National Public Safety Telecommunications Council (NPSTC)		
Priority and QOS - Public Safety Requirements		DATE: 3/12/2015
REQ NUM	Public Safety Requirement Statement	Footnote
Table 6. User Prioritization Requirements		
6-1	FirstNet SHALL develop a policy for the NPSBN that requires a nationwide standard for prioritization and QoS.	This requirement is not intended to preclude support for regional policy differences. As an example, there could be unique regional policies for operations associated with airports and other critical infrastructure sites; as well as urban and rural operational needs.
6-2	FirstNet SHALL define the default priority and QoS policies for all NPSBN users.	Note: In order to provide a consistent responder experience across the full NPBSN, day-to-day priority and QoS must behave similarly, regardless of where the responder is located within the NPSBN. In this context, the word "policies" means the priority and QoS that the NPSBN user receives in response to the user's own priority attributes (e.g., Type of User, Incident Role, etc.), type of Appliction used (e.g. MC Voice, Video, etc.) and user's group priority attributes (Type of Group, Incident Severity, etc.). FirstNet is encouraged to work with state and local government to define clear and concise default priority policies. The Default priority is the static priority that is established at the time the user device is provisioned. Dynamic priority, involving priority level changes based on incident assignment or urgent event, are addressed in Requirement X.X
6-3	FirstNet SHALL establish a policy whereby public safety applications (such as CAD and video which require QoS support for their proper operation) will utilize standardized mechanisms to inform the network of their prioritization and QoS attributes.	Note: In this context "standardized mechanisms" means FirstNet provided or approved specifications.

6-4	Pursuant to Section 6211 of the Act, Responder Emergency and Immediate Peril SHALL have the highest user priorities on the NPSBN or on a commercial wireless network.	NOTE: Public safety agencies need their Emergency and Immediate Peril urgent traffic priority assignments to carry over to commercial networks, when public safety users roam to a commercial network. It is understood that FirstNet negotiations with commercial carriers will ultimately define the realized priority the Responder Emergency and Immediate Peril capabilities receive while roaming on commercial system networks.
6-5	The lowest network priorities SHALL be reserved for those users who lease the spectrum for commercial and/or personal use.	
Table 40. Responder Emergency Requirements		
40-1	The Responder Emergency function can be initiated by a responder for him/herself or can be initiated by another authorized NPSBN user (e.g. incident commander or dispatcher) on behalf of the responder. When the function is initiated, an agency-defined list of applications will be given priority for the responder.	NOTE: there will be differences between the devices and applications used by law enforcement, fire, and EMS personnel and different safety risks associated with each group. An police agency may wish to program automatic high priority for voice and the officer's lapel video camera when the Emergency button is activated. A fire agency may program automatic high priority for voice and telemetry from the firefighters physiologic sensors measuring heart rate, temperature and air remaining in the SCBA tank.
40-2	The NPSBN SHALL provide the ability for the NPSBN user or other authorized user (incident commander or dispatcher) to clear an emergency condition.	
40-3	An authorized PSEN administrator SHALL be able to configure which NPSBN users can initiate and clear the emergency condition. This means, for example, the administrator can elect the responder, the dispatcher, or both to clear the emergency condition.	PSEN is the Public Safety Enterprise Network which represents the local agency IT network
Table 41. Immediate Peril Requirements		

41-1	The NPSBN SHALL provide the ability for the NPSBN user (or other authorized user) to initiate the Immediate Peril condition.	Immediate Peril conditions are those that do not meet the Emergency button criteria (which includes an immediate threat to the life of the first responder); and instead indicates an urgent situation in which the first responder needs to override their current priority and QOS configuration, during times of network congestion. This would typically occur if the life of a non first responder was in danger. For example, a paramedic must establish a video connection to a physician during times of network congestion. The use of the Immediate Peril functionality is determined by local agency policy. Because this feature may involve safety to life and property, it is one priority level below Responder Emergency. This is designed to provide more flexibility for the user agency and the first responder. The PSEN Administrator can enable or disable this functionality; as they would with other features and functions when provisioning a user device.
41-2	When the Immediate Peril condition is initiated, an agency-defined list of applications will be given priority for the responder. The exact elevated priority given to an application with Immediate Peril priority is a policy decision to be determined by the PSEN.	It is not intended that an agency would assign a priority level equal to the Emergency button priority level.
41-3	An authorized PSEN administrator SHALL be able to configure which NPSBN users can clear the immediate peril condition. This means, for example, the administrator can elect the responder, the dispatcher, or both to clear the immediate peril condition.	
Table 42. ICS Incident Priority Requirements		

