-sales analytics
Cities	Urban environments	Public spaces and infrastructure in urban settings; adaptive traffic control, smart meters, environmental monitoring, resource management
Outside	Between urban environments (and outside other settings)	Outside uses include railroad tracks, autonomous vehicles (outside urban locations), and flight navigation; real-time routing, connected navigation, shipment tracking

Figure 4: "Settings" for IoT Applications[6]

This broad array of environmental settings where IoT devices are used (i.e., offices, homes, public spaces, etc.) will continue to expand as people explore and adopt new more effective methods to perform their missions, tasks, and activities.

As shown in Figures 3 and 4 above, the evolutionary trend of IoT and its projected uses will drive a continuing need for additional bandwidth to accommodate the growth in traffic. As service providers have been in the center of this growth and network traffic has increased in some cases as much as 100,000% since 2007, the following perspectives may be useful in characterizing today's operating communications environment moving forward:

1. Network use and traffic types will continue to become increasingly heterogeneous (i.e., continued increase in the number of IoT devices and services will drive more network

[6] *The Internet of Things: an Overview*, The Internet Society, November 2015, p. 9

connections with diverse traffic profiles and performance requirements. User equipment and IoT device examples are offered for comparison and would likely be handled similarly in service providers' networks:

- Handset Uses:
  - Low bandwidth / low latency (i.e., Push-To-Talk / Real-Time-Text)
  - Low bandwidth / high latency (i.e., General web browsing)
  - High bandwidth / low latency (i.e., Video (streaming and real time communications)
  - High bandwidth / high latency (i.e., Application downloads and updates)

- IoT Uses:
  - Low bandwidth / low latency (i.e., Critical medical or infrastructure asset reporting (e.g., Smart Grid solutions), and some public safety IoT device reporting (e.g., Shot Spotter))
  - Low bandwidth / high latency (i.e., Non-critical uses like routine IoT device telemetry reporting)
  - High bandwidth / low latency (i.e., Remote video camera streaming in security solutions)
  - High bandwidth / high latency (i.e., Firmware Over-The-Air (FOTA) updates for connected cars/other assets)

2. The variety of use cases and users presented by IoT devices and services means that in developing prioritization schemas, operators would evaluate and implement prioritization techniques on a use case-by-use case basis, in the context of their overall network operations, and not on a strictly categorical basis (not, e.g. "all devices of X type receive Y forms of prioritization).

3. Video (streaming and real time communications) will continue to increase in volume to represent a preponderance of traffic in service providers' networks profiles.

4. The IoT is so expansive that existing standards and standards in development may not cover all emerging uses resulting in responsive actions versus planned

5. As the IoT comes to predominate network traffic and grows in importance globally, the risks are increasing to our highly reliable priority communications services as strong security measures have not been implemented.

5.3.1.4 Considering Priority Services in an IoT predominant world

The evolution of IoT technology will take it squarely into the operational realm of priority communications services. Government has a key role to play in bringing together standards bodies, platform and service providers, and Federal regulatory agencies to address how the IoT's "…billions of connected devices [are] so lacking in security that they are putting not only individual users at risk, but public and private infrastructure as well, including the infrastructure of the internet itself."[7]

[7] Taylor Armerding, "Can government really fix the IoT mess?", NetworkWorld article, January 7, 2017

To begin to address the IoT's challenges with the needs for priority services by key government, critical industry and public safety organizations and individuals, the Priority Services Working Group offers the following observations and recommendations:

1. Security is Imperative
    a. Challenge: The risk to communications (routine and priority) is of being overwhelmed by illegitimate traffic from cyber exploits of devices, not a volumetric uncertainty of the IoT.
    b. Rationale: This section of the WG 8 report. Also see "Strategic Principles for Securing the Internet of Things[8], recently published by DHS.
    c. Recommendation: Federal regulatory agencies with responsibilities for IoT products, services, and communications in conjunction with standards bodies, device manufacturers, platform and service providers could establish an agreed-upon national framework for enforceable security to safeguard the nation's communications infrastructure.

2. Jurisdictional Overlap
    a. Challenge: The overlap of governmental jurisdictions at International, Federal, State, Local, Tribal and Territorial levels with their sometimes overlapping responsibilities and anticipatory guidance can unnecessarily constrain the responsiveness needed by industry to address the geometric growth exhibited in the adoption of IoT devices.
    b. Rationale: Service providers need the maximum flexibility to offer multiple levels of prioritized services for any and all services they desire, in a manner that optimizes the use of their networks for the range of their customers (i.e., government, businesses, and consumers). This flexibility is of course mediated by compliance with the current FCC Open Internet Order restrictions; however, these would not apply to Public safety services and Non-Broadband Internet Access Services.
    c. Potential Response: As Federal agencies responsible for communications and priority services, FCC and DHS could play a significant roles in not only bringing industry together to forge a joint solution, but also set Federal guidance regarding IoT communications within the US.

The Internet of Things represents a significant opportunity for government, businesses and consumers to perform their tasks more efficiently and with greater flexibility in an ever-accelerating world. For key organizations and individuals with continuity of government (COG), continuity of operations (COOP), and public safety responsibilities, their use of IoT will necessitate priority services be extended to IoT to support their growing voice, video and data needs. The FCC and DHS would be key to forging a government-industry partnership to establish an enforceable, standards-based security framework that would greatly reduce incidents of cyber exploits to the IoT and the nation's communication infrastructure.

This would represents a shift in the way priority services have been supported in the nation's

[8] https://www.dhs.gov/securingtheIoT/

communications networks and the Working Group believes we must act now.

5.4 Network Framework

Existing priority services platforms (GETS, WPS, NGN-PS) are currently focused on providing priority voice calling services to support national security and emergency preparedness communications for government officials, emergency responders, critical infrastructure owners and operators, and vital industry members. Moving forward, Phase 2 of the NGN Priority Services Program will address priority data, video and information services capabilities on the service providers' wireline and wireless IP telecommunications networks. Priority data services are anticipated to include services such as email, short message service (SMS), enterprise access, Web access/browsing, and other currently used data services.

Many of these data services utilize the public Internet either completely or partially. According to forecasts[9] of total Internet traffic, more than 14 percent of monthly IP traffic will come from cellular connections by 2019, up from 4 percent in 2014. Additionally, by 2019, the forecast predicts that 53 percent of monthly IP traffic will come from Wi-Fi connections worldwide, up from 42 percent in 2014. The forecast also expects fixed access IP traffic to drop from 54 percent of all IP traffic in 2014 to 33 percent in 2019 as Wi-Fi and cellular traffic increases.

