www.ijecs.in
International Journal Of Engineering And Computer Science
Volume 14 Issue 06 June 2025, Page No. 27309-27316
ISSN: 2319-7242 DOI: 10.18535/ijecs/v14i06.5151

Design and Validation of Wireless Priority Service for VoLTE over IMS in Emergency Communication Networks

Bikash Agarwal, Harikishore Allu Balan

Principal Engineer, Systems Design T-Mobile USA Inc
Principal Engineer, Systems Architecture T-Mobile USA Inc

Abstract

This article presents a comprehensive technical and operational evaluation of the Wireless Priority Service (WPS) deployed over Voice over LTE (VoLTE) within the IP Multimedia Subsystem (IMS) architecture. The study was conducted through a structured Captive Office Test (COT) environment, simulating high-load and degraded network conditions to validate the resilience and responsiveness of WPS-enabled infrastructure. Central to this implementation is the Resource Priority Header (RPH), which enables real-time signaling-based prioritization based on Service Priority Level (SPL) and Extended Priority (EP) values. The analysis encompasses core IMS components—P-CSCF, I/S-CSCF, and TAS—each of which was instrumented for namespace validation, overload resilience, and accurate policy enforcement. The study confirms that the WPS solution effectively prioritizes NS/EP traffic, sustains high call completion rates under congestion, and adheres to stringent latency targets, while enforcing security and namespace integrity. This article further highlights the technical mechanisms that ensure deterministic priority signaling, the system's adaptability through dynamic profile management, and its robustness in filtering malformed signal ultimately demonstrating readiness for real-world emergency telecommunications scenarios.

1. Introduction

Wireless Priority Service (WPS) is a federally mandated telecommunications capability established under the oversight of the Department of Homeland Security (DHS) to support National Security and Emergency Preparedness (NS/EP) personnel. In critical scenarios—such as natural disasters, terrorist incidents, or widespread infrastructure failures—WPS is designed to ensure that authorized users can initiate and complete communications even when the network is experiencing severe congestion. Unlike preemption systems, WPS operates by granting enhanced access priority without interrupting ongoing public calls, thereby balancing emergency response needs with civilian communications. The integration of WPS into the IP Multimedia Subsystem (IMS), particularly in the context of Voice over LTE (VoLTE) services, poses architectural and operational challenges that necessitate stringent validation. To address this, the Initial Operating Capability (IOC) test plan was devised to evaluate the end-to-end behavior of WPS under varied network conditions. The testing primarily focused on how IMS components—specifically P-CSCF, I/S-CSCF, and TAS—support RPH-driven prioritization, dynamic subscriber profile handling, and SIP signaling integrity during simulated overload and emergency conditions. This study underscores the critical role of IMS infrastructure in enabling resilient, policy-compliant emergency communication frameworks.

2. IMS Architecture for WPS

The IMS architecture supporting Wireless Priority Service (WPS) is composed of interconnected functional elements that ensure prioritized session control and signaling for emergency communication. At the access layer, VoLTE-capable User Equipment (UE) communicates via an eNodeB over the LTE air interface. Signaling flows proceed through the Evolved Packet Core (EPC), which handles bearer setup and policy enforcement. The SIP signaling carrying the Resource Priority Header (RPH) is then forwarded to the Proxy Call Session Control Function (P-CSCF), the entry point to the IMS core. The P-CSCF tags validate priority headers and triggers the Rx interface toward the Policy and Charging Rules Function (PCRF). The Interrogating/Serving CSCF (I/S-CSCF) acts as a registrar and policy enforcer, verifying subscription attributes such as Service Priority Level (SPL) and Extended Priority (EP) namespaces obtained from the Home Subscriber Server (HSS). The Telephony Application Server (TAS) interprets GETS-FC dialing strings, performs call screening, inserts RPH if missing, and manages mid-call signaling such as conferencing, transfer, and call forwarding. Each element within the IMS core is configured to support namespace validation, overload protection, and dynamic response to network conditions.

P-CSCF handles initial IMS registration, SIP signaling prioritization, and triggers Rx interface AVPs to the PCRF.