42-1	The NPSBN SHALL allow an NPSBN users PQoS priority attributes (Responder Emergency state, Incident Status, etc.) to be altered dynamically based on the Incident and locally controlled needs.	This dynamic reassignment may occur via a CAD system interface which notifies the LTE network that specific user devices have been assigned to a high priority incident.
Table 54. General Requirements for the Nationwide Private IP Network		
54-2	The nationwide private IP network SHALL support end-to-end QOS. This is to guarantee a defined QOS behavior from an application to the UE.	End to end QOS is emphasized to ensure that congestion on backhaul and other network segments do not interfere with the assigned priority level. This is for traffic traveling within the FirstNet network. See 117-7 and 117-8 for end to end P&QOS requirements for traffic traveling between FirstNet and other networks
Table 77. Dynamic Role Re-Assignment Requirements		
77-1	Each PSEN administrator SHALL have the ability to change the users PQoS priority attributes (Responder Emergency state, Incident Status, etc.) based on the Incident and locally established needs.	This requirement is the manual process to manage dynamic priority assignments identified in Requirement 42-1.
77-2	Each PSE administrator SHOULD have the ability to reset individual users to the pre-incident settings in a one-step action.	This may occur manually or automatically. For example, clearing a public safety unit from the scene in the CAD system may revert the unit from an elevated priority back to a default priority.
Table 101. Encryption, Certificates, and Key Requirements		
101-4	The NPSBN SHALL support various transport mechanisms that preserve and protect end to end application data transmission to assure that QoS and Priority Services are maintained.	For example, VPN's are required by many agencies for criminal justice and health care data transfer. This is related to Requirement 54-2
Table 112. Priority and QoS Configuration Requirements		
112-1	When assigning default priority and QoS to an NPSBN-U, the authorized administrator (NPSBN or PSEN)SHALL have the ability to choose from a list of standardized 'templates.'	

112-2	It SHALL be possible for an authorized administrator (NPSBN or PSEN) to alter, in run-time (i.e., while the NPSBN is operating), the template assigned to an NPSBN-U or group of NPSBN-Us.	
Table 113. End-to-End Priority and QoS Requirements		
113-1	NPSBN backhaul, transport, and IP packet prioritization techniques SHALL be consistently applied to the entire NPSBN.	
Table 114. Quality of Service Requirements		
114-1	On a per-application flow basis, it SHALL be possible for the NPSBN to assign and control the packet latency and packet loss characteristics.	
114-2	The NPSBN SHALL be capable of determining which application flow a packet is associated with based on network configuration.	This requirement is related to Requirement 101-4 and 54-2
114-3	The NPSBN SHALL be capable of determining which application flow a packet is associated with when MVPN or VPN technology is being used.	
114-4	It shall be possible for an authorized NPSBN administrator to define templates (groupings) for combinations of packet loss and packet latency rates.	
Table 115. Admission Control Requirements		
115-1	The NPSBN SHALL distinguish between devices from public safety and secondary users during congestion to allow priority access for public safety/first responders when needed.	
115-2	The NPSBN SHALL implement mechanisms for the PSEN Administrator to manually restrict secondary user devices from making access attempts at the scene of an incident to minimize system performance degradation. This should not affect 9-1-1 calls originated by secondary users.	While this functionality should be handled automatically by the PQOS feature set in LTE, this requirement allows for a manual intervention if indicated. There may be secondary users on scene who are performing a public safety mission critical function and whose devices should not be restricted.