YEAR	Cellular Data	Wi-Fi	Fixed
2014	4%	42%	54%
2019	14%	53%	33%

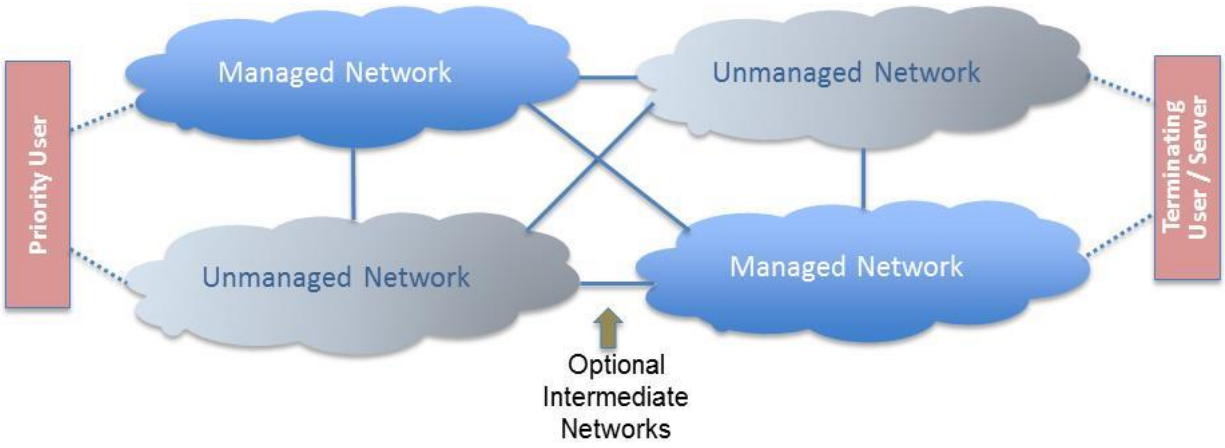
Cellular Data includes 3GPP based technologies such as 3G and 4G/LTE. In support of priority data services, 3GPP has specified a rich set of QoS and priority service mechanisms with the LTE standard. However, data forecasts indicate that the large majority of traffic will not be carried on a cellular data network (In 2014, 96% of all of data traffic was carried over Wi-Fi or fixed networks. This is expected to decrease to 86% by 2019). Most of these Wi-Fi/fixed network Internet data networks have no priority or QoS capabilities as deployed. This situation places significant challenges when considering a next generation priority services framework that provides a rich set of voice, data and video priority services that rely on the Internet data network infrastructure.

The role of the network within the priority services platform is to enforce priority levels on traffic associated with priority users. There are number of factors critical to this enforcement function:

- The priority user must be authenticated and authorized to receive priority treatment
- The network must be able to uniquely identify priority user traffic and associate the authorized level of priority to that traffic
- The network must then have prioritization means to apply to the identified traffic.
- For cases where networks interconnect, traffic prioritization indicators must be securely passed to interconnected networks for downstream prioritization.

[9] Cisco Systems May 27, 2015 news release summarizing the 10th annual Cisco® Visual Networking Index™ (VNI) Forecast (https://newsroom.cisco.com/press-release-content?type=webcontent&articleId=1644203)

It is important to realize that networks may not inherently possess the capabilities noted in the above points. In this document, we will define a "Managed Network" to mean a network that is capable of uniquely identifying priority user traffic, can associate the authorized level of priority to that traffic and has the means to apply the enforcement of prioritization to the identified traffic. Further, we define an "Unmanaged Network" as a network that cannot meet the above requirements.



The figure above illustrates a logical high level architecture for priority services. The Priority User on the left can connect to either (or both) a managed or unmanaged network. These networks may interconnect to one or more managed or unmanaged networks which further connect to the intended terminating user or server.

A priority services framework suitable for packet based networks must consider the fundamental distinction between the treatment of a circuit versus the treatment of a packet. Priority in a historical telephone system context addressed whether a telephone call (which used one channel in each of a succession of channel banks) could gain access to that succession of channels. The bandwidth, latency and error rate were determined by the channel itself which was fundamentally designed to meet real-time telephony needs. As such, priority in historical circuit networks was really an authority to gain access to a fixed and existing set of channels where each channel was more or less guaranteed to deliver a fixed bandwidth with known error, jitter and latency specifications. As such, we conclude that the "intent of priority" in circuit based networks implicitly assumes bandwidth, data error, jitter and latency of a channel so that higher level authorization to use said channel is sufficient to meet the priority user's communication needs.

In mapping these concepts to priority in packet based networks, we observe that priority access to a "channel" must include consideration for managing bandwidth, latency/jitter and packet loss to meet a desired Service Level Agreement (SLA[10]) appropriate for the application being invoked by the priority user. In packet networks, an SLA can be managed through various

[10] An SLA commonly includes a wide variety of terms and conditions relating to the definition of services, service performance, remedies for non-compliance, problem management, warranties, termination of agreement and similar topics. In this document, we mean specifically the aspects of an SLA that address service performance and associated metrics.

means and mechanisms that include:

- Packet priority policies in the schedulers of switches and routers
- Traffic policing or shaping
- Admission control
- Traffic engineering policies and procedures as applied to aggregates of data traffic.

An SLA may be applied to individual sessions / flows or broad aggregates of data. The details of the SLA are variable, and might be specified at the time of session initiation. Metrics of interest can include:

- Maximum bit rate supported
- Guaranteed bit rate (the session may be dropped if this guaranteed bit rate cannot be met or sustained)
- Average latency and jitter
- Packet loss rate averaged over a period of time

Different applications have different SLA needs. For example, the circuit based voice application typically expects approximately 64kb/s (more or less depending on the size of headers and the extent of compression used) of bi-directional guaranteed bandwidth with end-to-end one-way latency in the 150ms range[11]. Due to the natural resiliency of most voice coders, packet loss can be on the order of 1-2% without significant impact on voice quality.[12]

Alternatively, many if not most data applications assume reliable transport of data (no packet loss at the application layer). To implement this, TCP/IP is used to request retransmission of data that is lost or received in error. Retransmission, particularly on lossy links, can greatly increase effective latency while lowering overall effective throughput of the session. Additionally, video and other advanced data applications may require bandwidths in the 5-25Mb/s range.[13] Thus, these applications tend to be characterized by a need for broadband speeds with very low packet loss rates. Since streaming video is naturally buffered for playback, latency is much less of a concern.

It should be noted that it is quite possible for a packet based network to apply priority on a specific packet flow without knowledge of the SLA that may be needed for that flow. However, in those cases, the packet network can only guarantee that the priority flow receives "better" performance (as measured by bandwidth/throughput, packet loss and latency) than other packet flows sharing the transport resource, not that the application associated with this packet flow performs as needed. Indeed, in the context of a priority services framework, the goal is provide a priority user with sufficient network connectivity to enable a quality of experience consistent with the priority user's needs. The application SLA is the mechanism needed to accomplish this end goal.

[11] ITU-T (05/2003). "ITU-T Recommendation G.114, One-way transmission time". Retrieved 2016-04-05.
[12] ITU-T (11/2007). "ITU-T Recommendation G.113, Transmission impairments due to speech processing". Retrieved 2016-04-05.
[13] In the *2015 Broadband Progress Report And Notice Of Inquiry On Immediate Action To Accelerate Deployment* (FCC 15-10), the FCC noted in paragraph 30 that although there is no uniform standard for the bandwidth necessary to receive acceptable quality video, various providers have provided bandwidth recommendations that range from 5mb/s to 25mb/s.

Another key difference between a circuit connection and a packet based session relates to the security of the data being transported. In a circuit world, the network funnels all connection data through the "circuit" established for the connection. Thus the data is explicitly bound to the connection and therefor to the priority user. In packet based networks, the network looks at each packet individually in making packet routing / handling decisions. For each packet, the network must address, either explicitly or implicitly, three fundamental questions:

1. Is the packet associated with a priority user?
2. If so, what is the application specific SLA applicable to this packet flow?
3. What specific QoS policies must I apply to the packet to satisfy the SLA?

Additionally, these questions must be answered based on secure information to protect against spoofing, DDoS and other network oriented attack vectors.

The concepts expressed above can be illustrated through a simple example. Assume a network receives a packet from an untrusted source. This may be another network via a peering point, a connection to a customer location, or over a subscriber line / mobile device tunnel. Let us further assume that this packet is marked (e.g. via a DiffServe Code Point – DSCP) as needing some level of priority. The network edge functions receiving this packet must then assess:

- Is this packet associated with an authenticated priority user?
- Is this user authorized to receive priority handling for this is packet and the associated application?
- What is the SLA applicable to this packet flow and how do I translate a specific DSCP value into specific behaviors in the network to satisfy the SLA? Note that specific network behaviors associated with a DSCP marking are network dependent and as such, the intent expressed by the source network of the packet must be known in order to evaluate how to properly handle this packet.