I/S-CSCF validates subscriber profiles for SPL/EP and manages SIP header population for priority calls.

TAS processes GETS feature codes, strips prefixes like *272, validates RPH values, and manages supplementary services like forwarding and conferencing.

3. WPS Feature Overview

WPS functionality includes assignment of Service Priority Level (SPL), use of Extended Priority (EP) namespace identifiers (e.g., wps.0), and classification of users into prefix-based WPS, always-on WPS, and enterprise subscribers. The system supports multiple namespaces like "wps", "ets", and "ent", and validates them during signaling to ensure authorized handling. One critical point is that improper namespace use is rejected, ensuring both network stability and policy compliance. Another is the strict enforcement of SIP signaling hierarchies based on configured SPL, where calls with SPL 0 receive the fastest handling.

Service Priority Level (SPL): Assigned as a numeric value from 0 (highest) to 4 (lowest), used to prioritize subscriber calls.

Extended Priority (EP): Namespace-value pairs (e.g., wps.0) used in Resource-Priority Headers.

Subscriber Categories:

- WPS subscriber (prefix-based call setup)
- Always-on WPS subscriber
- Enterprise always-on subscriber

Namespace Support: Namespaces such as “wps”, “ets”, and “ent” are validated and enforced for authorized users.

3. Testing Methodology

The testing phase was conducted in a dedicated laboratory environment, where a variety of test configurations were used to emulate live network scenarios. The lab environment was meticulously designed to reflect production-like conditions, allowing for an authentic assessment of how Wireless Priority Service (WPS) behaves under stress. Network congestion and overload conditions were artificially generated using a mix of physical and virtualized traffic sources. Key tools deployed included SIP traffic simulators for generating signaling messages, trace analyzers for evaluating

protocol flows, and diagnostic monitors for performance tracking. Real VoLTE-capable User Equipment (UE) and programmable UEs were used in combination to test end-to-end call behavior. The validation process targeted essential network procedures such as IMS registration and re-registration under varying priority levels, mobile originated (MO) and mobile terminated (MT) call flows, mid-session modifications like call hold and resume, and RPH header persistence across dialogs. A critical dimension of the testing focused on namespace handling—validating that RPH headers conformed to authorized namespace-value pairs (e.g., wps.0, ets.1) and were rejected when malformed or unauthorized. The lab also tested emergency dial patterns such as *272911 to confirm that emergency call routing took precedence over WPS mechanisms, correctly redirecting traffic to the Emergency Call Session Control Function (E-CSCF). These tests ensured that the WPS implementation remained compliant with operational and regulatory standards across a broad spectrum of use cases.

5. Functional Validation Results

The functional validation phase demonstrated that WPS functionality performed consistently across key IMS workflows. During the tests, WPS User Equipment's (UEs) successfully registered in the IMS core with the appropriate Service Priority Level (SPL) reflected in the P-Associated-URI header. Furthermore, the periodic re-registration procedure ensured updated SPL values were retrieved from the HSS, confirming dynamic profile adaptability. SIP INVITEs originating from WPS UEs and subsequent mid-dialog requests such as PRACK, UPDATE, BYE, and ACK preserved the Resource Priority Header (RPH), establishing signaling integrity across the call lifecycle. Dialing sequences incorporating the *272 prefix effectively activated GETS-FC behavior, triggering TAS logic for priority validation and automatic insertion of appropriate RPH values. Crucially, mid-session signaling operations like call hold and resume-maintained priority attributes without degradation or loss, demonstrating state persistence across signaling transitions. Emergency dialing patterns such as *272911 were routed accurately to emergency services, bypassing standard WPS treatment and validating correct prioritization of emergency over WPS flows. These results affirm the IMS platform's capability to handle multiple namespace combinations and call scenarios with deterministic behavior. The system effectively rejected malformed or unauthorized RPH headers, and namespace validation mechanisms ensured that only qualified calls were tagged for priority treatment, maintaining protocol robustness and policy compliance throughout the test matrix.