115-3	The NPSBN SHALL automatically manage access for devices from secondary users during cell congestion to ensure first responders maintain appropriate PQOS access levels. This should not affect 9-1-1 calls originated by secondary users.	FirstNet has not yet defined public safety users. This requirement is designed around non public safety users
115-4	The NPSBN SHALL provide the ability for the PSEN Administrator to manually control access to the NPSBN for different classes of users.	The various classes of users are not yet defined; but FN will need an ability to manage different classes (first responders, critical infrastructure, secondary users, etc.) Manual control was intended to acknoweldge that a user may need to be changed in a non automatic way based on the realization that a user needs higher access
Table 116. Static Admission Priority Requirements		
116-1	The default admission priority for an NPSBN user shall be the combination of the Application priority from requirement 116-3 of this table and the default priority of NPSBN user, which is based on the user's normal role and is set when the NPSBN user is first configured.	
116-2A	The NPSBN SHALL support the following relative application priorities when administering the NPSBN-U's default admission priority (1 = highest relative priority): 1 Mission Critical Voice 2 Mission Critical Data 3 Mission Critical Video 4 Non Mission Critical Voice 5 Non Mission Critical Video 6 Non Mission Critical Data **NOTE This chart was changed to reflect the new categories created for 2014-2015**	The numbers should not be construed as actual NPSBN configuration values; rather relative rankings compared to the other listed applications. It is further understood that the rankings should be periodically reviewed as new applications become available. It is recognized there are multiple methods to realize text messaging (e.g., control channel, over-the-top, etc.) and the ability of LTE technology to satisfy this requirement varies with the method selected.

116-2B	The NPSBN user services and application **priority** SHALL be based on the NPSBN identity management system.	An identity management system is necessary in order to assign appropriate priority attributes to the responder.
Table 117. Dynamic Priority and QoS General Requirements		
117-1	The NPSBN SHALL provide a 'Dynamic Priority and QOS control service' to allow suitable PSEN and mobile applications to override the default day-to-day priority assigned by the PSEN administrator.	
117-2	NPSBN LTE users and Non-LTE public safety users SHALL NOT be burdened by the NPSBN with priority and QoS control outside of their operational paradigms. It is understood that human intervention is required to initiate a dynamic Priority and QoS change, but the act of performing this change should not significantly distract the responder. For example, the responder should be able to press an emergency button for a life-threatening condition and not have to enter an LTE terminal to adjust complex LTE priority and QoS parameters.	
117-3	The NPSBN SHALL provide an interface to each PSEN in order for PSE applications to invoke dynamic Priority and QoS changes for the PSE's associated NPSBN-Us. The intent is to say triggering Priority and QoS changes should be integrated into the responder's existing applications and workflow.	
117-4	The NPSBN SHALL provide a profile (documented configuration standards) to all entities using Priority and QoS. This profile will ensure consistent treatment of NPSBN user resources across the entire NPSBN.	

117-5	The NPSBN SHALL provide usage and/or billing records to individual agencies, identifying usage of dynamic priority and QoS controls described in this section.The intent is for agencies to be able to identify usage patterns of dynamic priority and QoS usage by specific NPSBN-Us.	
117-6	The NPSBN SHALL provide near-real-time notification to the PSEN Administrator and the initiating NPSBN-U's associated device(s) when any dynamic priority and QoS control described in this section has been activated or de-activated. The intent of this requirement is to provide notification to PSEN administrators and the NPSBN-U device that one or more of their NPSBN-Us are currently in a heightened usage state.	The intent of this requirement is to allow a PSEN administrator or local agency to have a flexible monitoring capability to be aware of network utilization including PQOS issues. This requirement also allows notification to the User Device that their requested priority was granted or denied.
117-7	NPSBN-Us operating on the NPSBN, when attempting to communicate with devices operating on <u>other networks</u>, SHALL be able to convey end-to-end priority needs to the interconnected IP-based system(s) in order to increase the probability of completing communications during periods of network congestion or impairment.	Responders often need to interact with the users and agencies that operate outside of the NPSBN system. Congestion in either the NPSBN or external (e.g., commercial) system can result in a lowered probability of call success. This requirement will likely have impact to interconnected systems (e.g., commercial carriers). If a telemedicine session from the paramedic going to the hospital ER crosses beyond the NPSBN network to the commercial network, it needs priorirty throughout the connection. This functionality is dependant on the ability to the NPSBN entity to negotiate appropriate arrangements with commercial carriers.