Generally, an IP packet has little information that can be used to address the above questions. Although the source and destination IP address embedded in the packet can be used for routing purposes, these addresses are generally not a reliable or secure indication of the source or destination user's identity. IP addresses can be masked as a result of NAPT functions and can be spoofed.

Mechanisms to address these questions can include:

- Use of secure encapsulation protocols – the packet in this case is a member of a stream of packets that utilize known secure encapsulation protocols such as IPsec or SSL based VPN technologies that securely bind the data within the packet to an authenticated session. These protocols can be used to ensure the integrity and confidentiality of the packet flow.
- Use of secure link technologies to ensure that the packet source address can be trusted and that the data has been transported from the source node with some integrity. Examples here can include the use of specific "priority service" APNs or dedicated bearers in mobile networks, MPLS LSPs or other dedicated link layer technologies.

Once the network has addressed these questions, it is then possible for the network to apply appropriate network and QoS policies to conform to the stated SLA for the authenticated priority user traffic. Many different mechanisms can be used to distribute and enforce QoS related

policies in support of an SLA including:

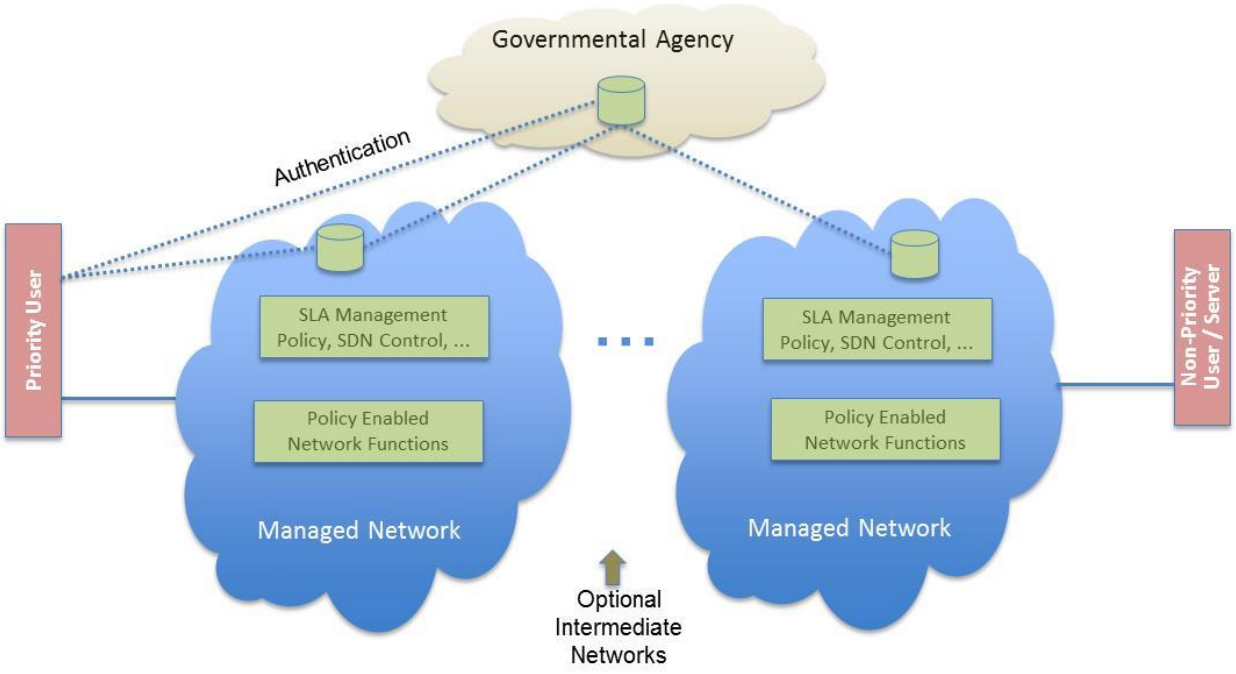
- Use of SDN control principles (e.g. via OpenDaylight) to differentially route traffic to meet SLA needs
- Use of policy based centralized control systems that can distribute QoS policies to various policy enforcement points in the network. For example, the 3GPP Policy and Charging Control system utilizes a PCRF (Policy and Charging Rules Function) to distribute QoS policy parameters in a consistent way from the 3GPP Radio Access Network to the packet data network gateway function located at the edge of the core IP network.

A key requirement implied in this discussion is that the priority user has been authenticated as a priority user. The authentication process involves multiple actors, specifically:

- Since we are specifically referring to governmental priority services, one or more governmental agencies must authorize a specific user (and/or user device) as being eligible for priority services with an associated role and set of application specific SLAs as needed. It is advantageous for governmental priority service authentication/authorization information to be centralized into one centrally managed database to avoid confusion and network complexity.
- Each network will need its own priority services authentication/authorization center to bind governmental priority authentication/authorization to device / subscriber identity and associated authentication/authorization. Additionally, SLA specific parameters and methods may vary from network to network.

These two different authentication domains can be linked in multiple ways. For example:

- Single sign-on techniques can be used to allow a user that has already received network access (typically via some level of network authentication), to first authenticate with a governmental priority services authentication center. This authentication step would then transfer a token to the user which can then be used to authenticate as a priority user in participating networks.
- Participating network authentication centers can interface directly (automatically or via manual intervention) with the centralized governmental authentication center to automatically bind a network device/subscriber authentication as a priority user with a specific role and associated SLA.



The figure above illustrates these basic concepts. Specifically:

- The priority user has been authenticated, directly or indirectly, with network operator and the controlling governmental agency.
- The authenticated user is then authorized to use a specific SLA (or multiple application specific SLAs) which is pushed down into the network appropriately to enable management of the priority user traffic
- The SLA is enforced for priority traffic via standard mechanisms such as SDN control and/or Policy rules controlling the appropriate network functions.

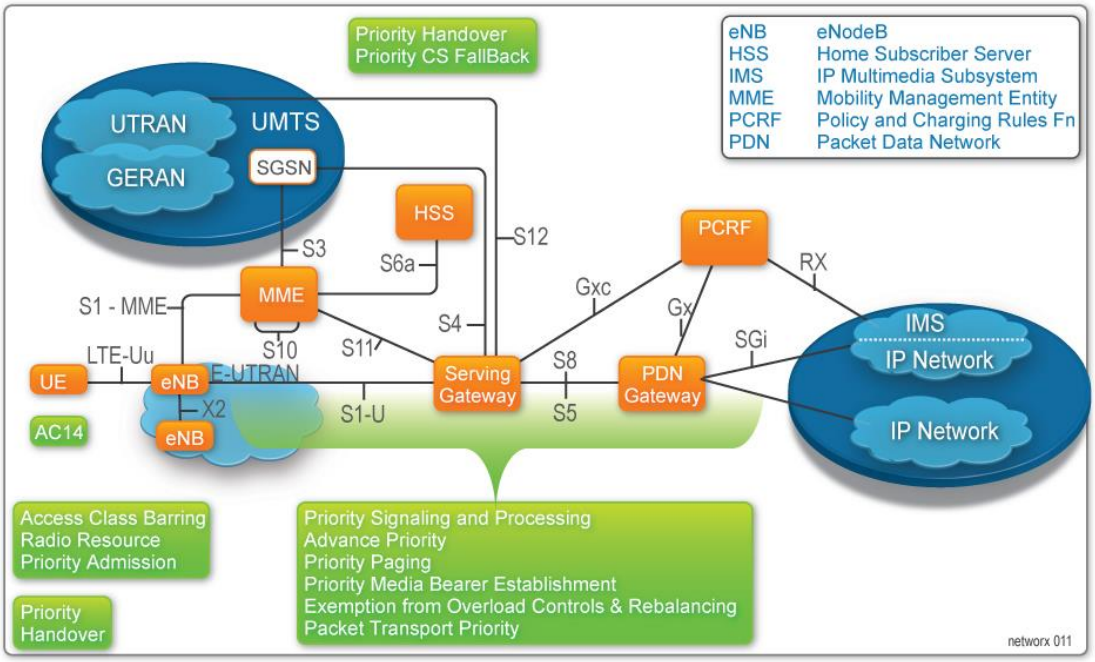
It is important to note that many commercial networks do not currently have the need to enforce application specific SLAs and as such, have not been designed or built to include the necessary capabilities to do so.