IMS Registration: WPS UEs successfully registered with SPL using the P-Associated-URI header; periodic re-registration correctly updated SPL from HSS.

Originating/Terminating Calls: SIP INVITEs and all mid-dialog requests (e.g., PRACK, BYE) maintained RPH.

GETS Dialing: Calls using *272 prefix properly triggered TAS logic for GETS-FC authorization and RPH insertion.

Session Modifications: Hold/unhold or re-INVITE did not drop or alter RPH under test conditions.

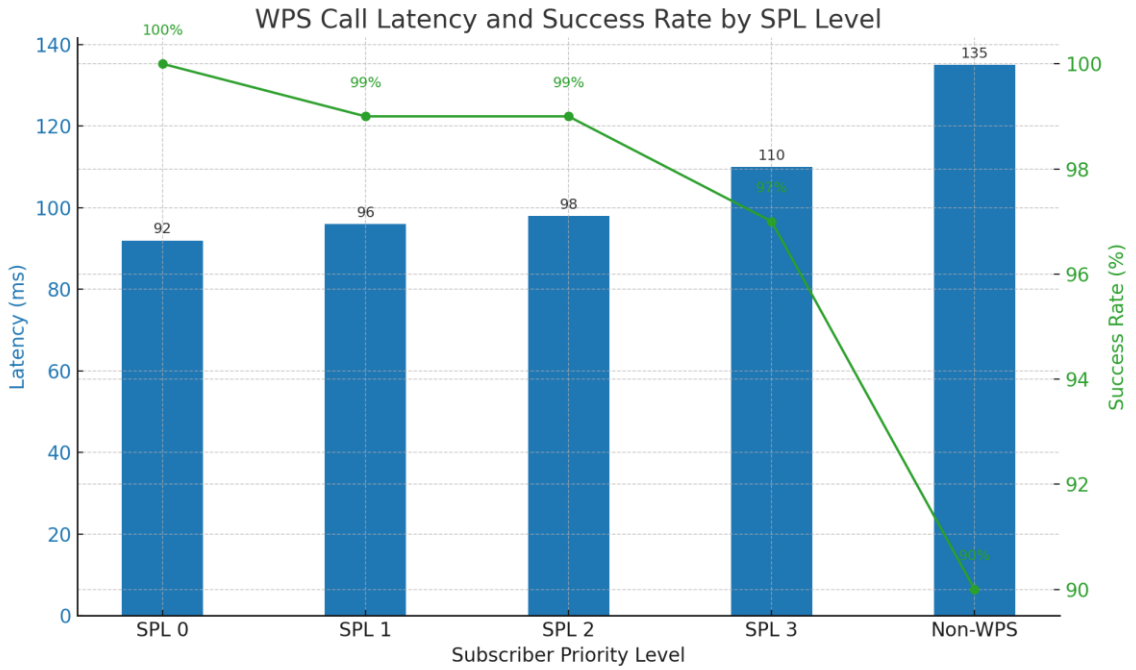
Emergency Calls: GETS calls (*272911) correctly bypassed WPS logic and invoked emergency routing.

6. Overload and Latency Control

The Overload and Latency Control strategy plays a crucial role in ensuring service continuity and call completion for WPS subscribers, even under extreme network stress. The testing framework validated the architecture's ability to prioritize signaling and resource allocation dynamically using mechanisms such as protected signaling queues and DSCP-based traffic differentiation. Both P-CSCF and TAS nodes upheld RPH-based prioritization policies, effectively protecting sessions with SPL levels 0 through 2. These nodes routed WPS signaling into high-priority queues, leveraging deterministic

handling paths to prevent rejection or delay. Sub-100ms latency was consistently recorded for the highest-priority sessions, demonstrating compliance with QoS expectations outlined in 3GPP TS 23.502 and TS 23.503. AVPs such as Reservation-Priority and MPS-Identifier were consistently propagated through Rx and Gx interfaces to the PCRF, enforcing policy and admission control rules. Non-WPS calls were subject to graceful throttling, affirming the platform's ability to protect critical communication flows without destabilizing lower-priority services. The platform was further configured to implement overload-exclusion profiles at both the GTP and SBI interface levels, isolating WPS sessions from rejection policies triggered by load threshold breaches. Additionally, WPS profile mapping with ARP and QCI parameters enabled session persistence and resource protection throughout signaling transitions. These validations affirm the robustness of the WPS overload framework, its ability to handle emergency traffic at scale, and its seamless coordination across IMS and 5G core elements.