117-8	When an NPSBN-U receives an incoming call from outside the NPSBN flagged with an appropriate priority message header, it SHALL be possible for the originating IP-based system to convey end to end priority needs to the NPSBN in order to increase the probability of completing communications during periods of network congestion or impairment. This is meant to include interconnected public safety, commercial, satellite, and other IP based networks.	This requirement supports the ability for users of the Next Generation Network Priority Services (NGN-PS) to effectively communicate with public safety personnel operating on the NPSBN."
117-9	It SHALL be possible for an authorized NPSBN-U to view in near real-time the current priority and QoS settings for themselves or for another NPSBN-U from the same PSE. The intent, for example, is for a responder or dispatcher to be able to see that a dynamic priority and QoS setting has been activated for a particular user.	
Table 118. Pre-emption Requirements		
118-1	The NPSBN SHALL support the ability to instantly remove resources from one NPSBN-U application and make those resources available to another NPSBN-U application.	
118-2	It SHALL be possible for an authorized NPSBN administrator (NPSBN and PSEN) to configure which applications can utilize resources previously assigned to other applications.	
118-3	The NPSBN SHALL support the ability to change whether or not a given application can be pre-empted, based on triggers from an application or NPSBN-U.	
Table 119. Priority and QoS for Secondary User Requirements		
119-1	Secondary users SHALL be able to access the NSPBN so long as the act of connecting to the NPSBN does not in any way interfere with or prevent a primary user from accessing the NSPBN. See Section 6.1.3.	

119-2	Secondary users SHALL be able to obtain resources from the NPSBN so long as the act of obtaining resources from the NPSBN does not in any way pre-empt resources previously obtained by a primary user or prevent a primary user from obtaining resources.	
119-3	When a primary user attempts to obtain resources and congestion is present, the NPSBN SHALL pre-empt secondary user resources in order to admit the primary user's resource request. The intention is to pre-empt high bandwidth applications first, such as streaming multimedia services, before pre-empting voice services.	
119-4	Should pre-emption be required, the NPSBN SHALL first pre-empt secondary user resources before pre-empting any resources used by a primary user.	
Table 120. General O&M QoS Management Requirements		
120-1	The NPSBN SHALL provide a means for PSEN Administrator or designee to configure the default priority (as defined in Table 6, Requirement #2) and QoS settings of users within their scope.	This could include device support staff as authorized by the agency PSEN administrator.
120-2	The NPSBN SHOULD provide an O&M tool to provide the QoS management capabilities described herein.	
Table 121. QoS Configuration Requirements		
121-1	The QoS configuration capability SHALL allow suitably authorized PSEN Administrators or designees to define/assign QoS roles for their PSE.	
Table 122. QoS Configuration History Requirements		
122-1	Suitably authorized PSE administrators SHALL be able to view a QoS configuration history for users under their authority.	
122-2	Suitably authorized PSEN Administrators or designees SHALL be able to view a QoS configuration history for users under their authority.	
Table 123. QoS Monitoring Requirements		

123-1	PSEN Administrators SHALL be able to view the real-time dynamic priority condition of all users under their authority.	
123-2	PSEN Administrators SHALL be able to retrieve information that allows for “post-mortem” evaluation of the effectiveness of QoS configurations in providing for effective incident communications.	
Table 124. QoS Control by O&M Users Requirements		
124-1	PSEN Administrators SHALL be able to modify the QoS role of users within their scope.	