5.4.1 Defining common levels of priority, and associated traffic management techniques

The figure below illustrates the areas where enhancements to the ATIS, 3GPP and IETF standards in support of priority services. These include:

- High Priority Access Process, including reserved Access Classes and access thresholding.
- Priority Paging to increase the probability that the calls/sessions call requests are admitted on the network during times of extreme congestion.
- Handover and Circuit Switched Fallback with Priority.
- Priority marking of SIP, Diameter, and H.248 Signaling messages.
- Priority call processing of calls/sessions.

- Priority routing of IP packets.
- Priority media Bearer Establishment.
- Exempting traffic from overload controls (SIP, Diameter, H.248, GTP) and rebalancing.



Access Class - Access Class Barring and High Priority Access: A UE with subscription to NS/EP is entitled to exclusive use of AC 14 [ATIS AC14], and is therefore entitled to the benefits during the Access Class Barring procedure [TS 36.331], and to benefits associated with usage of the highPriorityAccess value [TS 36.331, 36.413] of the Establishment Cause IE.

- Access Class Barring provides NS/EP subscribed UEs priority to initiate the RRC Connection Establishment procedure [LTE GIR]. This preferential treatment is a property of subscription and does not apply to a UE that is not a member of Access Classes 11 through 15 inclusive.

  The use case assumes that the RRC Connection is already established. Therefore, Access Class Barring does not provide a solution.

- High Priority Access: The NS/EP benefits of the highPriorityAccess value of the Establishment Cause IE were studied in detail [NS/EP HPA]. Nine benefits were identified:

  1. eNodeB: priority allocation of SRB1 resources,
  2. eNodeB: overload control exemptions in the E-UTRAN,
  3. MME: handling of the "Initial UE message" at the MME,
  4. MME: priority markings and treatments in S6a signaling to the HSS,
  5. MME: exemptions to APN-based SM congestion control,

6. MME: exemptions to subscribed-APN-based MM congestion control,
7. MME: exemptions to general MM congestion control,
8. MME: exemptions from rebalancing, and
9. PDN-GW: exemptions to overload controls.

The use case was evaluated to ensure that none of the nine above listed items could be employed to distinguish the two types of callers. Therefore, highPriorityAccess cannot be considered as a solution.

- Advance Priority at the Time of Attach - Advance Priority is a means to get priority for the transmission of the initial SIP INVITE for a call/session. Two forms of Advance Priority are specified in this standard: Advance Priority-SPR and Advance Priority-HSS. The implementation of one form of Advance Priority precludes the other; which form is implemented will depend on Service Provider preference and network impacts. As a consequence, all requirements that follow in this section on Advance Priority are conditional on the form of Advance Priority selected.
    - Advance Priority-SPR - Subscription to Advance Priority-SPR is determined based on setting of the "IMS Signaling Priority" information in the SPR. When Advance Priority-SPR is enabled to a particular APN, NGN GETS treatment for the IMS Signaling Bearer is enabled at the time of Attach to that APN, and it remains enabled independent of the status of any ongoing SIP call/sessions. In the case of an EPC with a GTP-based S5/S8 Interface the above requirement affects the transmission of the "CC-Request" command from the PDN-GW to the PCRF at the time of Attach. For a PMIP-based S5/S8 Interface, the requirement instead applies to the transmission of the "CC-Request" command from the S-GW to the PCRF at the time of Attach. If a network supports Advance Priority-SPR:
        - "IMS Signaling Priority" information shall be included in the SPR for each Service User with subscription to the service for each APN that supports IMS Signaling to indicate whether Advance Priority-SPR is enabled for a particular APN.
        - the "IMS Signaling Priority" information shall be marked as either set or not set for all APNs that support IMS Signaling in the subscription profile of a Service User, and shall be delivered to the PCRF at the time of Attach (PDN Connection Establishment).
        - , NGN GETS priority treatment for the Default Bearer and for the IMS Signaling Bearer associated with a particular APN shall be enabled at the time of Attach (PDN Connection Establishment) when the "IMS Signaling Priority" information for that APN is set.
    - Advance Priority-HSS - Advance Priority-HSS is a means to get priority for the transmission of the initial SIP INVITE for a call/session. If a network supports Advance Priority-HSS:
        - the HSS shall provision the Default Bearer for each APN used for NGN GETS to contain the highest Priority Level (the lowest numeric value) among the set of ARP values reserved by the Service Provider for use by NGN GETS and to contain a Pre-emption Vulnerability set to the "not-pre-emptable" value.

- the HSS shall provide the NGN GETS ARP to the MME at the time of Attach using the "Update-Location-Answer" command.
- NGN GETS priority treatment for the IMS Signaling Bearer shall be enabled at the time of Attach (PDN Connection Establishment).

QoS Parameters for the EPS: In LTE, QoS is specified at the level of the EPS Bearer, and as defined in Section 4.7 of [TS 23.401], uniquely identifies an SDF aggregate between a UE and a PDN gateway, and can be found in Appendix A. EPS bearer QoS is specified in Section 4.7.3 of [TS 23.401] by five (5) parameters:

- Allocation and Retention Priority (ARP): The ARP provides an indication of the priority to be applied in three situations:

  1. *In the allocation (establishment or modification) of an EPS bearer:* When the system cannot fulfill all requests, higher priority requests are accepted while lower priority requests are rejected.
  2. *In "exceptional" cases when an EPS bearer needs to be dropped:* When handover occurs and the target cell cannot support all the EPS bearers previously supported by the source cell, the priority indicates which ones should be supported and which should be dropped.
  3. *In the preemption of an EPS bearer:* When a new bearer (either an initial allocation or handover), marked as capable of preempting, is established by preempting an existing bearer marked vulnerable to preemption, only a bearer with a lower priority level may be chosen.

  Once successfully established, a bearer's ARP does not impact packet forwarding treatment. As per TS 23.401, "Once successfully established, a bearer's ARP shall not have any impact on the bearer level packet forwarding treatment (e.g. scheduling and rate control). Such packet forwarding treatment should be solely determined by the other EPS bearer QoS parameters: QCI, GBR and MBR, and by the AMBR parameters."

  As the use case presented assumes the bearer is already established, and it is assumed that preemption of other bearers is not allowed by policy, the ARP cannot be used to address the problem.

- QoS Class Identifier (QCI): QCI provides an index into a set of parameters controlling packet forwarding treatment. It is the only parameter that indicates priority for packet forwarding treatment and is the focus of the use case.

  QCI characteristics include priority level, Packet Delay Budget (PDB), and Packet Error Loss Rate (PELR). The PELR for both NS/EP and MCPTT QCIs is the same for the use case. The use case specifically explores the PDB and priority level of the QCI.