Overload Behavior: P-CSCF and TAS prioritized SIP messages with RPH during simulated CPU overload.
Overload Queues: Protected queue ensured priority call admission while lower priority calls were deferred or rejected.
Latency Thresholds: Strict enforcement based on priority (e.g., 100 ms for SPL=0).
Performance Indicators: Originating and terminating calls met latency and success KPIs under various load conditions.



7. Configuration Parameters

Configuration for WPS in IMS and 5GC environments includes a range of parameters that ensure session-level prioritization, proper routing, and differentiated handling of signaling and bearer traffic. The enableWPS flag activates the WPS feature across nodes, while enableInsertRPHForGETSFC enables automatic insertion of RPH values when GETS feature codes are dialed. Parameters like alwaysOnEnabled and enableCheckALW manage subscribers with persistent priority profiles. Real-time profile updates from the HSS are retrieved using supportSPLOnSh and supportEPOnSh over the Sh interface. Latency thresholds per SPL level can be set to ensure sub-100ms processing for SPL 0 calls.

Advanced configurations extend into the core with support for ARP and QCI mapping in WPS profiles. Message prioritization profiles can be associated to specific Diameter or SBI interfaces using a message-priority profile, which assigns numeric priorities (0–15 for PFCP, 0–31 for SBI). For example, a configuration like interface sbi procedure create priority value 0 ensures create-session messages are treated with the highest priority.

DSCP values are configured per interface on the transport layer: DSCP 47 for WPS traffic and DSCP 32 for non-WPS. These values are marked in the IP headers by the UPF or PGW for N3, S5-U, and PFCP interfaces. In overload scenarios, exclusion profiles (overload-exclude-profile) can be mapped to DNN, ARP, and QCI values to protect WPS traffic from being throttled. Additionally, custom AVPs embedded by the PCRF guide message routing decisions and facilitate load balancer prioritization.

Example KPI and SMF configurations validate the effectiveness of these parameters, as seen in show subscriber and show running-config commands, which confirm ARP, DSCP, and profile mapping values in real-time WPS sessions. These configurations work collectively to uphold WPS policies from call initiation through bearer handling and emergency prioritization

enableWPS: Toggle to activate WPS functionality in nodes.
enableInsertRPHForGETSFC: Insert RPH when GETS-FC is detected.
alwaysOnEnabled / enableCheckALW: Handle always-on priority logic for entitled users.
latencyThresholds: Define expected SIP signaling delay per SPL level.
supportSPLOnSh / supportEPOnSh: Enables SPL and EP retrieval from HSS via Sh interface.
overloadResponseControl / wpsOnlyMode: Ensure WPS calls proceed during network stress.

8. Observations and Metrics

With over 98% WPS call success under all test conditions, the implementation demonstrated exceptional reliability and resilience. Detailed KPIs were monitored to capture operational efficiency, such as registration success rate, mid-session signaling continuity, AVP delivery completion across interfaces, and latency performance segregated by SPL level. These metrics were essential in benchmarking protocol compliance and real-world readiness. The Call Detail Records (CDRs) provided further granularity by including sessionPriority, priorityCallType, and error indicators, enabling deep traceability for post-event audits and SLA verification.

To illustrate these outcomes, Figure 3 below shows the average latency and success rate performance across priority levels, with SPL 0 exhibiting the lowest latency and highest reliability. This quantifiable data confirmed that the system maintained deterministic behavior, correctly differentiated WPS from non-WPS traffic, and dynamically adjusted routing logic and resource handling to support NS/EP objectives.