  Two types, formally called resource types, of bearers are defined: GBR and non-GBR. They differ in the way QoS is specified in terms of the remaining QoS parameters below. GBR bearers have a GBR and MBR, and do not have an AMBR. Non-GBR bearers have an AMBR, and do not have either a GBR or MBR.

  - Guaranteed Bit Rate (GBR): The bitrate required to be allocated at the time of admission, specified separately for the upstream and downstream directions. The

concept of bitrate is orthogonal to priority. Thus specific bitrate requirements are not presented in the use case.

- Maximum Bit Rate (MBR): The maximum bitrate the scheduler may allocate to the bearer, specified separately for the upstream and downstream directions. The concept of bitrate is orthogonal to priority. Thus specific bitrate requirements are not presented in the use case.
- Aggregate Maximum Bit Rate (AMBR): There are two versions of this parameter. The APN-AMBR limits the total bit rate on all non-GBR bearers to a particular APN, and is specified for each PDN to which the UE has subscription. The UE-AMBR limits the total bit rate on all non-GBR bearers on all PDN connections. Both APN-AMBR and UE-AMBR are specified separately for the uplink and downlink directions. The concept of bitrate is orthogonal to priority. Thus specific bitrate requirements are not presented in the use case.

- *DIAMETER Indicators:* The "MPS-Identifier" AVP, "Reservation-Priority" AVP, and "DRMP" AVP are essential tools to signal the priority needs for a media flow via the PCC mechanisms to the EPS. These parameters are applied only at the time of establishment of an EPS Bearer.

  The use case assumes that the media paths for both users are established successfully. As these parameters do not apply once the path is established, they cannot be considered to solve the problem presented in the use case.

- *SIP Indicators:* The SIP "RPH" is used to convey priority indication to the IMS Core during the establishment of an NS/EP call/session. It applies only at the time of call/session establishment.

  The use case assumes the call/session is established successfully. As the "RPH" is used only at the time of call establishment, it cannot be considered as a solution to the problem in the use case.

5.4.2 Registration

GETS calls can be made from any phone/anywhere, using a universal access number, 710-627-4387 (710-NCS-GETS), with priority call routing and. Once issued, there is no special registration required (e.g., for wireless origination, normal mobile registration is used).

WPS is a subscription based service, so at the time of UE Registration network elements are pre-provisioned with the knowledge of the WPS user priority profile prior to call/session setup request. This allows the user's call/session to receive High Priority Access and Advance Priority at the Time of Attach.

There is no special registration required for 911 calls/sessions. As a matter of fact, 911 calls/sessions can be made without "normal" registration.

5.4.3 Authentication/Authorization

GETS is available 24x7 to Government-designated users. Users are authenticated and authorized by entering a valid 12-digit Personal Identification Number (PIN) to gain access to GETS. The user is then able to enter a destination number. If a GETS user has the appropriate privileges for the destination dialed (i.e., Domestic, International, Pseudo Destination Number (PDN), Number Translation), the call is allowed to proceed.

WPS as a subscription based service, the UE WPS service authentication is linked to the subscribers profile thereby the service authentication/authorization is part of normal registration.

5.4.3.1 Anti-Spoofing Factors

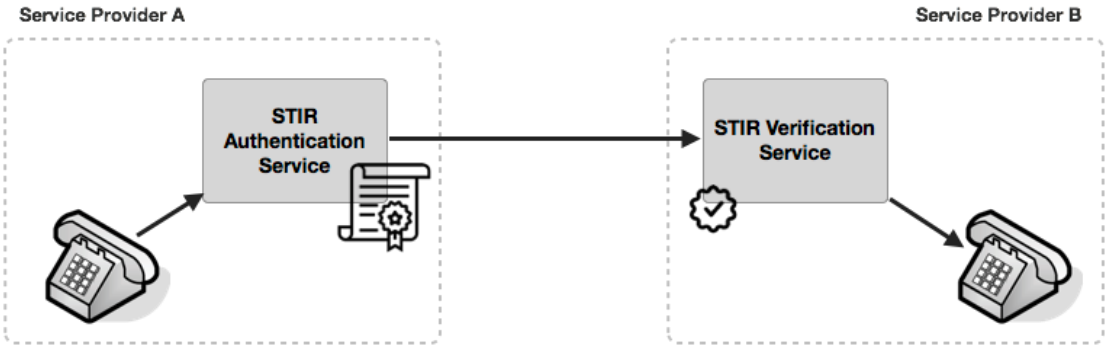
Currently, SS7 Circuit Switched networks rely on hop-by-hop security for ISUP call setup, as there is knowledge of the adjacent switch based on the physical trunk to the adjacent carrier's switch. In SS7 ISUP, the circuit trunk to the adjacent switch is seized prior to forwarding the ISUP IAM call setup message, which would contain an ISUP Calling Party Category of "ns/ep" for identifying NS/EP calls. By this, the receiving switch has knowledge of the sending carrier, and that the call is an authorized NS/EP call and should be treated with priority processing. In SIP, the Resource Priority Header (RPH) parameter "RPH: ets.0" is used to identify National Security / Emergency Preparedness (NS/EP) call requests in an Internet Protocol (IP) environment.

As carrier networks migrate to IP, there is no physical circuit trunk to give knowledge of the far end, the knowledge of the far end is based on an IP Address. Thereby the trust model is end-to-end and not hop-by-hop. Since this SIP RPH header is sent in clear text and can be inserted by any element in the path of the Session Initiation Protocol (SIP) INVITE request, NS/EP carriers need to verify the SIP RPH that was inserted by an authorized carrier before providing priority treatment to these requests. Another mechanism is required in order to trust that the call is an authentication and authorized NS/EP call.

It is proposed to define extensions to the standards that are defined for authentication and verification of caller identification for normal calls carried over an Internet Protocol (IP) networks. These standards are known as SHAKEN (Signature-based Handling of Asserted information using toKENs) defined in the Alliance for Telecommunications and Industry Solutions (ATIS) Session Initiation Protocol (SIP) Forum, and the IP Network-to-Network Interconnection Task Force, and STIR (Secure Telephony Identity Revisited) in the Internet Engineering Task Force (IETF).

The premise of STIR/SHAKEN is that telephone calls and the telephone numbers associated with the calls, when they are originated in a service provider network can be authoritatively and cryptographically signed by the authorized service provider, so that as the telephone call is received by the terminating service provider, the information can be verified and trusted.

The figure below illustrates the STIR/SHAKEN framework basic flow.



The document draft-ietf-stir-passport defines a token-based signature that combines the use of JSON Web Tokens, JSON Web Signatures, and X.509 certificate key pairs, or Public Key Infrastructure (PKI), to create a trusted signature. The authorized owner of the certificate used to generate the signature can be validated and traced back to the known trust anchor who signed the certificate. The PASSporT token includes a number of claims the signer of the token is asserting. The associated public certificate is used to verify the digital signature and the claims included in the PASSporT token. The public certificate is also used to validate the entity that signed the token through a Service Provider Identifier (SPID), as defined in draft-ietf-stir-certificates. The validated claims, and the validated identity of the entity signing the claims, can both be used to determine the level of trust in the originating entity and their asserted calling party information.

It is proposed to extend the "claims" defined in IETF Personal Assertion Token (PASSporT), draft-ietf-stir-passport-10, to support NS/EP calls and signing of the SIP RPH. The signing of the SIP RPH would be performed by the NS/EP authenticating carrier. Thereby, subsequent carriers could validate this is a NS/EP call and provide priority treatment.

5.4.4 Security

The development and deployment of any Priority Services Framework will require close attention to security at all phases of conception, architecture, design, deployment and operation of the priority services system.