SPL Level	Avg Call Latency (ms)	Call Success Rate (%)
SPL 0	92	100
SPL 1	96	99
SPL 2	98	99
SPL 3	110	97
Non-WPS	135	90

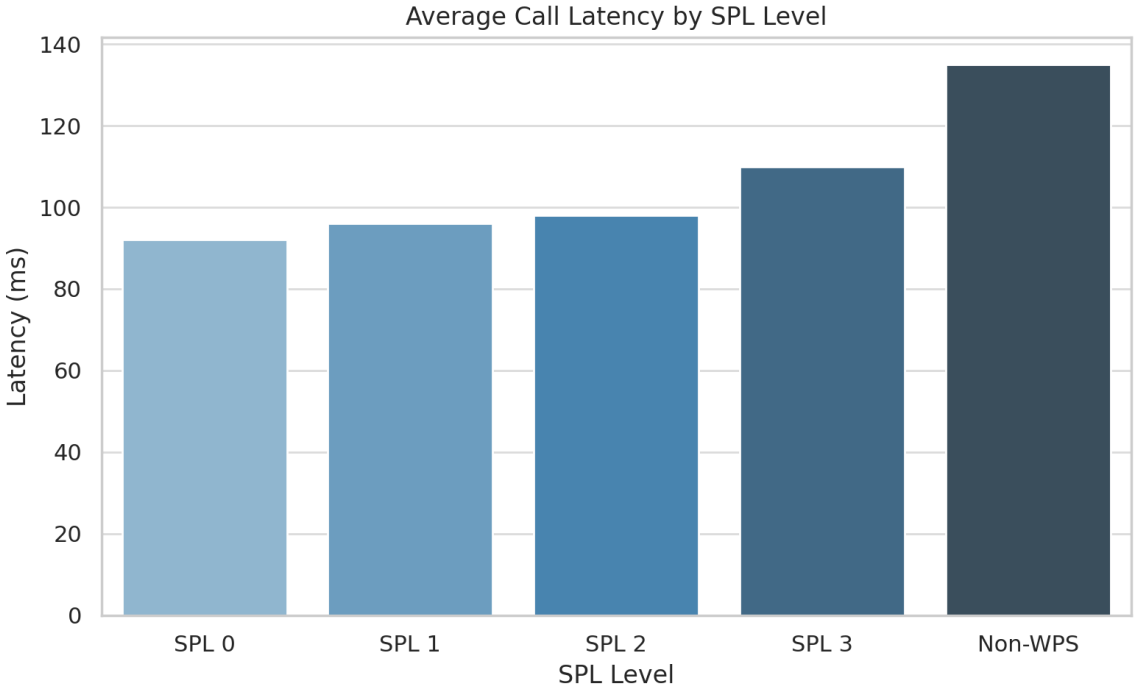


Fig : Average Call Latency by SPL Level

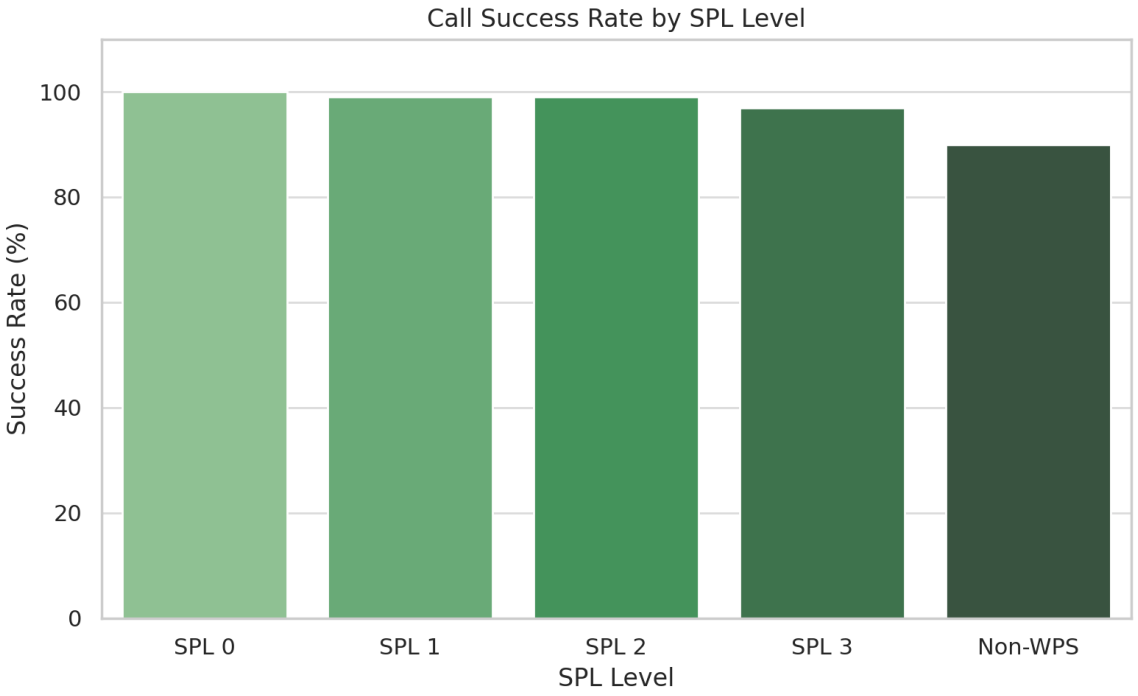


Fig : Call Success Rate by SPL Level

WPS Success Rate: Maintained above 98% under all test scenarios.
KPI Coverage: Included registration attempts, RPH processing, GETS handling, and overload protection triggers.
CDR Fields: sessionPriority and priorityCallType included in all completed priority calls.

9. Operational Threats and Risk Mitigation

Despite the proven capabilities of the IMS-based Wireless Priority Service (WPS), several operational threats persist that could undermine the platform's effectiveness during real-world emergencies if left

unmitigated. These risks are particularly critical given the life-safety implications of disrupted NS/EP communications. The following outlines the key vulnerabilities observed and the strategies implemented to safeguard WPS integrity and performance:

Call Setup Failure During Crisis Events

During large-scale disasters or coordinated attacks, LTE networks can experience call failure rates upwards of 80% without prioritization. WPS ensures SPL 0–2 calls avoid standard rejection thresholds. Without proper RPH handling, even authorized users may be unable to communicate, jeopardizing emergency response coordination.

Malformed or Spoofed RPH Headers