The fundamental system design for Priority services must include consideration of security best practices. For example:

- Priority users should be mutually authenticated and authorized using known robust security protocols and mechanisms.
- Sufficient access controls, firewall technology and related mechanisms should be in place to help insure that only authenticated priority users receive priority.

- Priority related network elements should include sufficient intrusion detection/prevention technology with available mitigations for DDoS attacks.
- When appropriate, mechanisms should be available to ensure that priority data communication meets confidentiality/privacy and integrity requirements.
- Priority communications systems should include mechanisms to meet non-repudiation, auditability and accountability requirements.
- Staff involved with operating and managing Priority Services systems should be trained in applicable security practices
- The various methods and procedures developed in support of management and operation of Priority services should be reviewed to insure compliance with security best practices.

A plethora of security best practices and standards exist in the industry. At this time, standards exist to cover a wide variety of security topics. The International Telecommunication Union (ITU) provides a summary of existing, approved ICT security standards[14].

Additionally, the National Institute of Standards and Technology (NIST) *Framework for Improving Critical Infrastructure Cybersecurity* was developed in response to Executive Order 13636 (2013)[15]. This Executive Order calls for development of a voluntary cybersecurity framework that will "provide a prioritized, flexible, repeatable, performance-based, and cost-effective approach, including information security measures and controls, to help owners and operators of critical infrastructure identify, assess, and manage cyber risk"; critical infrastructure being "systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." The resulting Cybersecurity Framework developed by NIST in collaboration with industry, provides guidance on managing cybersecurity risk.

Finally, the Communications Security, Reliability and Interoperability Council (CSRIC) has charted a number of working groups to address various aspects of security.

6 FirstNet Considerations

In addition to the above, Working Group 8 notes the significant impact the deployment of FirstNet and next generation 9-1-1 will have on priority services users and network in the coming years. With that in mind, and understanding that future collaboration between government agencies, operators, and priority services users will be a critical priority as FirstNet proceeds, the working group poses the following questions for continued assessment by future CSRICs or other relevant policy forums:

[14] International Telecommunication Union. 2015. *ICT Security Standards Roadmap Part 2: Approved ICT Security Standards*. http://www.itu.int/en/ITU-T/studygroups/2013-2016/17/ict/Pages/ict-part02.aspx

[15] The White House. "Executive Order no. 13636—Improving Critical Infrastructure Cybersecurity," *Federal Register*, Vol. 78, No. 33, pp. 11739-11744. February 12, 2013. Government Printing Office: Washington D.C. http://www.gpo.gov/fdsys/pkg/FR-2013-02-19/pdf/2013-03915.pdf

- Will FirstNet "Local Control" capabilities over user profiles carry over to public (non-Band 14) networks?

- Will FirstNet users be allowed to preempt other traffic when using public (non-Band 14) networks?

- How will the Quality of Service for FirstNet traffic be managed on public networks, relative to public traffic and other priority traffic such as WPS?

- What LTE access class(es) will be assigned to FirstNet users when on public networks?

- What degree of control will the FirstNet carrier have in assigning traffic to spectral bands?

- How will FirstNet High Power User Equipment be handled on public (non-Band 14) networks?

- What measures are carriers allowed/encouraged/free to take in differentiating 911 traffic from other high-priority access traffic (i.e., FirstNet, WPS)?

- Are carriers allowed/encouraged/free to apply access class barring to 911 traffic?

Will FirstNet "Local Control" capabilities over user profiles carry over to public (non-Band 14) networks?

The FirstNet RFP describes the expectation that the network will provide "both national and local control over prioritization, preemption, provisioning, and reporting". Authorized FirstNet users would be able to dynamically modify various aspects of network behavior and traffic treatment. In certain cases, such as prior to full deployment and in rural or indoor areas, FirstNet traffic will likely be carried on non-Band 14 network resources. The complex combination of traffic on these networks, which are shared with public and other priority traffic, raise the risk that local control could have adverse consequences.

Will FirstNet users be allowed to preempt other traffic when using public (non-Band 14) networks?

FirstNet documents indicate that they are planning to make use of preemption capabilities for traffic on their private network, terminating traffic of some users in favor of others. FirstNet traffic is likely to be carried on public networks for a significant period of time while the private network is being deployed, and even afterwards at certain times and in specific locations. To date, preemption of public voice traffic has not been allowed.

- During times when FirstNet traffic is carried on the public network, will preemption be allowed?
- What types, classes and priority levels of traffic would be subject to preemption (e.g., Voice, Video, Data, machine-to-machine, 911, WPS)?

How will the Quality of Service for FirstNet traffic be managed on public networks, relative to public traffic and other priority traffic such as WPS?

International standards include specific priority levels and traffic treatments for managing the quality of service of data/signaling packets associated with mission-critical push-to-talk (MCPTT), a service of high importance to FirstNet users. The priority and traffic treatment for MCPTT are well suited for the service when run on a dedicated network, but create risks of starving other services, and even network control, on shared networks.

Using the standardized priority and traffic treatments for MCPTT when carried on the public network could adversely affect other services, such as Voice over LTE, as well as network stability. This risk will be even greater if similar priority treatments are defined for mission critical video and data services. Multicasting, as defined in Evolved Multimedia Broadcast Multicast Service (eMBMS), offers a means of handling multi-party traffic efficiently, but requires that resources be set aside *a priori* and not used for other purposes.

- Will resources be reserved for eMBMS for FirstNet use on public networks?

What LTE access class(es) will be assigned to FirstNet users when on public networks?

International standards define Access Class Barring, and corresponding Access Classes, as a means to manage attempts to send traffic when networks are in danger of being overloaded. The international standards specify a set of high-priority access classes (values 11-15) that can be treated specially, with the following recommended allocation:

- 15 Public Land Mobile Network (i.e., service provider) Staff
- 14 Emergency Services
- 13 Public Utilities (e.g., water/gas suppliers)
- 12 Security Services
- 11 For Public Land Mobile Network (i.e., service provider) user

ATIS standards in the U.S. specify that Access Class 14 should be reserved for NS/EP usage. International standards do not specify a priority order between the access classes 11-15, but the standards do provide the means for differentiation among them. Assigning FirstNet users to Access Class 14 would eliminate the possibility of differentiating FirstNet and WPS traffic; assigning them to any other access class would leave that option open.

What degree of control will the FirstNet carrier have in assigning traffic to spectral bands?

The carrier selected to implement the FirstNet network may be looking to make use of both the FirstNet-assigned, Band 14, spectrum and the carrier's assigned spectrum. Such shared usage of these different bands raises concerns, related to the relative treatment of different traffic types. These concerns include a) appropriate treatment of non-FirstNet traffic carried on the Band 14 spectrum, where it might be subject to preemption due to FirstNet traffic, and b) potential impact of FirstNet traffic on other traffic if both are carried on spectrum other than Band 14.

- Will there be rules, regulations or guidance for the FirstNet carrier associated with

assigning these types of traffic to the spectral bands?

How will FirstNet High Power User Equipment be handled on public (non-Band 14) networks?

Part 90 service rules governing the Band 14 spectrum allow public safety users to employ equipment that operates at higher powers than wireless devices operating on the public network. Use of such high-power equipment when roaming onto non-Band 14 networks could cause interference with other, less powerful, devices.

What measures are carriers allowed/encouraged/free to take in differentiating 911 traffic and other high-priority access traffic (i.e., FirstNet, WPS)?

International standards for fourth generation wireless networks provide a mechanism to give 911 and similar "emergency calls" priority in gaining access to network resources. Such priority was not present in standards for earlier technology generations. There are several standardized priority mechanisms that can be used to differentiate such traffic (Access Class, Establishment Cause, Allocation and Retention Priority).