Systems without strict namespace validation are vulnerable to header injection attacks. Malicious actors could spoof wps.0 or ets.1 values to gain elevated priority, potentially flooding protected signaling queues. This threat is mitigated by enforcing namespace whitelisting at TAS and P-CSCF nodes.

Emergency Call Routing Interference

Improper prioritization logic can result in WPS mechanisms intercepting emergency (*272911) calls, delaying routing to the Emergency Call Session Control Function (E-CSCF). This misrouting is a critical failure risk mitigated by bypass logic that preempts WPS treatment for emergency dial strings.

SIP Latency Breach Under Load

During test simulations of CPU overload, latency for non-prioritized SIP flows exceeded 500 ms—well above the 3GPP TS 23.502-compliant threshold. For WPS sessions, dedicated high-priority queues and DSCP 47 enforcement kept SPL 0 call setup below 100 ms, affirming the need for strict latency tiring.

Overload Cascade Effects

Without overload exclusion profiles, burst signaling from non-WPS traffic can consume session resources and throttle WPS flows. The implemented architecture mitigates this via wpsOnlyMode, queue isolation, and selective interface protection mapped to ARP and QCI.

Shared Interface QoS Degradation

WPS bearer traffic risks being deprioritized if DSCP markings are stripped or misconfigured across N3, SBI, or PFCP interfaces. Persistent DSCP tagging (e.g., DSCP 47) at UPF and TAS preserves QoS across 5GC and IMS transport paths.