Granting priority to the potentially large number of 911 callers that is equal to or greater than the priority offered to smaller prioritized groups (i.e., WPS and FirstNet users) would put the smaller groups at a significant disadvantage. With freedom to apply differentiation measures, carriers could implement policies that protect the integrity of the other services.

Are carriers allowed/encouraged/free to apply access class barring to 911 traffic?

International standards provide the means for carriers to apply access class barring to 911 calls on a per-cell basis. Current standardized means of 911 access control are extremely coarse, only providing carriers with on/off control of 911 calls at any time. In a crisis situation, a massive number of 911 calls would likely overwhelm the resources of the associated Public Safety Answering Point, which means many of these calls are likely to be unsuccessful. Giving these attempts priority access to the wireless network wastes resources.

Carriers have indicated a reluctance to make use of the barring feature for fear of being responsible for blocking critical calls for assistance. Freedom to apply the Access Class Barring to 911 traffic would enable carriers to implement policies that make resources available for other high-priority traffic. In addition, enhancements to standards are likely required to provide finer control of barring for 911-type traffic and feedback on congestion at the PSAP would provide carriers with additional information

7 Conclusion

The members of Working Group 8 thank all those who have contributed research and perspective to this CSRIC report, and look forward to supporting continued collaboration with policy-makers, service providers, and Users of Priority Services.

Appendix A - QoS Parameters for the EPS

3GPP Standardized QCI characteristics[16]

QCI	Resource Type	Priority Level	Packet Delay Budget	Packet Error Loss Rate (NOTE 2)	Example Services
1	GBR	2	100 ms	10^{-2}	Conversational Voice
2		4	150 ms	10^{-3}	Conversational Video (Live Streaming)
3		3	50 ms	10^{-3}	Real Time Gaming
4		5	300 ms	10^{-6}	Non-Conversational Video (Buffered Streaming)
65		0.7	75 ms	10^{-2}	Mission Critical user plane Push To Talk voice (e.g., MCPTT)
66		2	100 ms	10^{-2}	Non-Mission-Critical user plane Push To Talk voice
5	Non-GBR	1	100 ms	10^{-6}	IMS Signaling
6		6	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
7		7	100 ms	10^{-3}	Voice, Video (Live Streaming) Interactive Gaming
8		8	300 ms	10^{-6}	Video (Buffered Streaming) TCP-based (e.g., www, e-mail, chat, ftp, p2p file sharing, progressive video, etc.)
9		9			
69		0.5	60 ms	10^{-6}	Mission Critical delay sensitive Signaling (e.g., MC-PTT Signaling)
70		5.5	200 ms	10^{-6}	Mission Critical Data (e.g. example services are the same as QCI 6/8/9)

[16] An exerpt from 3GPP TS 23.203: Policy and charging control architecture (Release 13), Table 6.1.7

Appendix B: Stress / Congestion Events

The Federal interagency community developed 15 all-hazards National Planning Scenarios for use in national, Federal, State, and local homeland security preparedness activities. Their objective was to develop a minimum number of credible scenarios to establish the range of response requirements to facilitate preparedness planning. The 15 scenarios are:

- Scenario 1: Nuclear Detonation – 10-kiloton Improvised Nuclear Device
- Scenario 2: Biological Attack – Aerosol Anthrax
- Scenario 3: Biological Disease Outbreak – Pandemic Influenza
- Scenario 4: Biological Attack – Plague
- Scenario 5: Chemical Attack – Blister Agent
- Scenario 6: Chemical Attack – Toxic Industrial Chemicals
- Scenario 7: Chemical Attack – Nerve Agent
- Scenario 8: Chemical Attack – Chlorine Tank Explosion
- Scenario 9: Natural Disaster – Major Earthquake
- Scenario 10: Natural Disaster – Major Hurricane
- Scenario 11: Radiological Attack – Radiological Dispersal Devices
- Scenario 12: Explosives Attack – Bombing Using Improvised Explosive Devices
- Scenario 13: Biological Attack – Food Contamination
- Scenario 14: Biological Attack – Foreign Animal Disease (Foot-and-Mouth Disease)
- Scenario 15: Cyber Attack

Each scenario discussed the following information:

- Scenario Overview
  - General Description
  - Detailed Attack Scenario
- Planning Considerations
  - Geographical Considerations/Description
  - Timeline/Event Dynamics
  - Meteorological Conditions (where applicable)

  - Assumptions
  - Mission Areas Activated
- Implications
  - Secondary Hazards/Events
  - Fatalities/Injuries
  - Property Damage
  - Service Disruption
  - Economic Impact
  - Long-Term Health Issues

Since the scenarios were compiled to be the minimum number necessary to develop the range of response capabilities and resources, other hazards were inevitably omitted, such as frequently occurring natural disasters, such as tornadoes.

The information provided in each scenario was used to hypothesize an event's impact on the communications infrastructure. In general, the communications impact of the scenarios could be categorized into two types:

- Sudden impact events: In these events, communications peaks immediately after the event and diminishes as a function of the elapsed time after the event. Three sudden impact events are defined:
  - Terrorist Attack: Assumed to occur in Washington, DC, which has a large contingent of GETS and WPS users
  - Scenario 9: Natural Disaster: Major Earthquake: Assumed to occur in San Francisco
  - Tornado: Assumed to occur in the suburbs of Nashville
- "Slow developing" events: These events are associated with natural disasters that can be predicted and prepared for in advance. Communications ramps up during preparation, holds somewhat steady during the event, peaks immediately after the event to start recovery efforts, and then diminishes as a function of elapsed time after the event. Three "slow developing" events are defined:
  - Scenario 3: Pandemic: Assumed to occur in Los Angeles
  - Scenario 10: Major Hurricane: Assumed to occur in New Orleans
  - Major Snowstorm / Blizzard: Assumed to occur in Boston

The magnitude of the communications traffic at a given component is typically greater for sudden impact

events than for slow developing events. The traffic mix also differs between the two event types. The following subsections hypothesize user communication profiles for each of the six events.

SUDDEN IMPACT EVENT – TERRORIST ATTACK

A set of IEDs are set off in a coordinated fashion around the Capitol, Rayburn House Office Building, Supreme Court, and Library of Congress while both the Congress and Supreme Court are in session. Public traffic in the area is twice as large as normal given the issues being discussed in Congress and the Supreme Court. The IEDs cause casualties and damage to buildings and vehicles.

Estimated Population in Area of Impact

There are 10,000 Congresspersons and staffers on Capitol Hill, and 1,800 Capitol Hill Police. The Supreme Court has 475 employees, and the Library of Congress has 3,200 employees. There are 30,000 people that live in the Capitol Hill district, of which 25 percent are assumed to be home at the time of the incident. Washington averages 50,000 tourists per day, of which ten percent are assumed to visit the Capitol. Thus 28,000 public users are assumed to be in the impacted area.

Washington, DC has approximately 20,000 WPS users. It is assumed that 15% (3000 users) are in the impacted area.

Public Telecommunications Activities

Immediately after the attack, 80% of public attempt to make a voice call to local family or friends saying they are fine. Twenty percent attempt to make a 911 call. If unsuccessful, 60% reattempt a voice call, while 40% try SMS. Attempts continue until communications are successful.

Next activity is a call to family and friends who are remote. This is done by 50% of the public, first trying a voice call, and then SMS.

After the above activities, 35% of public communicates with social media on event (e.g., tweets, video uploads).

Two hundred reporters from various news organizations enter impacted area and start tweeting and streaming videos.