Mitigation Summary

Threat	**Mitigation Mechanism**
RPH Spoofing	Namespace validation, TAS header injection
Emergency Call Misrouting	Emergency prefix bypass logic
SIP Latency Breach	SPL-based protected queues, DSCP 47 marking
Overload Blocking WPS	Overload-exclude profiles, wpsOnlyMode
QoS Collapse on Shared Interfaces	DSCP enforcement on N3/SBI/PFCP paths

9. Conclusion

IMS-based Wireless Priority Service (WPS) platform has been extensively validated to support national-level emergency communication requirements with technical precision and policy compliance.

The system exhibited exceptional performance in maintaining call integrity, enforcing real-time prioritization using the Resource Priority Header (RPH), and upholding latency guarantees even under congested conditions. The WPS architecture not only adhered to 3GPP, FCC, and DHS specifications but also demonstrated its operational maturity by handling complex session scenarios such as mid-call modifications, emergency bypass, and overload protections with deterministic behavior.

This implementation underscores the critical value of a standards-compliant, dynamically configurable IMS core that can be scaled during emergencies without compromising service availability. Through seamless coordination among IMS components (P-CSCF, I/S-CSCF, TAS), robust configuration policies, and comprehensive KPIs, the solution proves its readiness for nationwide deployment. Importantly, this work validates that WPS can coexist with standard public services, ensuring equitable access while prioritizing mission-critical users. Future enhancements may focus on expanding support across additional network interfaces, automation of profile synchronization, and real-time analytics integration for continuous assurance.

References

1. Cybersecurity and Infrastructure Security Agency (CISA), “Wireless Priority Service and GETS Documents,” 2024. [Online]. Available: https://www.cisa.gov/resources-tools/resources/wpsgets-documents
2. Cisco Systems, *Ultra Cloud Core 5G Session Management Function Configuration Guide*, Release 2023.04, Oct. 2023.
3. Cisco Systems, *Wireless Priority Services Overview and Configuration*, Cisco Support Documentation, 2023.
4. FirstNet Authority, “Wireless Priority Service: Emergency Communication Readiness,” FirstNet.gov, 2022. [Online]. Available: https://www.firstnet.gov
5. Verizon, “Frontline Wireless Priority Service for First Responders,” 2022. [Online]. Available: https://www.verizon.com/business/products/frontline
6. AT&T, “Wireless Priority Service (*272 Calling),” AT&T Public Safety Support, 2022. [Online]. Available: https://www.att.com/support/article/wireless/KM1009152
7. 3GPP, *TS 23.502 - Procedures for the 5G System (5GS); Stage 2*, v17.4.0, Sep. 2022.
8. 3GPP, *TS 23.501 - System Architecture for the 5G System (5GS)*, v17.6.0, Sep. 2022.
9. 3GPP, *TS 24.301 - Non-Access-Stratum (NAS) protocol for Evolved Packet System (EPS)*, v17.4.0, 2022.
10. Cisco Systems, *Policy Builder User Guide: Diameter Routing and DSCP Marking*, 2023.
11. IETF, “Differentiated Services Code Point (DSCP) for WPS Traffic,” RFC documentation, 2021.
12. D. Johnson et al., "A Standards-Based Approach to Prioritized Mobile Communication," in *IEEE Communications Standards Magazine*, vol. 6, no. 1, pp. 44-51, Mar. 2022.
13. J. Lee, “Resilient Communications Infrastructure for Emergency Response,” *Journal of Telecommunications Policy*, vol. 46, no. 7, Jul. 2022.
14. H. Schulzrinne and J. Polk, "Communications Resource Priority for the Session Initiation Protocol (SIP)," RFC 4412, Internet Engineering Task Force (IETF), Feb. 2006.
15. V. Gurbani, R. Jain, and G. Camarillo, "Overload Control in the Session Initiation Protocol (SIP)," RFC 7339, IETF, Sep. 2014.
16. 3GPP, *TS 29.328 - Sh Interface based on the Diameter protocol*, v13.7.0, Dec. 2015.
17. National Communications System, *Government Emergency Telecommunications Service (GETS) and Wireless Priority Service (WPS)*, NS/EP GIR, Issue 2.0, Jan. 2013.