People outside the affected area, when hearing of the event, attempt to contact 10% of the people in the affected area. Attempts are made via voice, then SMS, then social media.

NS/EP User Telecommunications Activities

Immediately after the attack, 30% of users make a WPS call to coordinate a response to the event. Seventy percent make a GETS call. After the first call, 50% make a second NS/EP call.

Damage to Telecommunications Infrastructure

None.

Intercarrier Traffic

Assume 20% of traffic stays on-net and 80% goes off-net.

SUDDEN IMPACT EVENT – MAJOR EARTHQUAKE IN SAN FRANCISCO

A Richter 7.0 earthquake hits San Francisco during rush hour.

Estimated Population in Area of Impact

The population of San Francisco is approximately 800,000.

There are approximately 13,000 WPS users in California. The population of California is approximately 39 million. Thus San Francisco is approximately two percent of the population. If this ratio also maps into WPS users, there are 260 WPS users in San Francisco.

Public Telecommunications Activities

Immediately after the earthquake, 80% of public attempt to make a voice call to local family or friends saying they are fine. Twenty percent attempt to make a 911 call. If unsuccessful, 60% reattempt a voice call, while 40% try SMS. Attempts continue until communications are successful.

Next activity is a call to family and friends who are remote. This is done by 50% of the public, first trying a voice call, and then SMS.

After the above activities, 35% of public communicates with social media on event (e.g., tweets, video uploads).

Reporters start tweeting and streaming videos.

People outside the affected area, when hearing of the event, attempt to contact 30% of the people in the affected area. Attempts are made via voice, then SMS, then social media.

NS/EP User Telecommunications Activities

Immediately after the earthquake, 30% of users make a WPS call to coordinate a response to the event. Seventy percent make a GETS call. After the first call, 50% make a second NS/EP call.

Damage to Telecommunications Infrastructure

Two cases are assumed: 25% damage to infrastructure and 75% damage to infrastructure.

Intercarrier Traffic

Assume 20% of traffic stays on-net and 80% goes off-net.

SUDDEN IMPACT EVENT – TORNADO IN NASHVILLE AREA

A Fujita Scale 2 (F2) tornado creates a 10 mile path of destruction in the Nashville area.

Estimated Population in Area of Impact

The population of the Nashville Metropolitan Statistical Area is approximately 1.9 million.

There are approximately 1500 WPS users in Tennessee. The population of Tennessee is approximately 6.6 million. Thus the Nashville area is approximately 29 percent of the population. If this ratio also maps into WPS users, there are 435 WPS users in the Nashville area.

Public Telecommunications Activities

Immediately after the tornado, 50% of public attempt to make a voice call to local family or friends saying they are fine. Ten percent attempt to make a 911 call. If unsuccessful, 60% reattempt a voice call, while 40% try SMS. Attempts continue until communications are successful.

Next activity is a call to family and friends who are remote. This is done by 20% of the public, first trying a voice call, and then SMS.

After the above activities, 10% of public communicates with social media on event (e.g., tweets, video uploads).

Fifty reporters from various news organizations enter impacted area and start tweeting and streaming videos.

People outside the affected area, when hearing of the event, attempt to contact 25% of the people in the affected area. Attempts are made via voice, then SMS, then social media.

NS/EP User Telecommunications Activities

Immediately after the tornado, 30% of users make a WPS call to coordinate a response to the event. Seventy percent make a GETS call. After the first call, 50% make a second NS/EP call.

Damage to Telecommunications Infrastructure

Damage to infrastructure is assumed to be 25%.

Intercarrier Traffic

Assume 20% of traffic stays on-net and 80% goes off-net.

SLOW DEVELOPING EVENT – PANDEMIC IN LOS ANGELES

An influenza outbreak causes the Federal, State and local governments in Los Angeles to declare a state of emergency and require all people to stay home for 48 hours.

Estimated Population in Area of Impact

The population of Los Angeles is approximately 3.9 million.

There are approximately 13,000 WPS users in California. The population of California is approximately 39 million. Thus Los Angeles is approximately ten percent of the population. If this ratio also maps into WPS users, there are 1,300 WPS users in Los Angeles.

Public Telecommunications Activities

Voice traffic and social media traffic volume is normal, but comes from residential locations rather than offices. Ninety percent of residences are teleworking; 80% are also simultaneously involved in video streaming or gaming.

Reporters are assumed to shelter in place.

NS/EP User Telecommunications Activities

All NS/EP users make calls during the peak hour.

Damage to Telecommunications Infrastructure

None.

Intercarrier Traffic

Assume 20% of traffic stays on-net and 80% goes off-net.

SLOW DEVELOPING EVENT – MAJOR HURRICANE IN NEW ORLEANS

A Category 3 hurricane traverses New Orleans over a 24 hour period. People either stay at home or move to public shelters to ride out the storm.

Estimated Population in Area of Impact

The population of New Orleans is approximately 379,000.

There are approximately 1,800 WPS users in Louisiana. The population of Louisiana is approximately 4.7 million. Thus New Orleans is approximately eight percent of the population. If this ratio also maps into WPS users, there are 144 WPS users in New Orleans.

Public Telecommunications Activities

Voice traffic and social media traffic volume is half of normal, and comes from residential locations (primarily wireline) and shelters (primarily wireless). Ten percent of residences are teleworking; 50% are involved in video streaming or gaming.

During storm, 80% of public attempt to make a voice call to local family or friends saying they are fine. Twenty percent attempt to make a 911 call. If unsuccessful, 60% reattempt a voice call, while 40% try SMS. Attempts continue until communications are successful.

Next activity is a call to family and friends who are remote. This is done by 50% of the public, first trying a voice call, and then SMS.

Five hundred reporters from various news organizations enter impacted area and start tweeting and streaming videos.

People outside the affected area attempt to contact 30% of the people in the affected area. Attempts are made via voice, then SMS, then social media.

NS/EP User Telecommunications Activities

All NS/EP users make calls during the peak hour.

Damage to Telecommunications Infrastructure

Two cases are assumed: no damage to infrastructure and 25% damage to infrastructure.

Intercarrier Traffic

Assume 20% of traffic stays on-net and 80% goes off-net.

SLOW DEVELOPING EVENT – MAJOR SNOWSTORM / BLIZZARD IN BOSTON

A major snowstorm / blizzard hits Boston and shuts down the city for a 48 hour period.

Estimated Population in Area of Impact

The population of Boston is approximately 1.9 million.

There are approximately 2,300 WPS users in Massachusetts. The population of Massachusetts is approximately 6.8 million. Thus Boston is approximately 28 percent of the population. If this ratio also maps into WPS users, there are 644 WPS users in New Orleans.

Public Telecommunications Activities

Voice traffic and social media traffic volume is normal, but comes from residential locations rather than offices. Ninety percent of residences are teleworking; 80% are also simultaneously involved in video streaming or gaming.

During storm, 80% of public attempt to make a voice call to local family or friends saying they are fine. Twenty percent attempt to make a 911 call. If unsuccessful, 60% reattempt a voice call, while 40% try SMS. Attempts continue until communications are successful.

Next activity is a call to family and friends who are remote. This is done by 50% of the public, first trying a voice call, and then SMS.

Five hundred reporters from various news organizations enter impacted area and start tweeting and streaming videos.

People outside the affected area attempt to contact 30% of the people in the affected area. Attempts are made via voice, then SMS, then social media.

NS/EP User Telecommunications Activities

All NS/EP users make calls during the peak hour.

Damage to Telecommunications Infrastructure

None.

Intercarrier Traffic

Assume 20% of traffic stays on-net and 80% goes off-net.